UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
GESTÃO DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO

ANNE CAROLINE DIAS BEZERRA

A SEGURANÇA DA INFORMAÇÃO ATRAVÉS DA IMPLEMENTAÇÃO DO ITIL PARA MICRO E PEQUENAS EMPRESAS

TRABALHO DE CONCLUSÃO DE CURSO

CURITIBA
2019

ANNE CAROLINE DIAS BEZERRA

A SEGURANÇA DA INFORMAÇÃO ATRAVÉS DA IMPLEMENTAÇÃO DO ITIL PARA MICRO E PEQUENAS EMPRESAS

Trabalho de Conclusão de Curso apresentado ao Curso de pós graduação em Gestão de tecnologias da informação e Comunicação da Universidade Tecnológica Federal do Paraná, , como requisito parcial à obtenção do título de pós graduando Agrônomo.

Orientador: Prof. Msc. Christian C. S. Mendes

CURITIBA

2019

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Câmpus Curitiba
Diretoria de Pesquisa e Pós-Graduação
IV CURSO DE ESPECIALIZAÇÃO EM GESTÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

TERMO DE APROVAÇÃO

A SEGURANÇA DA INFORMAÇÃO ATRAVÉS DA IMPLEMENTAÇÃO DO ITIL PARA MICRO E PEQUENAS EMPRESAS

Por
Anne Caroline Dias Bezerra

Esta monografia foi apresentada às **17:00 h** do dia **10/05/2019** como requisito parcial para a obtenção do título de Especialista no CURSO DE ESPECIALIZAÇÃO EM GESTÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO, da Universidade Tecnológica Federal do Paraná, **Câmpus Curitiba**. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho:

1	**X**	Aprovado
2		Aprovado condicionado às correções Pós-banca, postagem da tarefa e liberação do Orientador.
3		Reprovado

_____

Prof. _____
UTFPR - **Alexandre Jorge Miziara**

_____

Prof. _____
UTFPR – Christian Carlos Souza Mendes

_____

Prof. Msc. Alexandre Jorge Miziara
UTFPR – Coordenador do Curso

A “Ata de Defesa” e o decorrente “Termo de Aprovação” encontram-se assinados e devidamente depositados na Coordenação do Curso de Gestão de tecnologias da informação e comunicação da UTFPR Câmpus Curitiba, conforme Norma aprovada pelo Colegiado de Curso.

AGRADECIMENTOS

Agradeço primeiramente a deus por me acompanhar nesta jornada. A minha família que mesmo longe me incentivou desde o início dessa caminhada e me proporcionou apoio nos momentos de tristeza e desafios. Agradeço em fim ao professor Christian Mendes que orientou de maneira que eu pudesse concretizar esse trabalho.

“A tarefa não é tanto ver aquilo que ninguém viu, mas pensar o que ninguém ainda pensou sobre aquilo que todo mundo vê.” (Arthur Schopenhauer)

RESUMO

BEZERRA, Anne. A segurança da informação através da implementação ITIL para micro e pequenas empresas. 88 f. TCC, (Gestão de tecnologias da informação e comunicação), Universidade Tecnológica Federal do Paraná. 2019.

.

A segurança da informação é um assunto que vem crescendo e tomando um âmbito de pesquisa muito amplo, com a domesticação de dispositivos mobiles e a internet e tornou-se parte essencial do cotidiano da sociedade. Contudo, do ponto de vista corporativo, vê-se milhões de informações secretas e sensíveis circulando diariamente entre esses ativos tecnológicos. Devido a isso, as micro e pequenas empresas tem sofrido um atraso de estruturação nesse contexto de segurança de desses ativos, por isso essa pesquisa visa entender os principais fatores que estão atrelados a esse cenário e com resultados obtidos será estruturada uma modelagem baseada no contexto organizacional e regional nas quais as micro pequenas empresas estão inseridas.

Palavras-chave: Segurança da informação, Governança em TI, ITIL, ISO 27001, Micro e pequenas empresas, Lei geral de proteção de dados.

ABSTRACT

BEZERRA, Anne. Information security through ITIL implementation for micro and small businesses. 35 f. TCC, (Information Technology and Communication Management), Universidade Tecnológica Federal do Paraná. 2019.

Information security is a growing subject and taking a very broad scope of research, with the domestication of mobile devices and the internet, it has become an essential part of society's everyday life. However, from the corporate point of view, millions of sensitive and secret information are seen and circulating daily among these technological assets. Due to this, the micro and small businesses have suffered a delay of structuring in this context of security of these assets, for that matter, this research aims to understand the main factors that are linked to this scenario and with results will be structured a modeling based on the organizational context that the small businesses are are embedded

Keywords: Information Security, IT Governance, ITIL, ISO 27001, Micro and Small Businesses, General Data Protection Act.

LISTA DE ILUSTRAÇÕES

Figura 01. Percentual de microempresas que possuem uma política de segurança em TI/TIC formalmente definida, 2010 Fonte: IBGE, diretoria de pesquisas, Coordenação de Industrias, Pesquisa sobre o uso de tecnologias da informação e comunicação nas empresas 2010.....114
Figura 02. Percentual total de incidentes reportados ao CERT.br por ano Fonte: CERT BR, 2013.....115
Figura 03. Ciclo de vida de serviços ITIL Fonte: TSO, 2012.....37
Figura 04. Sete passos do processo de melhoria Fonte: TSO 2012 49
Figura 5. Classificação de empresas conforme a ocupação. Fonte: SEBRAE, 2014.....60
Figura 06. Modelo de ciclo de vida baseado em *PDCA* Fonte: Realizada pelo autor.....74
Figura 07. Modelo de passos do processo baseado em PDCA e ciclo de vida ITIL. Fonte: Realizado pelo autor 75

LISTA DE TABELAS

Tabela 01. Conceitos chaves dos Serviços de estratégias Fonte: VERHEIJEN, 2008 adaptado pelo autor ..40
Tabela 02. Papéis chaves da Estratégia de serviço. Fonte: TSO, 2012. Adaptado pelo autor. 42
Tabela 03. Processos e atividades chaves de design de serviço Fonte: TSO, 2012 , adaptado pelo autor.....44
Tabela 04. Papéis chaves do processo de Design de serviço. Fonte: TSO 2012, Adaptado pelo autor. 44
Tabela 05. Processos de transição de serviço Fonte: VERHEIJEN 2008, Adaptado pelo autor.....46
Tabela 06. Atividades de transição de serviço. Fonte: Verheijen 2008, Adaptado pelo autor.....46
Tabela 07. Processos de operação de serviço. Fonte: VERHEIJEN 2008, Adaptado pelo autor.....48
Tabela 08. Atividades de operação de serviços. Fonte: VERHEINJEN 2008, Adaptado pelo autor.....48
Tabela 07. Características de estrutura da MPE. Fonte: CAMPONAR 2004 apud LEONE 1999, adaptado pelo autor 61
Tabela 08. Variáveis consideradas referentes a estrutura MPE 69
Tabela 09. Constantes consideradas na estrutura MPE.....69

LISTA DE GRÁFICOS

Gráfico 01. Fonte: Realizada pelo autor 63
Gráfico 02. Fonte: Realizada pelo autor 64
Gráfico 03. Fonte: Realizada pelo autor 65
Gráfico 04. Fonte: Realizada pelo autor 65
Gráfico 05. Fonte: Realizada pelo autor 66

LISTA DE SIGLAS E ACRÔNIMOS

TIC – Tecnologia da Informação e Comunicação

LGPD – Lei geral de proteção dos dados

MPE – Micro Pequena Empresa

TI - Tecnologias da informação

ITIL – *Information Tecnology Infraestructure Libary*

VPN – *Virtual Private Network*

PK*I* – *Public Insfraestructure Key*

ISMS – Information Security Management System

PDCA – *Plan Do Check Act*

ITSM –*Information Technology Service Management*

CEO – Chief Executive Office

SUMÁRIO

1 INTRODUÇÃO **113**
2 OBJETIVOS E ORGANIZAÇÃO DO TRABALHO **115**
2.2 Objetivos gerais e específicos 115
2.3 Organização do Trabalho 116
3 REFERENCIAL TEÓRICO **116**
3.1 Segurança da informação 116
3.2 Pilares e Princípios da segurança da informação 117
3.3 Normas do sistema de gestão de segurança da informação ISO/IEC 27001 119
3.4 Técnicas da segurança da informação 21
3.5 ISO/IEC 27001 23
3.5.1 Requisitos de contexto organizacional **23**
3.5.2 Contexto de liderança **24**
3.5.3 Contexto de Planejamento **25**
3.5.4 Contexto de suporte **28**
3.5.5 Operação **30**
3.5.6 Contexto de Avaliação de desempenho **31**
3.5.7 Melhorias **32**
3.6 A infraestrutura da tecnologia da informação 33
3.7 ITIL 35
3.7.1 Fases do Ciclo de vida ITIL **37**
3.7.2 Considerações ITIL **50**
3. 8 Riscos e vulnerabilidades 50
3.9 Ataques 53
3.10 Atacantes 55
3.11 Lei Geral de proteção de dados 56
3.11.1 Base Legal **57**
3.11.2 Obrigações da organização detentora **58**
3.12 A segurança da informação em mpes (micro e pequenas empresas) 59
3.12.1 Perfil das MPES **59**
3.12.2 Como é tratada **61**
4 LEVANTAMENTO DE DADOS **63**
5 RESULTADOS **68**
5.1 Proposta do novo modelo para MPEs 68
6 CONCLUSÕES **78**
7 Anexo I **79**
7 REFERÊNCIAS **84**

1 INTRODUÇÃO

No cotidiano atual no qual estamos inseridos hoje, é muito comum se deparar com notícias de ataques cibernéticos contra indivíduos ou organizações, vazamento de dados sensíveis ou roubo de informações privilegiadas, por isso, cada vez mais o assunto segurança de dados e informação nos atuais parâmetros da sociedade é imprescindível, o que favorece a discussão e a necessidade de pesquisa sobre esse tema.

Hoje com a expansão da internet, das tecnologias, e do valor das informações que trafegam em dispositivos móveis como celulares, tablets e computadores, torna-se inviável não possuir um método efetivo que proporcione a segurança destes ativos.

Dentro do contexto organizacional, a tecnologia e a rede de computadores se vê como objeto de trabalho e faz parte do dia-dia do negócio. Em uma pesquisa realizada pela 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 é importante observar a importância e o crescimento deste setor para a economia brasileira, outra pesquisa realizada pelo IBGE em 2010 demonstra que o uso das Tecnologias da Informação e Comunicação (TIC's) dentre as empresas pesquisadas, 2,2 milhões cerca de 80,8% delas utilizam computadores, 2,1 milhões totalizando 76,9% delas fazem o uso da internet e por fim cerca de 2,3 milhões, aproximadamente 83,3% utilizam o telefone celular como ferramenta de trabalho. Esses dados nos ajudam a concluir 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.

