Universidade Tecnológica Federal do Paraná (UTFPR)
Pró-Reitoria de Pesquisa e Pós-Graduação
Diretoria de Pesquisa e Pós-Graduação Campus Curitiba
Curso de Especialização em Gestão da Tecnologia da Informação e Comunicação.

Eli Junior Lombardi

Metodologia para criação de uma Política de Segurança da Informação para uma Empresa Pública.

Monografia de Especialização

Curitiba

2014

Eli Junior Lombardi

Metodologia para criação de uma Política de Segurança da Informação para uma Empresa Pública.

Monografia de conclusão do Curso de Especialização em Gestão da Tecnologia da Informação e Comunicação da Universidade Tecnológica Federal do Paraná (UTFPR).

Orientador: Prof. Christian Carlos Souza Mendes

Curitiba

2014

RESUMO

Este trabalho se propõe a estudar a atual situação da política de segurança da informação em uma instituição pública do governo estadual e a propor uma forma de implementação de uma política, desenvolvida com base na ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação, na ABNT NBR ISSO/IEC 27004 - Tecnologia da informação – Técnicas de segurança – Gestão da segurança da informação-Medição, recomendações do PMBOK e ITIL e na bibliografia disponível sobre o tema.

Palavras-chave: Segurança da Informação. Implementação. Metodologia.

ABSTRACT

The present paper intend to examine the current state of an information security policy at a state public government institution and propose a way to implement a policy, developed based on the ISO / IEC 27002 - Information technology - Security techniques - Code of practice for information security controls**,** on the ISO/IEC 27004 - Information technology – Security techniques – Information security measurement management, PMBOK and ITIL recommendations, and the available literature on the subject.

Keywords: Security Policy. Implementation. Methodology.

SUMÁRIO

1 Introdução

A evolução tecnológica ocorrida nos últimos 50 anos e caminhando cada vez mais a passos largos, trouxe uma expressiva valorização de um importante ativo na vida das empresas e organismos governamentais: a informação. A informação influencia cada vez mais na geração de novos produtos, idéias, quebra de paradigmas, evolução tecnológica. A construção de novos conhecimentos é baseada na grande quantidade de informação armazenada anteriormente, num ciclo sucessivo e exponencial. O que antes era palpável transformou-se em algo intangível e de grande valor, que é a informação nas suas diversas formas de acesso e armazenamento. Cada vez mais a informação influencia na tomada de decisão e na definição do rumo que o negócio deve tomar, deixando de ser somente a análise e o controle da atividade fim de uma instituição ou empresa e passando ela mesma a ser parte da atividade.

Necessário se faz, portanto, que se preserve esta informação toda com a importância que ela exerce dentro da vida de uma instituição pública ou privada, de modo a garantir sua privacidade, sua integridade, seu descarte seguro e sua disponibilidade às pessoas que a utilizarão como tomada de decisão ou na própria execução de sua atividade. Surge a necessidade da segurança da informação.

Segurança da informação, segundo Sêmola, não é apenas a instalação de softwares de firewall, criptografia, gestão de acessos e produtos relacionados à tecnologia da informação. Os processos de segurança devem permear todas as atividades da empresa, formando um conjunto de regras, procedimentos e ferramentas que em conjunto irão dar o nível de segurança desejado e garantir a sua continuidade [Sêmola, 2013].

Este trabalho se propõe a estabelecer uma Política de Segurança de Informação que possa permear toda uma Organização Pública Estadual com o objetivo de garantir um padrão de Segurança, sua implementação e continuidade.

Segundo o Gartner, “Política de segurança da Informação refere-se à coleção de regras escritas encapsulando requisitos para o comportamento organizacional que sejam significativos o suficiente para ser formalizada” [Mcmillan, 2012]. Ou: “Área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou a sua indisponibilidade”. Uma boa política não traz garantias de um programa de segurança eficaz, mas uma má política geralmente leva a um programa medíocre e imaturo. A boa política é um exercício de comunicação de risco de preferência por pessoas que tenham uma sólida experiência na área, que tenham habilidades para fazem uso dos melhores processos e técnicas comprovadas para o planejamento e elaboração de política, o que pode fazer grande diferença na forma como ela será eficaz na redução do risco [Heiser 2012].

A política deve ser escrita para uma compreensão clara do resultado esperado. O objetivo é influenciar comportamentos. Em alguns casos, um objetivo adicional pode ser o de fornecer um mecanismo legal que torna mais fácil para disciplinar ou demitir funcionários com base em comportamentos que não estejam de acordo com a política. Porém uma política que enumera de forma exaustiva todos os atos possíveis que podem

resultar em demissão ou punição de um empregado pode ser um dispositivo legal útil, mas encoraja o cinismo, o que é contraproducente. [Heiser 2012].