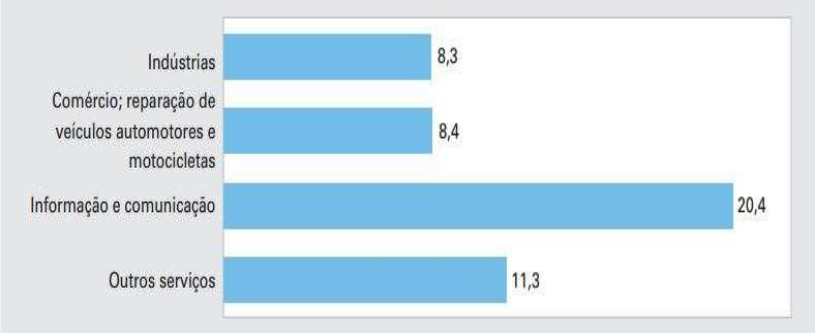
A partir desses dados que objetam uma clara curva de potencial de crescimento dentro do contexto de MPEs é possível expor uma importância que a segurança pode adquirir conforme

o crescimento do uso de tecnologias no setor MPEs, somado ao crescimento de sua representação no PIB na economia brasileira. Resultantes que se incluídas 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 em 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 o setor de manufatura e principalmente nas pequenas empresas nas quais, foram o alvo de 31% dos ataques em 2012, a Symantec ainda acrescenta que as MPEs são alvos atraentes, por não darem a devida importância a ferramenta ou políticas que as proteja 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 e tabela a seguir.

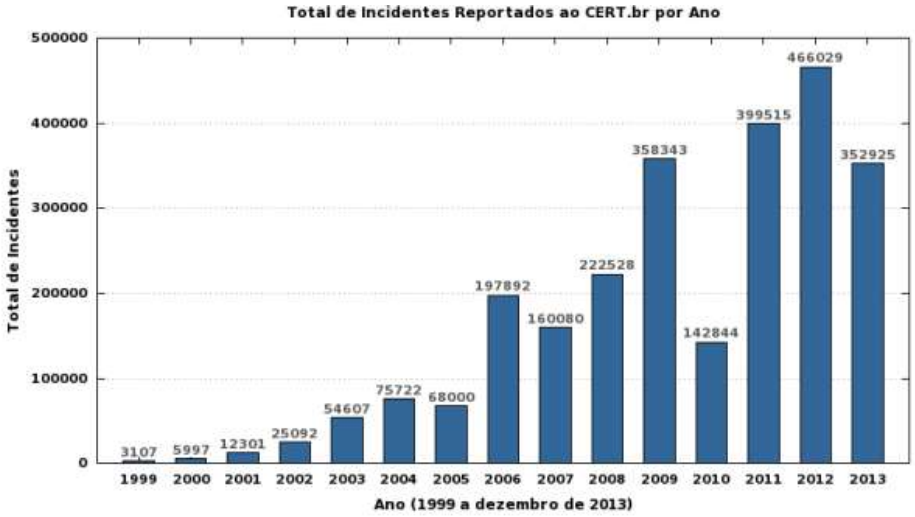
Figura 01. Percentual de microempresas que possuem uma política de segurança em TI/TIC formalmente definida, 2010



Fonte: IBGE, diretoria de pesquisas, Coordenação de Industrias, Pesquisa sobre o uso de tecnologias da informação e comunicação nas empresas 2010.

A seguir também é demonstrado através dos dados do CERT (2013) o percentual de incidentes relacionados à segurança da informação progressivamente ao longo dos anos.

Figura 02. Percentual total de incidentes reportados ao CERT.br por ano



Fonte: CERT BR, 2013.

2 OBJETIVOS E ORGANIZAÇÃO DO TRABALHO

2.2 Objetivos gerais e específicos

O principal objetivo desse trabalho, através de pesquisa bibliográfica entender as métricas de modelagem internacional de segurança da informação ISO 27001, dos aspectos estruturais da infraestrutura do ITIL, tudo isso levando em consideração como ela pode ser utilizada e quais de seus aspectos podem ser implementados de forma satisfatória em 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. Propor um documento de boas práticas para uso por parte das micro e pequenas empresas;

2.3 Organização do Trabalho

Este Trabalho, além desta introdução, está dividido em 04 principais capítulos e anexos.

O Capitulo 3 apresenta o referencial teórico e as definições sobre a Segurança da informação e seus componentes, pilares, técnicas, ferramentas e sobre a norma ISO/IEC 27001, ITIL e da lei geral de proteção de dados.

O Capitulo 4 é apresentado a problemática da segurança da informação em MPEs, discorrendo sobre o perfil das MPEs, como é tratado o assunto e um levantamento de dados obtidos.

O Capitulo 5 apresenta os resultados e as propostas do novo modelo e metodologia atribuída.

Por fim a conclusão apresentará as considerações finais de acordo com a pesquisa realizada e por fim as referências bibliográficas

3 REFERENCIAL TEÓRICO

3.1 Segurança da informação

Um conceito básico que define a Segurança da Informação de acordo com Beal (2005) é algo que resume um processo inerente a proteção de dados informacionais diante as possíveis ameaças quanto a sua integridade, disponibilidade e confiabilidade.

Entende-se por segurança como algo que seja livre de qualquer perigo, riscos ou danos. Segundo o dicionário Aurélio 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”. 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). Ou seja, faz referência a implementação de métodos, de políticas de prevenção, do monitoramento do acesso, do uso incorreto ou modificação não autorizada dos recursos que compõe este sistema. Os sistemas computacionais, atualmente, possuem uma interligação através de uma infraestrutura de redes, onde também atribuem-se 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, junto a essa fundamentação é necessário, segundo RHODES-OYSLEY (2013) levantar alguns questionamentos que justificam a importância e a necessidade de um algum tipo de infraestrutura de 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 apresentação 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. Definir, alcançar, manter e melhorar a segurança da informação podem 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". A partir disso pode-se afirmar que a segurança, do ponto de vista computacional para as organizações, se tornou uma vantagem competitiva e não apensas uma necessidade.

3.2 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 da segurança em rede de computadores como um conjunto de métodos, procedimentos e políticas que protegem uma rede computacional que possui dados. Este dado nada mais é que a informação bruta, e a informação é um resultado da organização desses dados. Em redes de computadores, pacotes ou datagramas são caracterizados como uma estrutura de transmissão de dados que são enviados através de um sistema de comunicação, a rede 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. Com a finalidade de prover segurança em redes de computadores há a necessidade de garantir algumas propriedades. (KUROSE, 2010) define 4 propriedades estreitamente interligadas:

> **Confidencialidade:** Somente o remetente e o destinatário pretendido devem poder entender o conteúdo da mensagem transmitida. O fato de abelhudos poderem interceptar a mensagem exige, necessariamente, que esta seja cifrada de alguma maneira para impedir que uma mensagem interceptada seja entendida por um interceptador. Esse aspecto de confidencialidade é, provavelmente, o significado mais comumente percebido na expressão *comunicação segura.*
> **Autenticação do ponto final:** O remetente e o destinatário precisam confirmar a identidade da outra parte envolvida na comunicação, confirmar que a outra parte realmente é quem alega ser. A comunicação pessoal entre seres humanos resolve facilmente esse problema por reconhecimento visual. Quando entidades comunicantes trocam mensagens por um meio pelo qual não podem ver a outra parte, a autenticação não é assim tão simples. Por que, por exemplo, você deveria acreditar que o e-mail que recebeu e que contém uma sentença afirmando que aquele e-mail veio de um amigo realmente veio daquele amigo? **Integridade de mensagem:** Mesmo que o remetente e o destinatário consigam se autenticar reciprocamente, eles também querem assegurar que o conteúdo de sua comunicação não seja alterado, por acidente ou por má intenção, durante a transmissão. Extensões das técnicas de soma de verificação que encontramos em protocolos de transporte e enlace confiáveis podem ser utilizadas para proporcionar integridade à mensagem.
> **Segurança operacional:** Hoje quase todas as organizações (empresas, universidades etc.) possuem redes conectadas a internet pública. Essas redes podem ser comprometidas potencialmente por atacantes que ganham acesso a rede por meio da internet pública. Os atacantes podem tentar colocar worms nos hospedeiros da rede, adquirir segredos corporativos, mapear as configurações da rede interna e lançar ataques DoS.

Porém alguns outros autores como TANENBAUM (2011) incluem mais uma propriedade que deve-se também garantir, o não repúdio que é definido por BAR (2003) como sendo “suficiente evidência para persuadir a autoridade legal a 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.

É importante definir 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 é compreendida a existência de mais um agente 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 foi percebido 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 a proteção dos dados na rede, e na investigação e a aplicação de serviços de proteção das informações, algumas dessas propriedades já foram acima citadas são elas: confidencialidade, autenticação, integridade da mensagem e segurança operacional além de outras que foram consideradas por outros autores como muito importantes, sendo elas sigilo, e o não repudio TANENBAUM (2011).

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

É inegável o valor que uma norma de certificação acrescenta no domínio de gestão de empresas, novas certificações vem 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 um objeto chave de competitividade no panorama 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, implementar requisitos que mantenham e melhore continuamente o sistema de segurança da informação”. Surgindo em 1989 dos primórdios do comercio e indústria do reino unido, através das necessidades de um código de boas práticas deste departamento (MOURA, 2007); e a partir daí se transformou na família SGSI (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)

Que são as normas de padrões de competências estabelecidas e documentadas internacionalmente que temos hoje, sendo que as mais utilizadas como referência e mencionadas em publicações de pesquisa são as 27000, 27001 e 27002.

3.4 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 (UNKNOW, Whashington Journal 2014), a segurança de rede envolve diversas áreas.

Existem algumas das políticas que podem ser feitas para o acesso seguro de serviços e informações, Segundo QUINTAO (2005) os conceitos 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):

- Identificação do usuário e autorização de controle de acesso

O nível mais simples dos mecanismos, a identificação do usuário, é um mecanismo que parece ser ingênuo e as vezes até inofensivo é um passo extremamente importante para garantir a segurança e a confiabilidade da rede, este mecanismo garante que somente tenha acesso a rede usuários cadastrados, e o mais importante, determina uma teia de acesso para cada nível de usuário, ou seja, nele é determinado quais conteúdos e serviços tais determinados usuários possuem a permissão de acesso. Nos tempos atuais para o controle de acesso a combinação *login* e senha já não é o suficiente para fazer a garantia da rede, hoje em grandes empresas são utilizados certificados digitais, biometria e outros tipos de mecanismos. Fora do ambiente corporativo é frequentemente utilizado o firewall que sobre definição é método e dispositivo utilizado como uma política de segurança, nele é possível fazer um filtro de pacotes, ou de proxy de aplicações. O firewall protege a conexão entre a interconexão de uma ou mais redes.

- Proteção de dados armazenados

Este mecanismo se diz respeito no conceito de integridade da informação, a integridade da mensagem diz respeito quando a informação é armazenada seja física ou logicamente (hardware, nuvem, banco de dados) para que isso seja feito de maneira que não quebre a integridade da mensagem é preciso adotar alguns sistemas como o antivírus, e ou sistemas que fazem a autenticação e autenticidade da mensagem.

- 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 algumas táticas que são empregadas, são elas (YOURDON, 2002): Criptografia é a codificação da mensagem de forma que sejam ininteligíveis 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 usado é pra quando a informação é interceptada, que haja a autenticação do usuário, que a mensagem só seja aberta caso haja a confirmação de que aquele usuário tenha permissão de acesso a informação.

- Auditoria de acesso as informações

Auditoria é uma pratica comum em empresas, onde um sistema mantem registros das atividades e transações realizadas pelos usuários do sistema (YOURDON, 2002). Através dessa prática é atribuído uma cadeia de usuários com acesso e permissões exclusivas, o usuário administrador, que pode ter um acesso privilegiado e o controle dos dados e acessos de todos os indivíduos do sistema, ele também é responsável por monitorar a rede e seus usuários, e é capaz de perceber se existe algum usuário malicioso tentando acessar dados fora da sua teia de acesso através da pratica de manter registro e logs de trafego e na análise desses registros.

- Monitoramento de intrusos

Uma prática que envolve sistemas específicos, sistemas que fazem monitoramento de ataques, esses sistemas fazem também analise e diagnostico de vulnerabilidades já explicitado 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.

3.5 ISO/IEC 27001

Foi embasado por (MOURA, 2007) que a modelagem de especificações incluem requisitos de controle de segurança personalizado para que seja adaptável para as características e exigências de cada organização e suas partes competentes, trazer como parâmetros de resposta métodos que implementam, operam, monitoram, revisam, mantem e melhoram o sistema de gestão documental da segurança da informação(SGSI) dentro da organização é uma característica bem especifica 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 as partes interessadas". Além de esta norma ter como base a política organizacional e implementação da segurança, também foi projetada para ser flexível e como resultado introduziu o modelo cíclico "PLAN-DO-CHECK-ACT" (PDCA).

> Planejamento (Estabelece o SGSI): Estabelece a política SGSI, objetivos, processos e procedimentos relevantes para a gestão de risco e melhora a segurança da informação para fornecer resultados de acordo com os objetivos globais da organização.
> Fazer (Implementar e operar o SGSI): Implementação das políticas , controles, processos e procedimentos do SGSI.
> Checar (Monitoramento e revisão do SGSI): Avaliar e, quando aplicável, medir o desempenho do processo contra a política SGSI, objetivos e experiência pratica e relatar os resultados para o gestor para revisão.
> Agir (Manutenção e melhoria do SGSI): Tomar ações corretivas e preventivas, com base nos resultados da auditoria interna da gestão do SGSI. (CAMPONAR, 2004)

As variáveis das práticas organizacionais serão apresentadas nas seções posteriores, elas se referem a operações que devem ser adotadas e que implicam em 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 processo.

3.5.1 Requisitos de contexto organizacional

A ISO pode ser aplicada em qualquer contexto organizacional, para que isso aconteça a mesma conversa sobre quais os níveis de entendimento que devem estar claro no contexto da organização, logo nos primeiros tópicos da regulamentação é documentado que deve-se entender e determinar 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 e abraça-lo a ao sistema para que não afete ambas as partes é um argumento importante para a implementação do padrão.

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 determina-lo será preciso dos 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 devem 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 deve estabelecer, implementar, manter e melhorar continuamente o sistema de gestão da segurança da informação (ISO/IEC, 2013).

3.5.2 Contexto de liderança

- **Liderança e compromisso**

A liderança e a alta administração devem demonstrar seu compromisso com o sistema de gestão de segurança através dos seguintes argumentos:

> Garantindo que os objetivos da política de segurança da informação estejam estabelecidos;
> Assegurando que a integração dos requisitos do sistema de gestão de segurança da informação nos processos da organização;
> - Assegurando que os 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 resultado pretendido(s);
> - Dirigindo e apoiando as pessoas a contribuir para a eficácia do sistema de gestão da segurança da informação;
> - Promovendo melhoria continua;

- Apoiando outros relevantes;
(ISO/IEC, 2013).

- **Políticas**

Neste tópico é necessário 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” (ISO/IEC, 2013) além dessas condições as políticas de segurança devem satisfazer essas qualidades, e estar disponíveis e documentada; estar disponível para as partes interessadas e ser aberta dentro da organização (ISO/IEC, 2013).

- **Papéis organizacionais, responsabilidades e autoridades**

Neste tópico é importante que a alta gestão garanta que haja autoridades e responsabilidades aos papeis e funções importantes a informação. É importante delegar essas 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) é importante que fique claro o papel de cada um na gestão da segurança da informação.

3.5.3 Contexto de Planejamento

- **Ações para enfrentar os riscos e oportunidades**
  - **Geral**

Estabelecer objetivos de segurança da informação orientadas para a *ISMS (Information Structure Management System)* é um parâmetro importante quando se trata deste contexto de habilidades que a organização precisa considerar. Esse planejamento é imprescindível e deve ser considerado o contexto organizacional, que deve ser coerente em sua totalidade e competências, tais que devem ser levantadas nos requisitos de contexto organizacional

anteriormente dissertado. Esses pontos devem ser alinhados a um ponto em que permitam uma linha de coerência que leve em consideração ambos os lados dos riscos e oportunidades e o contexto organizacional. A norma ISO/IEC 27001 (2013) 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).

- **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 seja feita 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 em 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 análise de risco e fazer uma análise de critério e prioridade, cada um desses processos são importantes e devem ser documentados sobre cada passo de avaliação dos riscos conforme é explicitado pela norma ISSO/IEC 27001 (2013).

- **Tratamento de riscos de segurança da informação**

Neste tópico a norma ISSO/IEC 27001 (2013) trata em 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) seleção de opções de tratamento de riscos adequado, tendo em conta o risco e os resultados da avaliação;
> B) determinar todos os controles que são necessárias 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.
> F) 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).

- **Objetivos de segurança da informação e planejamento para alcança-los.**

Ter objetivos é o primeiro passo para definir uma estrutura de planejamento para alcança-los. Anteriormente vimos 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, isso traz mais coerência e conformidade ao *ISMS*, neste tópico esse assunto não é tratado diferente, a ABNT NBR ISSO/IEC 27001 (2013) regula que os objetivos de segurança da informação devem ser consistentes com a política de segurança, assim como ter requisitos de aplicações de segurança da informação, os resultados da avaliação de riscos e de tratamento deles, outro ponto muito importante é a comunicação, esses requisitos e objetivos devem ser passados adiante, assim como deve estar em constante atualização e manter sempre estas práticas documentadas, e então após o estabelecimento dos objetivos é importante que a organização planeje como alcançá-los e determine passos bem definidos, como exemplo, como será feito, quais recursos serão necessários, quem será o responsável, o tempo de conclusão e

como será avaliada no término, se os objetivos foram alcançados em sua totalidade e se houve atrasos . São tratamentos de uma fase de consolidação de uma prática de processo que deve estar estruturada e adequada ao padrão organizacional.

3.5.4 Contexto de suporte

- **Recursos**

Neste módulo é importante uma rede que disponibilize instancias, componentes e recursos que satisfaçam as necessidades dos processos *ISMS*, a descoberta ou disponibilização de recursos devem ser projetados para considerar um domínio de aplicação especifico e devem ser sensíveis a melhorias continuas, 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 continua do sistema de gestão de segurança da informação". (ISO/IEC, 2013)

- **Competências**

Neste requisito é proposto uma relação entre competências dos recursos humanos disponíveis, portanto é preciso se certificar que os colaboradores estão de acordo, alinhados e que possuem competências necessárias para realização de seu papel para que não afete o desempenho da segurança da informação, além de garantir que esses comportamentos estão sendo cobertos, com os ativos sendo educados e treinados dentro destas boas práticas, outro princípio importante é a documentação como prova de competência e como ação aplicável de transferência dessa competência, este modulo 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 onde exige que a informação tem de ser documentada. (ISO/IEC 27001, 2013).

- **Consciência**

A consciência dos colaboradores da organização é o assunto tratado 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 quais as implicações e inconformidades são resultantes no *ISMS* caso esses requisitos não sejam atendidos. (ISSO/IEC 27001, 2013).

- **Comunicação**

Neste requisito é tratado 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".

- **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 a ISO pode ser notado que a norma exige (ISO/IEC 27001, 2013) em grande parte dos processos de boas práticas que se mantenha uma documentação. A partir disso é possível enxergar a importância de que a documentação carrega quando o assunto é boas práticas no contexto *ISMS*. Por isso não poderia faltar na regulamentação um tópico sobre o mesmo. 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, também a organização deve se assegurar de que haja uma descrição detalhada de identificação (título, data, autor, número de referência) que tenha um formato padrão e que passe sempre por uma análise e aprovação.

Existe tópicos que falam sobre o controle dessas informações documentadas onde se é exigido que a documentação esteja propriamente disponível porém adequadamente protegida, também é ressaltado os seguintes parâmetros: ISO/IEC 27001 (2013) 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.”

Assim sendo é percebido a importância da documentação no *ISMS*, seu tratamento faz parte tanto das boas práticas como uma maneira de desenvolver processos concisos e alinhados a expectativa da organização.

3.5.5 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. O controle pode ser enxergado como uma fase desse processo no qual a organização deve planejar, implementar e controlar todos os processos que englobam e impactam de alguma forma a segurança da informação. Neste tópico a regulamentação trata a implementação de um plano para alcançar objetivos citados nos tópicos de ações para enfrentar riscos e oportunidades e nos objetivos e planos para alcança-los. Dentro deste plano operacional é exigido 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, é exigido 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).

Tendo em conta sempre o resgate do levantamento dos objetivos e dos planos para alcança-los 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 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 deve ser planejado, controlado e avaliado as operações necessários para atender aos requisitos do *ISMS*, os discutidos 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
- E implementar um plano de tratamento de riscos de segurança.

Em suma 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 suas consequências quando necessários.

3.5.6 Contexto de Avaliação de desempenho

- **Monitoramento, medição, análise e avaliação**

Neste tópico a norma se dedica em falar sobre avaliação de desempenho e da sua eficácia no sistema SGSI, alguns tópicos são determinados para que a organização os preencha, a avaliação constitui-se 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 análise dos resultados e medições seja provada na documentação (ISO/IEC 27001, 2013).

- **Auditoria interna**

O processo de auditoria interna é um método chave para avaliar e acompanhar o desempenho do *ISMS*, através dela é possível verificar o desempenho de processos e ferramentas para auxiliar sua melhoria continua. 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 pela norma, é explicitado de maneira clara e objetiva pois é uma prática importante que traz respostas e resultados de avaliação que se feitas de maneira adequada conduzem grandes resultados e impactam na qualidade da *ISMS*.

- **Gestão de avaliação**

Neste tópico cabe a alta a administração garantir a contínua pertinência, adequação e eficácia dos passados tópicos e de quaisquer 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 avaliados um 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 estatuto 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*.

3.5.7 Melhorias

O tópico final trabalha requisitos que abordam a não-conformidade e medidas corretivas, é discorrido (ISO/IEC 27001, 2013) que 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 (ISO/IEC 27001, 2013) é o de fazer um estudo que determine essas causas e se existem similaridade em

outros processos, implementar alterações e ações corretivas quando necessário, avaliar sua eficácia e documentar a caráter dessa inconformidade bem como as causas, consequências e ações tomadas subsequentemente, assim sendo, a organização deve buscar através dessas boas práticas melhoria continua, reagindo sempre a inconformidades, as corrigindo e se adequando para que torne o *ISMS* mais eficaz .

3.6 A infraestrutura da tecnologia da informação

O termo infraestrutura foi definido por G. C. BOWKER (2010) como :"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 infraestrutura "Abrange também as entidades mais abstratas como os protocolos (humanos e computacionais), normas e memória". Como foi definido a cima pode-se concluir que a infraestrutura de suporte a informação envolve recursos diversos tanto humanos como lógicos e computacionais.

No âmbito computacional a infraestrutura da informação é definida pela NFS (2006) como sendo uma "Cyber infraestrutura que integra hardware de computação, redes de dados, sensores digitalmente habilitados, observatórios de instalações experimentais, um switch interoperável de software e serviços de middleware e ferramentas".

Em uma organização é possível identificar diversos conjuntos de fatores que contribuem para uma boa infraestrutura de tecnologias, tais como celulares, computadores, servidores entre outros. Normalmente tais dispositivos são responsáveis pelo processamento de informações que trafegam diariamente em um ambiente corporativo organizacional, por isso a proteção de dados circulados nesses dispositivos precisam ser contemplados.

Com isso podemos dizer que uma estrutura de segurança dentro de uma organização segura não envolve somente um único componente, e sim um conjunto de elementos lógicos, físicos, humanos e organizacionais, que pode ir de ferramentas de software antivírus, à conscientização dos deveres e responsabilidades dos colaboradores a praticas *anti-phishing* e engenharia social são exemplos de bons exercícios a serem seguidos que ajudam a proteger os dados que ali residem.

A partir disso, E. H. DINIZ (2010) definiu uma estrutura de segurança da informação em camadas, sendo elas a camada física, camada lógica e a camada humana.

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 disse "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 é 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".

Quando o assunto é a infraestrutura desses meios computacionais foi visto anteriormente que a segurança de dados em rede devem ser feitas a partir do meio lógico, através de aplicações de segurança, e foi exposto que uma estrutura organizacional segura deve atender não somente a parte lógica como também a física e a humana. Quando se pensa na estrutura da segurança de dados somente no meio lógico implica-se em uma segurança básica com aplicações médias de níveis lógicos porém com alto risco de incidentes de segurança, para se construir uma estrutura completa foi exposto que deve se aderir aos aspectos: físicos, que podem envolver desde o controle de acesso, câmeras de monitoramento e policiamento. E ao aspecto humano, um dos maiores problemas atualmente quando se trata de segurança, de acordo com SCHNEIER; VIEIRA (2001, apud DINIZ 2010) o recurso humano "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 finalidade de prover uma composição de agentes que tornam a estrutura mais segura para a informação.

Sabendo dos riscos atrelados ao mundo informacional tecnológico dentro de organizações coorporativas, podemos nos apoiar à ITIL (*Information Technology Infrastructure Library*) que é um conjunto de práticas detalhadas para gerenciamento de serviços de TI (ITSM) que se concentra no alinhamento de serviços de TI com as necessidades dos negócios.

3.7 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 tratar do processo de gestão de tecnologias da informação.

A ITIL é tratada como um princípio de boas práticas na governança de TI, e segundo (VERHEIJEN, 2008) "A boa prática é uma abordagem ou método que fora comprovado em prática. Boas práticas podem ser um sólido apoio para as organizações que querem melhorar seus serviços de TI."

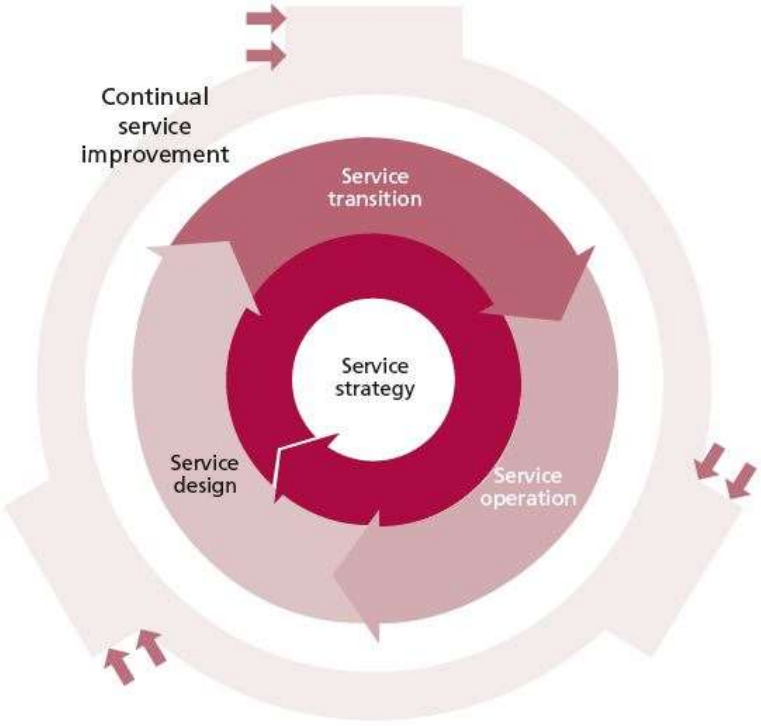
A ITIL é abordada como um conjunto preceitos que foram aprimorados ao longo dos anos que encorajam o encontro dos melhores requisitos de recursos de capacidades, habilidades, processos da estrutura de governança de TI. É um padrão reconhecido mundialmente como uma fonte confiável das melhores práticas de *ITSM (Information Technology Service Management)*, é exposta por TSO (2012) como sendo uma importante estrutura que possui técnicas de gerenciamento de serviços e controles de gestão. (TSO, 2012) ainda acrescenta que a ITIL "Centra-se na medição continua e melhora da qualidade do serviço de TI prestado, tanto na perspectiva de negócio quanto na do cliente." Dentro desta perspectiva que a ITIL destaca é importante perceber as principais contribuições que essa infraestrutura agrega a uma organização, sendo elas: 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; E a melhoria da prestação de serviço de terceiros. (TECHEXCEL, 2012), outros autores (TSO, 2012) complementam 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 a 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 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 a 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 as infraestrutura ITIL estabelece para uma organização, é importante agora, entender como funciona os processos e suas boas práticas de governança, e como eles são divididos. A ITIL v3 Core 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 no ciclo de vida dos requisitos de serviços ITIL.

Figura 03. Ciclo de vida de serviços ITIL



Fonte: TSO, 2012

De acordo com VERHEIJEN (2008) é descrito que o ciclo de vida de serviços ITIL são baseados no conceito de gestão de serviço, no qual é relacionado com os conceito 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 os quais aumentam as chances na obtenção de resultados desejados. Outro conceito descrito é o de valor que é mencionado por (VERHEIJEN, 2008) 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 considerações características que são adeptos as boas práticas ITIL.

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

3.7.1 Fases do Ciclo de vida ITIL

Após observarmos na Figura 01 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 sua 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 , VERHEIJEN, (2008) discorre 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 políticas 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."

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

- **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 porquê 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? (VERHEIJEN, 2008)

Dentro dos conceitos básicos que são utilizados para responder essas perguntas e formular uma estratégia, são através dos quatro P's formulados (VERHEIJEN apud MINTZBER 1994) que são usadas como ponto de partida:

> • 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 01 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 as seguintes conceitos chaves que também ajudam a responder as perguntas que objetivam o serviço de estratégia. Os conceitos estão descritos na tabela a seguir.

Tabela 01. Conceitos chaves dos Serviços de estratégias

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 de 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 análises de impacto de cada prestador de serviço.

Fonte: VERHEIJEN, 2008 adaptado pelo autor

Como esta fase do ciclo de vida tem como objetivo melhorar suas competências básicas, é preciso definir alguns processos e atividades chaves que impulsionem e acarretem no cumprimento desse objetivo.

Esses processos e atividades são separadas por TSO (2012) como: primeiro, estratégia de gestão de serviços de TI, que é uma gestão estratégicas voltadas aos ativos tecnológicos com planos operacionais que garantes que todas as alterações no contexto do negócio seja atualizada no plano estratégico para garantir sua coerência, ele ainda descreve que “a finalidade

de uma estratégia de serviço é articular como um provedor do serviço o que permitirá 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; E segundo, serviço de gestão de portfólio, que possui como finalidade segundo 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; E por fim o 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, são definidos pelo mesmo os papeis chaves que devem ser desempenhados nesta fase do ciclo de vida ITIL, que estão discorridos na seguinte tabela.

Tabela 02. Papéis chaves da Estratégia de serviço.

Papel	Responsabilidades
Gerente estratégico de TI	Formula e comunica a estratégia de TI e se assegura 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	Define serviços e atendimentos, gerencia e mantem portfolio e mantem a relação de comunicação a todas as partes interessadas
Gerente de relacionamento do negócio	Mantem uma relação com o cliente, compreendendo –o e combinando suas necessidades com os resultados obtidos necessidades e

Gerente financeiro	Mantem modelos financeiros com as informações de custo e valor dos serviços de TI
Gerente de demanda	Identifica os perfis de atividade dos usuários e garante que o recursos atendam a demanda
Chefe de recursos	Responsável por liderar e dirigir a terceirização dentro da organização

Fonte: TSO, 2012. Adaptado pelo autor.

- **Serviço de Design**

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 segundo o mesmo, 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 descreve os processos e atividades chaves que devem ser feitos para uma boa exercício dessa fase, que estão descritas na seguinte tabela 03.

Tabela 03. Processos e atividades chaves de design de serviço

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 catalogo 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 às 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	Fornece um ponto de foco e gestão relacionada aos 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 serviços 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 negócio 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 políticas e documentação de design. Gestão de riscos e de todos os processos.

	Alinhamento com todas as estratégias e politicas organizacionais e de TI.

Fonte: TSO, 2012 , adaptado pelo autor.

Tabela 04. Papéis chaves do processo de Design de serviço.

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 políticas 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.

Fonte: TSO 2012, Adaptado pelo autor.

- **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. Dentro desta operação foi definida por TSO(2012) 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. É explicitado por TSO(2012) 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.

Esses conceitos básicos são definidos por (VERHEIJEN, 2008) e são descritos como importantes para que esta fase de transição seja aplicada de forma efetiva na organização, ele ainda 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 as 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, ajudam no apoio a transferência de conhecimento, que é importante assegurar-se de que os conhecimentos existentes estejam disponíveis pra uso, para consultas e reutilização em procedimentos semelhantes; Além de assegurar-se de que os colaboradores envolvidos estejam comprometidos com o processo de transição de serviços e que estejam cientes dos requisitos e de todo 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 05 e 06.

Tabela 05. Processos de transição de serviço

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	Gerencia 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.

Fonte: VERHEIJEN 2008, Adaptado pelo autor

Tabela 06. Atividades de transição de serviço.

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.

Fonte: Verheijen 2008, Adaptado pelo autor.

- **Serviço de Operação**

O propósito da operação de serviço tem a ver 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) com a seguintes características:

> O ***Service Desk,*** é o único ponto de contato para os usuários, ele lida com tudo, incidentes, solicitações de acesso e solicitações de serviços. O objetivo principal do *Service Desk* é restaurar "o serviço normal" para os utilizadores o mais rapidamente possível; **A gestão técnica** refere-se aos grupos, departamentos ou equipes que fornecem técnicas e conhecimentos de gestão global da infraestrutura de TI, o técnico de gestão desempenha um duplo papel. ele possui todos os conhecimentos técnicos e conhecimentos relacionados à gestão da infraestrutura e fornece o real recurso para apoiar o ciclo de vida ITSM(*IT service management*); **Gestão de operações de TI**, executa as atividades operacionais diários necessários para
> gerenciar a infraestrutura de TI, de acordo com os padrões de desempenho definidos durante Service Design**; Aplicação de gestão** é responsável por gerenciar aplicativos em seu ciclo de vida. Gerenciamento de aplicativos também desempenha um papel importante na concepção, testes e melhoria de aplicativos que fazem parte 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 sequência é tratado os processos e atividades fundamentais que englobam esta fase do ciclo de vida, relacionados nas tabelas 07 e 08 a seguir.

Tabela 07. Processos de operação de serviço.

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.

Fonte: VERHEIJEN 2008, Adaptado pelo autor

Tabela 08. Atividades de operação de serviços.

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).

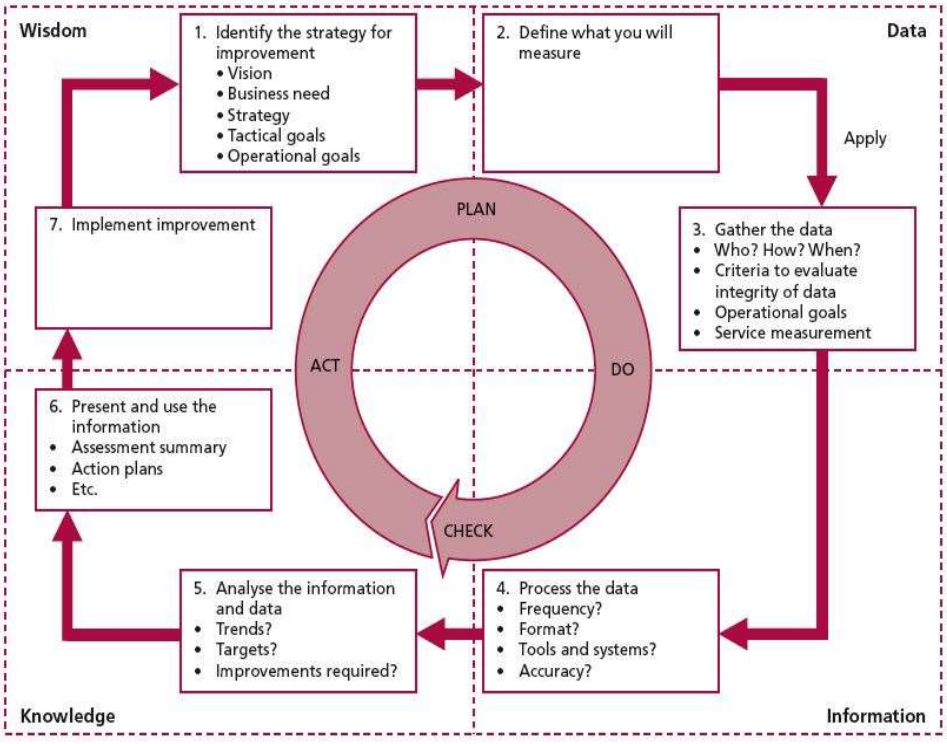
Fonte: VERHEINJEN 2008, Adaptado pelo autor.

- **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 continua, esta etapa tem como intuito de fazer a continua 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 de acordo com TSO(2012) 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 04, 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.

Figura 04. Sete passos do processo de melhoria



Fonte: TSO 2012

Cada passo dessa estrutura demonstrada acima faz parte das táticas de governança estratégicas que são definidas lá 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 no passo 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 são processados, este passo é visto como chave para se entender o impacto desses componentes sobre a infraestrutura de TI, enquanto no passo cinco cabe a ele analisar essas informações, processando os resultados e notando os comportamentos e rotinas resultantes analisa-las se as seguintes questões são respondidas: Estamos cumprindo as metas? Existem tendências claras? É necessário uma ação corretiva? Qual seu custo? E a partir disso, no passo seguinte, passo seis, é feito 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)

3.7.2 Considerações ITIL

A OGC (2014) delibera a importância que a implementação dos processos que compõe o ciclo de vida ITIL estrutura um modelo operacional de alto nível para a organização, seus processos compõem uma estrutura na qual é composta por processos de melhoria nos quais quando implementados, 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 para que seus processos fiquem interligados uns aos outros (como no ciclo de vida) fazendo com que a estrutura da organização seja viva em um ciclo constante de amadurecimento e melhoria.

3. 8 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 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 à segurança da informação são os riscos e ameaças que a segurança física pode ocasionar. 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 e 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 por OUSLEY (2013) 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 com uma política de segurança especificas contra ameaças naturais físicas, que começam desde uma boa instalação elétrica quanto ao número de extintores de incêndio disponíveis, medidas como essa 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, BAGCHI; (2009) 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.

Avançando para 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 usualmente 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 especificas 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
> **Inpeção física** Visitas ao local;
> **Análise de documentos** Análise de documentos de incidentes; (ARRAJ, 2013, apud ISO/IEC 27005)

Essas práticas e métodos de gerencia vulnerabilidades é usada 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 ISSO/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.

3.9 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 é uma pessoa que explora uma vulnerabilidade o que resulta em ataque ao sistema, e prejudica alguma propriedade dos componentes desse sistema. Esses ataques são resultantes da exploração de vulnerabilidades encontradas no sistema , e ao entender como funciona 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 e essa vulnerabilidade são exploradas e se torna o ponto de acesso dos agentes atacantes. Os 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 encontra-se 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, não entradas vulneráveis utilizadas por agentes nocivos para penetrar e ter acesso a dados; existem 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

número 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 distribuída, no qual os ataques estão distribuídos em vários sistemas, “As maquinas 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, uma tática que falsifica os endereços IPs alterando seu cabeçalho para conseguir ter o acesso autorizado; Outra técnica muito conhecida é a de ***Spam***; ***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***, Os *sniffers* 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.

3.10 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 temos, pois ambos servem para nomear pessoas com habilidades invasoras, porém segundo 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 específico 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; ***Black hats,*** Um hacker de chapéu preto/negro 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 os **Engenheiros 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 segundo (CLAYTON S.SILVA, 2012), explica o porquê da 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 notem, esses tipos de abordagem não podem ser previstos ou detectados por algum sistema ou administrador, tornando um método eficaz para a quebra e violação da segurança.

3.11 Lei Geral de proteção de dados

A proteção e o tratamento de dados pessoais é um direito fundamental, para isso foi estabelecido a LGPD que é a sigla da lei geral de proteção de dados pessoais que foi sancionada em agosto de 2018 e estabelece regras sobre coleta, armazenamento e compartilhamento de dados particulares.

Ela foi baseada na GDPR (*General Data Protection Rule*) europeia, que segundo **A. OREL, I. BERNIK , (2018) [A OREL, I BERNIK - Studies in health technology and informatics,**

2018 - researchgate.net] fomenta os direitos individuais e a importância de procedimentos que afetam processadores e controladores de dados sensíveis privados.

A lei LGPD entra em vigência em 2020 e tem como principal objetivo, proteger a privacidade, assegurar a transparência, fomentar o desenvolvimento, padronizar, regulamentar, assegurar a segurança jurídica e o favorecimento à concorrência (LGPD Brasil 2018).
Com a LGPD sancionada no país, ela ajuda a complementar estrutura legais que regulamentam o uso de dados hoje.

3.11.1 Base Legal

Sob o contexto da LGPD foi regulamentado sobre taxas punitivas regras especificas que garantem a proteção de dados pessoais ao titular dos dados.

Sob este contexto, é importante objetivar e analisar os tópicos mais relevantes para essa pesquisa, sendo eles:

• Consentimento do titular dos dados pessoais

A LGPD estabelece que é necessário a obtenção de consentimento do titular do dado, é de responsabilidade o detentor obter a autorização e informar de forma que fique claro a autorização da utilização e do tratamento de dados pessoais para uma finalidade determinada. O consentimento deverá ser fornecido por escrito em cláusula destacada ou por qualquer outra ação afirmativa que demonstre o aceite do titular.
Também está prescrito em lei caso haja mudança na utilização dos dados para a qual o aceitação do titular foi obtida, neste caso, o detentor dos dados deverá informar previamente o titular sobre tal mudança.

- Interesse legítimo:

Para a utilização e tratamento de dados pessoais é necessário que o interesse do controlador ou de terceiro seja legitimo e permitido pela LGPD, desde que tal tratamento não viole os direitos e liberdades fundamentais do titular dos dados e que medidas para garantir a transparência de tal tratamento sejam adotadas. O interesse legítimo deverá ser verificado a partir da análise da situação concreta e com base nos princípios de proteção da lei.

- Tratamento de Dados Pessoais Sensíveis:

Considerando o caráter de dados particulares sensíveis, a LGPD determina o consentimento para o tratamento de dados pessoais sensíveis deve ser fornecido de forma específica e objetiva. O detentor é responsável por ganhar o consentimento e deve se preocupar em obter uma autorização específica para o tratamento de dados pessoais sensíveis.

- Término do Tratamento:

O término do tratamento de dados pessoais deverá ocorrer quando for verificado que a finalidade para a qual o consentimento foi obtido foi alcançada ou que os dados deixaram de ser imprescindíveis ou pertinentes ao objetivo buscado. O termino do tratamento pode acontecer em determinadas circunstâncias: Com o fim do período de tratamento; sob desejo do titular dos dados; por determinação judicial.

3.11.2 Obrigações da organização detentora

Ao se adentrar especificamente a análise dos principais pontos da LGPD que esclarece as principais obrigações que sucumbem os detentores de dados, deve-se destacar que a referida lei discorre principalmente sobre a tratativa quando se detém dados sensíveis, por isso pode-se fazer necessário incluir como influencia o aspecto da intimidade, do Art. 5º, inciso X da Constituição Federal de 1988, o qual faz a separação entre privacidade, segredo e intimidade. (HUBMANN apud COSTA JÚNIOR, 2007). Com a sanção dessa nova lei, os dez princípios emergem com os princípios da privacidade estabelecidos em constituição federal, por isso deve ser abordado que a LGPD elenca dez princípios que a organizações devem estar em conformidade quanto ao tratamento de dados.

> **Finalidade:** O tratamento de dados pessoais deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, observadas as finalidades originárias.
> **Adequação:** O tratamento de dados pessoais deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento.
> **Necessidade:** O tratamento de dados pessoais deve ser limitado ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados

pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.
Livre acesso: É garantida aos titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.
Qualidade dos dados: É garantido aos titulares que seus dados sejam exatos, claros, relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. **Transparência:** É garantido aos titulares o direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.
Segurança: Devem ser utilizadas medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.
Prevenção: Devem ser adotadas medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
Não discriminação: Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.
Responsabilização e prestação de contas: Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (F. Mattos, 2018)

3.12 A segurança da informação em MPEs

3.12.1 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,) essas empresas são classificadas de acordo com sua receita bruta anual, segundo o (SEBRAE, 2014b) este termo pode ser empregado a pequenos negócios que são divididos nas seguintes categorias "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." As MPES constituem-se de qualquer tipo de organização legalmente formalizada que possui um potencial econômico de movimentação de emprego que se adequam a estas categorias legalmente declarada na receita. Outra forma de classificar uma MPE é através da sua ocupação, como demostrado na tabela a seguir.

Figura 05. Classificação de empresas conforme a ocupação.

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

Fonte: SEBRAE, 2014

Em sequência é necessário caracterizar essas MPEs, e 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 ainda segue demonstrando as dimensões que esse setor possui, dos quais as MPEs representam no contexto de serviços e comércios cerca de 98% 99% respectivamente do total de empresas formalizadas, além de representar aproximadamente 44% de empregos formais e 70% de empregos gerais. Com esse levantamento fica claro 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) os primeiros 2 anos de vida.

Aprofundando essa análise de características, é também possível discutir, as principais características que se encontram na estrutura de gestão de uma MPE, segundo a tabela 10 a seguir que descreve suas principais características.

Tabela 07. Características de estrutura da MPE.

Características Organizacionais	Características de tomada de decisão	Características Individuais
-Pobreza de recursos;	-Tomada de	-Onipotência do

-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.	decisão intuitiva; -Horizonte temporal de curto prazo; -Inexistência de dados quantitativos; -Alto grau de autonomia decisória; -Racionalidade econômica, política e familiar.	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.

Fonte: CAMPONAR 2004 apud LEONE 1999, adaptado pelo autor

Depois de visualizarmos esses aspectos, 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.

3.12.2 Como é tratada

Quando é o assunto é a segurança da informação no contexto de MPEs os recursos para pesquisa são escassos, visto que micro 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 alvos de roubo, interceptação, alteração ou simplesmente se perder na rede , contexto no qual contribui para a diminuição da confiabilidade do sistema de informação. Outro aspecto muito negligenciado é a discriminação sobre a estrutura que asseguram a informação, e começa no pensar de 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

se aprofunda tanto na adoção de ferramentas no contexto software, hardware, mas também no contexto estratégico de gestão de recursos físicos e humanos, 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 quando a segurança da informação é tratada e que estão inseridas no contexto 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 impedem que a MPEs satisfaçam essas necessidades que a *ISMS* impõe.

Tratando agora do contexto de gestão de uma MPE sobre como é tratado em dimensões estratégicas e organizacionais as implicações de *ISMS,* de acordo com THONG (2001), as MPEs não costuma 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, MPEs possuem uma tendência de fazer planejamentos de curto prazo, que são menos burocráticos, menos complexos e possui resultados mais rápidos porém tendem a não ser tão duradouros. Ainda dentro da questão da estrutura de gestão a falta de recursos é discorrido por Thong (2001) como sendo uma das problemáticas mais importantes quando se é pensando em implementar uma estrutura de segurança da informação, facilmente é encontrado argumentos de que a organização não é grande o suficiente ou não possui recursos suficientes para esse tipo de estrutura, esta é uma condição que está intimamente ligada a condição de MPE em que a organização está inserida, pois para ser uma MPE ela deve estar dentro desta condição, já que as mesmas são conhecidas como pobres de recursos. Também é discutido por (THONG 2001 apud GALÊS; WHITE 1981) sobre recursos de tempo que são tratados de maneira mais restritas em pequenas empresas, nos quais os colaboradores tendem a lidar com quantidades de responsabilidades maiores devido ao número limitado de colaboradores. Esse argumento é confirmado quando eles 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 é que caso aconteça a

implementação da ISMS em uma MPE ela 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.

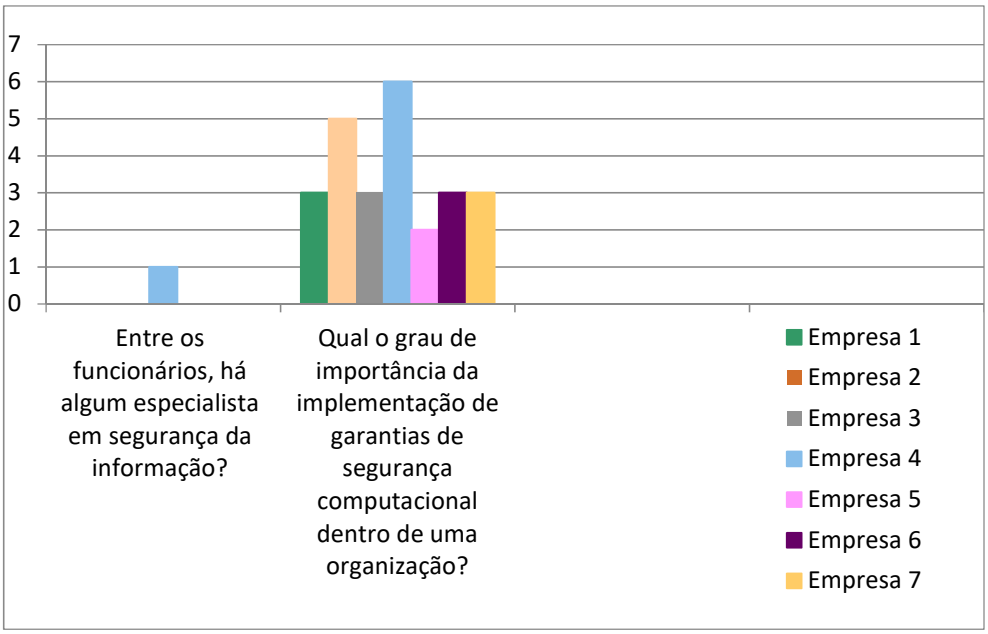
4 LEVANTAMENTO DE DADOS

Com base em uma pesquisa regional em Barueri feita para entender o problema e os mecanismos de segurança, sobretudo o conhecimento do usuário sobre ferramentas ou requisitos, normas e estruturas de governança e qual a sua capacitação sobre tal nas empresas da região, para nos dar a 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 de Barueri e identificar uma possível solução para tal.

O levantamento foi feito através de uma pesquisa com questões relevantes ao tema, dos quais seria 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 adquiridos através de uma visita as empresas e coletadas através de uma pesquisa com algumas perguntas que seguem no ANEXO 01 os resultados desta coleta estão apresentados nos seguintes gráficos.

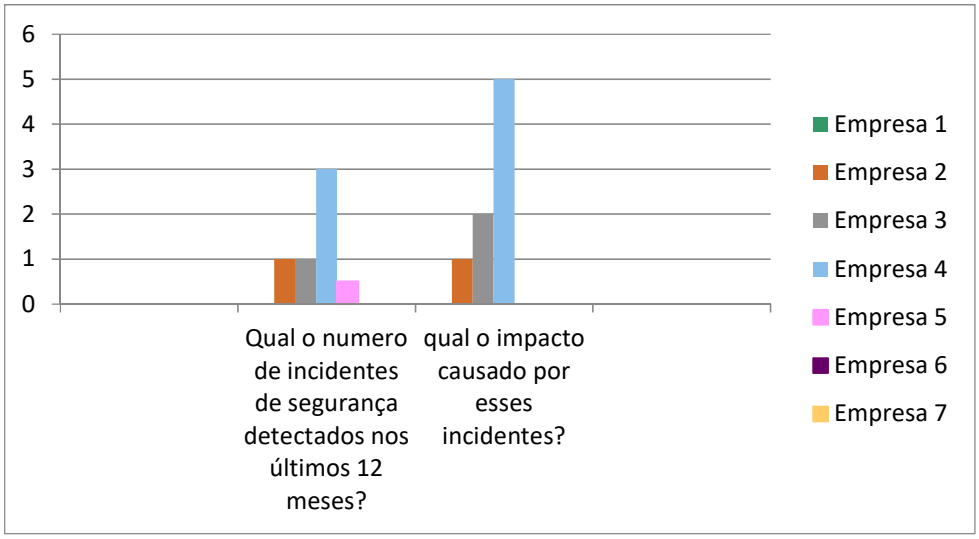
Gráfico 01.



Fonte: Realizada pelo autor

Conforme o gráfico 01 demonstra a questão que ressalta a dúvida sobre a existência de funcionários especialista em segurança da informação, com base no que foi respondido, entre as empresas que foram abordadas nenhuma tinha um especialista formalmente contratado 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.

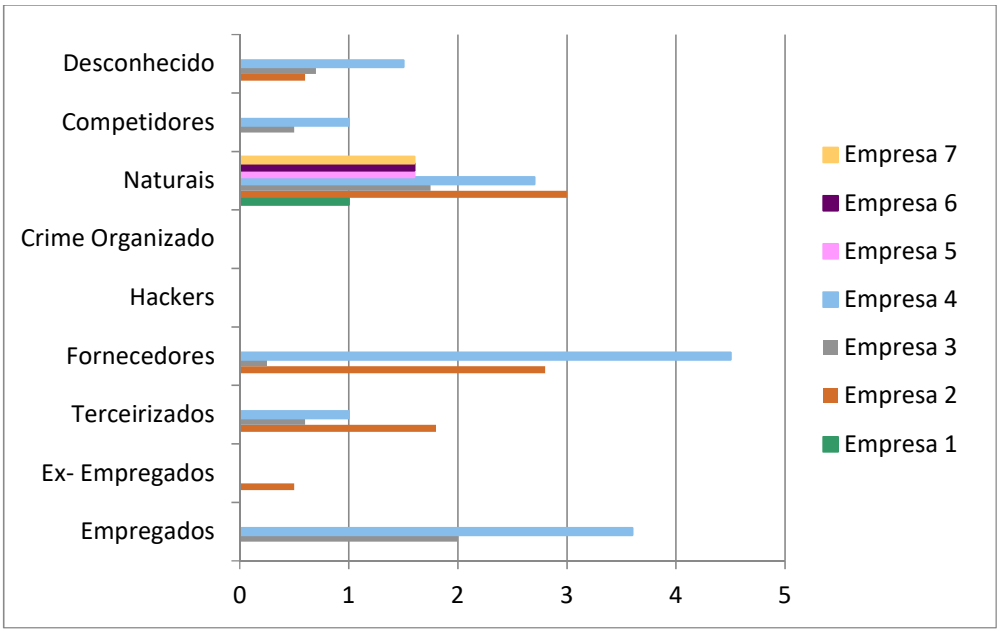
Gráfico 02.



Fonte: Realizada pelo autor

O gráfico 02 indica o número de incidentes ocorridos em um período de 12 meses não foi considerado alto com uma média de 1,5 anual, sendo assim o impacto causado pelos mesmos é diretamente proporcional aos incidentes acusados.

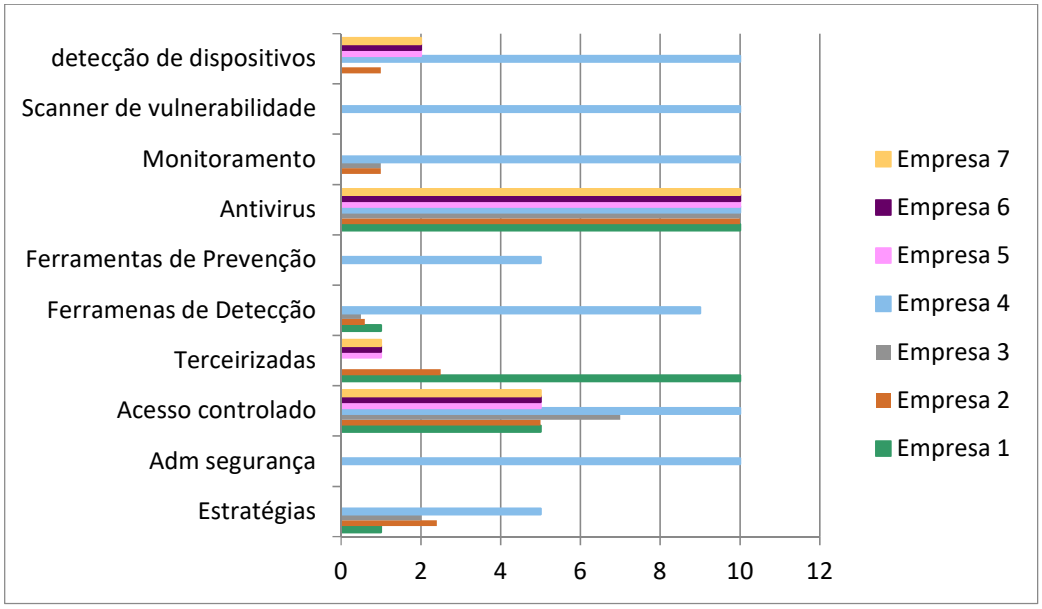
Gráfico 03.



Fonte: Realizada pelo autor

O gráfico 03 acusa as causas dos incidentes relatados nos últimos 12 meses e foi demonstrado que a estimativa de causas dos incidentes em sua grande maioria foram naturais ou através de empresas terceiras.

Gráfico 04.

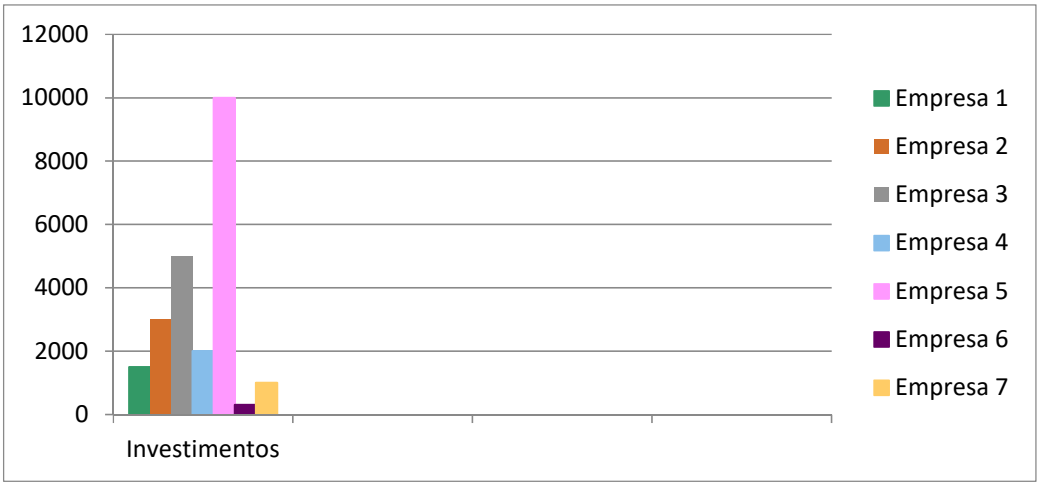


Fonte: Realizada pelo autor

Sobre os mecanismos de segurança utilizados foi detectado algumas variantes comuns entre as empresas sendo que pode-se notar que os mecanismos mais utilizados são os mais

genéricos, e os mais citados, enquanto os mais característico de ambientes de segurança suas variantes no gráfico foram menores.

Gráfico 05.



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 uma conversa aberta sobre as dificuldades que a empresa possuía em relação ao tema, quando fora discutido que questões de perda de dados, falta de backup, quedas de energia, e até roubo são requisitos que entram dentro do 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 em questões falta de experiência de colaboradores e que os mesmos estejam 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.

Baseados 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, constatou-se que há grandes estratégias de segurança, 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 as 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 impor tais práticas, foi o que aconteceu na empresa 4.

No transcorrer da pesquisa também foi notado que nas empresas menores, os entrevistados acreditavam que a segurança era importante e sabiam da existência das normas e padrões de segurança da informação, porém, admitiram ser um conhecimento ralo e não as tinham implantadas em sua organização, assim sendo foi lançado a pergunta do porquê tais normas não são praticadas, e com base nas respostas foi feito uma média de que cerca de 6,8% das empresas entrevistas acreditavam que o orçamento de segurança é muito alto para o porte da empresa e 42% admitiu ser por falta de conhecimento na área e 70% por estarem sobrecarregados e não terem tempo, isso se dá a um fato limitante por não haver uma pessoa especifica e qualificada para tratar do assunto, em contrapartida as duas outras maiores empresas visitadas empresa 4 e 5 alegaram que a criação da estratégia de segurança é satisfatória e um aspecto básico para a estrutura da empresa.

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

Esta é a problemática, motivação e justificativa maior do trabalho, 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 que as mesmas se encaixem 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.

5 RESULTADOS

5.1 Proposta do novo modelo para MPEs

Dentro os dois modelos estudados (ITIL e ISO 27001) com todas as suas práticas, processos e políticas que foram consideradas, foram evidenciadas as necessidades que em suma devem ser praticadas para cobrir todas as necessidades e normas que são necessárias para a organização em um âmbito geral. 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 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 uma micro 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 todas seus princípios e requisitos tem como característica principal orientar o gerenciamento da TI e seu 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 as 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 uma micro 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 ISO

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 governança 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:

Tabela 08. Variáveis consideradas referentes a estrutura MPE

Variáveis	Comportamento
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 09. Constantes consideradas na estrutura MPE

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, 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 política 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.

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. Após todo o estudo e levantamento de informações foi definido quais os requisitos que compõe o fluxo *PDCA* são relevantes dentro do contexto da organização de uma MPE.

A proposta desse novo modelo engloba os seguintes fatores:

- Contexto organizacional:

O contexto organizacional é onde se atribui a estrutura das boas práticas que englobam a segurança do patrimonial e informacional da empresa, partindo disso, é importante definir soluções técnicas e de processos para garantir a proteção do seu negócio, para isso, é importante uma equipe que defina todos os processos de segurança para tratar aspectos organizacionais e estratégicos.

Uma gestão eficaz, tem como principal objetivo, 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. fazer com que as decisões e ações que englobam a segurança da informação estejam alinhadas aos objetivos e estratégias do negócio da organização. Por isso em qualquer ocasião ou circunstancias quando já se tem métricas e processos definidos, basta segui-las para obter o resultado esperado, é indicando que, qualquer ação de segurança exige alinhamento com o negócio da empresa.

Dentro da gestão existe a elaboração e manutenção das politicas de gestão de segurança da informação, organizações que pretendem gerenciar a segurança da informação em seus negócios precisam fazê-lo de forma sistêmica. A segurança da informação precisa fazer parte das atividades de todos na organização. Para isso, é necessário um documento que promova e fomente a ideia. Uma Política de Segurança da Informação bem definida é uma das mais importantes medidas a serem tomadas, já que será a base de princípios que seguidos pela gestão, essa política de segurança deve definir o tratamento que deve ser dado às informações armazenadas, processadas ou transmitidas no ambiente convencional ou no ambiente de tecnologia.

É importante que esse documento englobe declarações relativas a:

a) definição da segurança da informação, suas metas globais, escopo e importância da segurança da informação como um mecanismo que habilita o compartilhamento da informação.

b) declaração do comprometimento da direção, apoiando as metas e princípios da segurança da informação, alinhadas ao negócio.

c) estrutura para estabelecer os objetivos de controle e os controles, incluindo uma estrutura de gerenciamento de risco.

d) definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo registro dos incidentes de segurança da informação.

Outro princípio importante que dever ser ressaltado é a a gestão de continuidade do

negócio que tem como objetivo, impedir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar que a sua retomada ocorra em tempo hábil. Para isso, planos de continuidade do negócio, incluindo controles para identificar e reduzir riscos, devem ser desenvolvidos e implementados, visando assegurar que as operações essenciais sejam rapidamente recuperadas, é uma forma de mitigar risco e também de tornar incidentes administráveis de maneira que possam contorná-los de forma rápida e eficiente.

A) Contexto de liderança :

Exercer a função de liderança em um determinado grupo está diretamente ligado ao poder social, e poder social é a capacidade de um indivíduo influenciar positivamente as pessoas para uma determinada direção ou até mesmo mudar a direção da ação. As perspectivas de uma boa liderança estão em enxergar as possibilidades para mudar as situações onde os outros só veem dificuldades. As empresas estão sofrendo ataques constantemente, e quando chega o momento de estruturar um plano de ação, muito regularmente o fator humano, a gestão do time é deixado de lado. Os gestores e lideres tem que reconhecer que alguns métodos podem ser soluções para grandes problemas, É preciso haver uma ação coordenada, ampla, e em vários níveis, integrar a equipe, da direção da organização, a todas as áreas. E isso requer uma mudança de comportamento, a visão de segurança tem que deixar de ser somente do TI. Tem que pertencer a toda a organização. É necessário que todas as as áreas e as pessoas trabalhem cientes de seu papel, das normas de segurança e em um nível de cooperação muito maior, e a liderança precisa estar envolvida diretamente. É importante criar um responsável pela manutenção da moral e diretrizes de segurança e também de passar essas informações a todo os times, essa pessoa também cuidará especificamente de uma crise cibernética, um grupo que lide somente com ameaças de alto nível.

- Contexto de suporte:

A) ANÁLISE, AVALIAÇÃO E TRATAMENTO DE RISCO

O processo de avaliar riscos precisa ser um processo contínuo de forma a cobrir todo o

ambiente organizacional. Convém também, que a análise/avaliação de riscos de segurança da informação tenha seu escopo definido e inclua os relacionamentos com as análises de outras áreas, se necessário, antes de considerar o tratamento de um risco, a organização deve definir os critérios para determinar se os riscos podem ser ou não aceitos. O risco é aceito se ele é baixo ou se seu custo do tratamento não é economicamente viável para a organização. Para cada um dos riscos identificados, uma decisão sobre o tratamento do risco precisa ser tomada e por fim uma análise e avaliação dos projetos e gestão desses incidentes precisa ser feita, com foco no que foi realizado, e suas metas alcançadas e as dificuldades e o que precisa ser ajustado.

B) GESTÃO DE ATIVOS

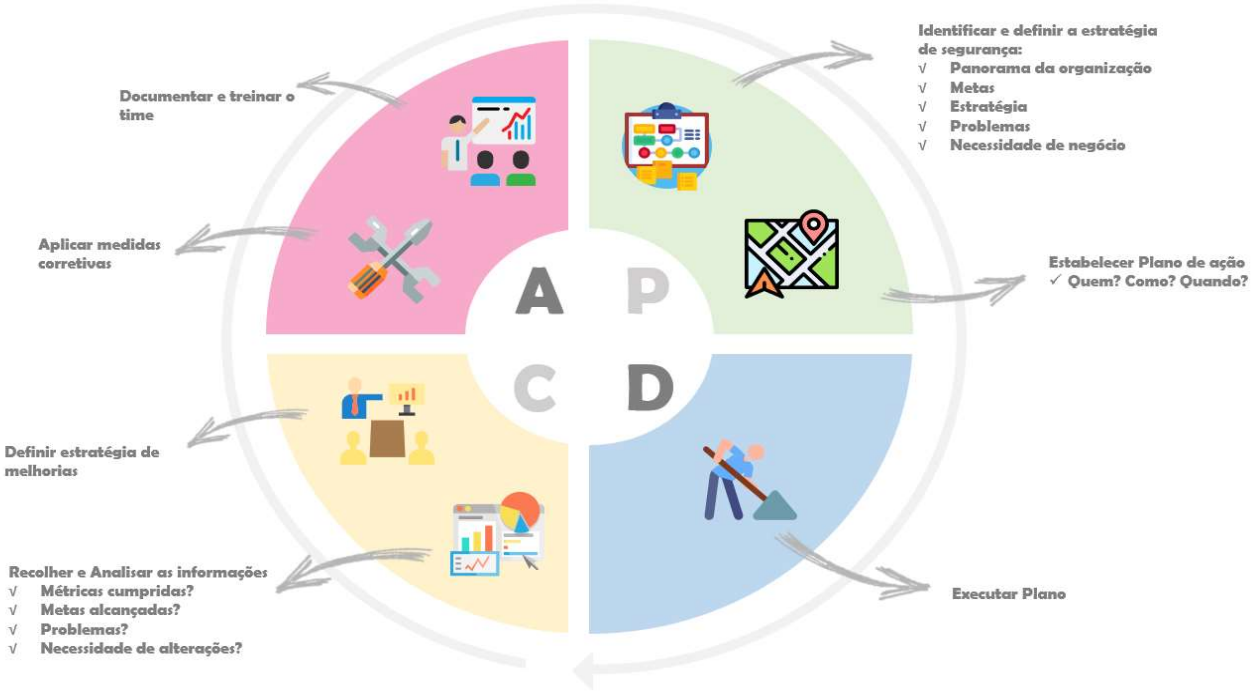
A informatização é hoje peça fundamental no dia-a-dia profissional. Por que ela é necessária para a constante utilização dos ativos de uma empresa. Ativo de informação é qualquer elemento de valor para a empresa que manipula, processa, armazena, transporta ou descarta a informação, incluindo a informação em si. Segundo a norma ABNT (2005), a gestão de ativos tem como principal meta, a proteção adequada dos ativos da organização e que estes sejam inventariados e tenham um proprietário responsável.

Para alcançar e manter esta proteção a gestão deve tratar dos seguintes aspectos:

- Inventário dos ativos
- Proprietário dos ativos
- Forma correta e aceitável de utilização dos ativos
- Comunicação entre as partes relacionadas
- Documentação da informação

Após definir todos os processos de gestão acima, esse processo vai ser a base de todo o ciclo PDCA, que terá um novo objetivo, neste novo modelo o ciclo ele será focado no contexto de segurança, e incorporado dentro da organização.

Figura 06. Modelo de ciclo de vida baseado em *PDCA*



Fonte: Realizada pelo autor

Dentro do ciclo é importante englobarmos todos os serviços que englobam as métricas da ITIL, Serviço de Estratégia

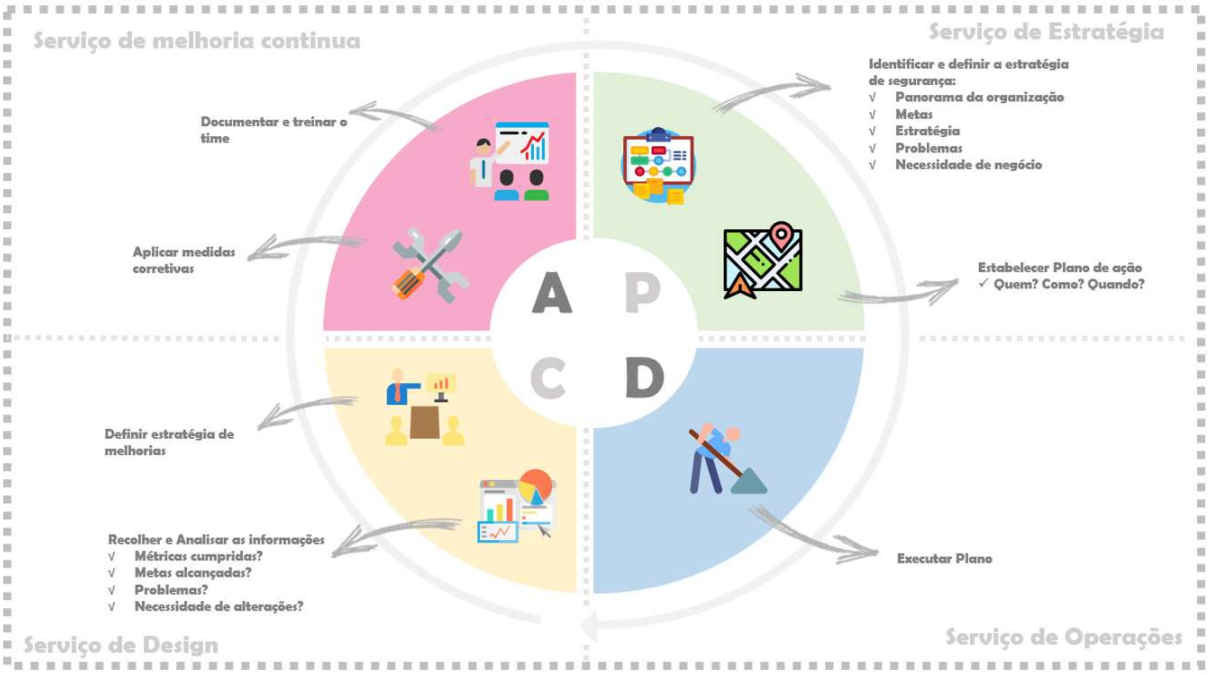
C) Serviço de Design

D) Serviço de Operações

E) Serviço de Melhoria continua

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

Figura 07. Modelo de passos do processo baseado em PDCA e ciclo de vida ITIL.



Fonte: Realizado pelo autor

Existe 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 são mais uteis no cotidiano de uma MPE.

Como ponto inicial podemos observar como demonstrado acima, o ciclo de vida PDCA que podemos encontrar tanto nos processos da ITIL como no da ISO 27001 foi mantido com alguns conceitos que ajudam na formalização dos processos que uma empresa independente de seu porte deve possuir, na etapa de planejamento é o momento no qual deve ser definido tudo o que a empresa representa. Definir em que escopo ela está inserida, quais são seus objetivos e como esses objetivos serão alcançados, é nesta etapa em que um planejamento estratégico e processual deve ser definido e alinhado com as necessidades e contexto da organização, além de deixar claro o papel de cada líder dentro desse processo. Esse é um comportamento que foi considerado 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 considerada completamente 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 processual, 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.

Subsequente a isso no ciclo existe o processo de fazer, que engloba as características ITIL de design de serviço e serviço de operações, que na norma também se trata de boas práticas no ponto de vista operacional. A partir disto é necessário manter os requisitos extraídos na etapa de planejamento e agir de conforme foi objetivado, manter padrões de processos e métricas que ajudem a manter a consistência operacional e o alcance de objetivos e metas de forma sólida. Todos os processos que foram julgados importantes para uma empresa principalmente quando a mesma possui metas a atingir e uma qualidade de processos e produto a atender, e através do vasto referencial teórico realizado em boas práticas é claro de que processos formalizados e consistentes implicam diretamente na consistência do produto ou serviço bem como sua qualidade, no qual entregas são cumpridas e qualidade são atendidas ambas variantes que são vistas como vantagem competitiva em um nicho pequeno em que uma MPE 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, esta etapa foi incluída, pois foi julgado importante entender e enxergar quais os obstáculos enfrentados para atingir o objetivo que fora acertado no processo de planejamento, e ter a oportunidade de visualizar os problemas ocorridos durante uma fase do processo é possível avançar para a fase de Agir, que é implementar ações corretivas que melhorem o processo e sua qualidade, esta é uma fase na qual introduz a rotatividade do ciclo, fazendo com que a gestão da organização 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 continua. Processo no qual foi julgado imprescindível para uma micro pequena empresa, onde as mesmas se diferenciam de suas competidoras por uma variante muito pequena ou inexistente, e que este pode se tornar sua vantagem competitiva, pois é um processo que as ajudam a acompanhar as tendências de mercado e as deixa capaz de atualizar-se e manter-se 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 é uma importante variante que poucas MPEs conhecem ou exploram, pensando nisso foi elaborado diretrizes de segurança baseadas em todas as normas e processos que vimos no decorrer desse trabalho, esses processos não somente englobam a segurança de ativos da informação através de suas boas práticas resulta em processos bem definidos que derivam na melhor utilização de recursos físicos, lógicos e humanos, reduz custos, evita erros, fraudes, diminui consequências de acidentes maliciosos ou naturais, protege o ativo informacional da empresa e melhora a qualidade do serviço ou produto.

6 CONCLUSÕES

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.

7 Anexo I

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?

Gestão de ativos

10. Existe um inventário de todos os ativos importantes?
11. Todos os ativos e informações possuem um proprietário (pessoa ou organismo que tenha uma responsabilidade autorizada para controlar a produção, o desenvolvimento, a manutenção, o uso e a segurança dos ativos)?
12. Existem regras para o uso da Internet?
13. Existem regras para o uso do e-mail?

14. Os funcionários estão adequadamente instruídos sobre as suas responsabilidades e papéis pela segurança da informação?
15. Houve treinamento sobre a política de segurança da informação para os funcionários?
16. Existe um processo formal para a devolução de todos os equipamentos, documentos corporativos, softwares, dispositivos de computação móvel, cartões de crédito, cartões de acesso, manuais e informações armazenadas em mídia eletrônica entregues a pessoa que está saindo?
17. Existe um processo de documentar as atividades que este funcionário, fornecedor ou terceiro, antes que ele encerre suas atividades na empresa?
18. Os direitos de acesso do funcionário são retirados após o encerramento de suas atividades?

Incidentes

19. Qual o número de incidentes de segurança detectados nos últimos 12 meses?
    - 0 ou nenhum
    - 1 a 9
    - 10 a 40
    - 50 ou mais
    - Não sei
20. 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
21. 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

22. Existe algum tipo de controle de gastos direcionados para projetos desse contexto?
23. Qual o orçamento anual alocado para projetos de implementação, melhoria ou controle da segurança da informação?
    - pequeno
    - médio
    - inexistente
    - não sei

Mecanismos

24. 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
25. 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

26. 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
27. 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
28. Você conhece as normas de padronização de garantias de segurança da informação ISO 27000/27001 ou 27002?
    - Sim
    - Não
    - Não sei
29. Sua organização possui certificação ISO 27000/27001 ou 27002?
    - Sim
    - Não
    - Não sei
30. Você conhece a infraestrutura ITIL?
    - Sim
    - Não
31. Sua organização possui implementado alguns tipos de processos que estão relacionados aos processos ITIL? De seu conhecimento?

- Sim
- Não
- Não sei

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

Dificuldades

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

Satisfação

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

7 REFERÊNCIAS

ABNT, Associação Brasileira de Normas Técnicas. **NBR14724-Informação e documentação-trabalhos acadêmicos**. 3. ed. 11 p. Rio de Janeiro : ABNT. 2011. ISBN 978-85-07-02680-8. Disponível em: <http://pt.slideshare.net/LazinhaSantos/nbr-14724-2011-nova-norma-da-abnt-para-trabalhos-acadmicos-11337543>. Acesso em: 10/12/2018.

IBGE, **INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA**. Normas de apresentação tabular. Rio de Janeiro, 1993. 60 p. Disponível em: <http://biblioteca.ibge.gov.br/visualizacao/monografias/GEBIS - RJ/normastabular.pdf>. Acesso em: 10/12/2018.

BEAL, Adriana. **Conceitos e Princípios Básicos da Informação. Segurança da Informação**. São Paulo: Atlas, 2005.

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

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

MATTOS, F, 2018,SEBRAE, Disponivel em: <http://www.sebrae.com.br/sites/PortalSebrae/ufs/mt/noticias/micro-e-pequenas-empresas-geram-27-do-pib-do-brasil,ad0fc70646467410VgnVCM2000003c74010aRCRD>. Acesso em: 20/12/2018

CERT, **Estatísticas dos Incidentes Reportados ao CERT.br**, Disponível em:< www.cert.br/stats/incidentes/>. Acesso em: 20/12/2018.

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**, 04/06/2018 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: 11/06/2018.

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: 20/05/2018.

E. H. DINIZ, T. A. Gestão de Segurança em Internet Baking: Estudo de casos Brasileiros.

17/12/2018 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

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: 11/02/2019.

NFS, C. C. NSF's Cyberinfrastructure vision of 21st century discovery v. 7.1, 16/12/2018 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: 11/06/2018.

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 22/02/2019 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: 11/01/2018.

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

TECHEXCEL. ITIL Implementation and Process Guide. 04/06/2018 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.