Uma boa política deve conter um conjunto de regras executáveis, não longa demais e não omissa demais. A comunicação clara das etapas de implantação deve garantir que os comportamentos esperados serão seguidos por serem bons para todos e não temidos.

Portanto queremos tratar na instituição pública A, a segurança da informação como um processo de gestão e não como solução tecnológica apenas. Queremos o envolvimento das pessoas desde suas pequenas atitudes cotidianas até a participação na melhoria contínua dos processos de segurança. A idéia é que os cadeados devem ser colocados antes de arrombada cada porta.

1.1 Tema

Este documento aborda a segurança da informação, a elaboração de uma política de segurança e a sua implantação na organização.

Segundo a ISO 27002, Segurança da Informação é: *"Proteção da Informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar os riscos, maximizar os retornos sobre os investimentos e oportunidades de negócio"* [ABNT NBR ISO 27002:2005].

Uma informação é tida como segura quando atende os três requisitos básicos de segurança da informação: Confidencialidade, Integridade e Disponibilidade. Acrescentamos mais dois requisitos que são: Autenticidade e Legalidade.

- **CONFIDENCIALIDADE:** Pressupõe que a Informação deverá estar disponível apenas para as pessoas devidamente autorizadas;
- **INTEGRIDADE:** Garante que a Informação não será destruída ou corrompida;
- **DISPONIBLIDADE:** As Informações deverão estar disponíveis sempre que forem necessárias.
- **AUTENTICIDADE:** Garantia de que as entidades identificadas em um processo de comunicação como remetentes ou autores sejam exatamente o que dizem ser;
- **LEGALIDADE:** Garante que as informações estão de acordo com o formato definido em lei.

Conforme Moreira a política de segurança é um conjunto de normas e diretrizes destinadas à proteção dos ativos da organização, sendo caracterizada pela tentativa de manter a confidencialidade, a integridade e a disponibilidade da mesma, independentemente de onde ela esteja. A Política de Segurança passa a ter uma importante função, visando à proteção dos ativos para que os negócios não parem e o ambiente fique seguro. [Moreira 2001]

A política é relevante em relação ao que se deve proteger e porque se deve proteger; deve definir as responsabilidades pela proteção; e servir de base para interpretar cenários e resolver problemas que venham a surgir no futuro.

A parte central da política é, naturalmente, as declarações e seus artigos. Estes devem ser de alto nível. Os artigos se articulam a partir de requisitos de uma forma que a liderança e as equipes da unidade de negócios possam os entender, os executar e os defender facilmente. Não existe um número mágico de declarações ou artigos dentro de uma política. Como as declarações são de alto nível, normalmente há um número relativamente baixo de artigos, sendo a maior parte dos detalhes implementados através de outros documentos e procedimentos operacionais. Ou seja, a política não esgota a informação sobre segurança, mas sim define um modelo a ser seguido e detalhado por documentos de apoio.

Na fase de implementação a organização deve criar uma estrutura de gerenciamento para controlar a transição dos serviços e políticas para o ambiente de produção. Para atingir esse objetivo é necessário que a direção e os gestores aprovem a política de segurança da informação, aloquem os recursos necessários, coordenem e conduzam a implantação da segurança da informação em toda a organização.

A cadeia de aprovação é fundamental para o sucesso da implementação da política, devendo ser documentada. Se possível, é aconselhável a formação de um grupo de gestão sênior para a avaliação preliminar, antes da aprovação final pelo diretor ou por uma função equivalente. Uma política que leva a aprovação apenas do diretor, pode ser disputada por outros líderes técnicos dentro da empresa, isto se a aprovação não foi mutuamente acordada.

1.2 Objetivos

Este trabalho tem como objetivos a redação de uma política de segurança da informação, com base na ISSO 27002, e um projeto de implementação que se utilizará da metodologia de gerenciamento de projetos recomendada pelo PMBOK, com gestão de processos baseada no modelo PDCA, e medições com base na ISO 27004, explicadas no item 3.

A redação da política de segurança da informação foi realizada com base nas recomendações da ISO 27002, que serve de referência para todos os funcionários da instituição A, prestadores de serviço, fornecedores, estagiários e empresas terceirizadas que prestam serviço de TI, compreendendo hospedagem, armazenamento, desenvolvimento e outros.

Este trabalho não se propõe a definir ou redefinir termos técnicos ligados a esta área do conhecimento, mas se atem a aspectos práticos que garantem o sucesso da implantação e da manutenção do plano de segurança.

1.3 Justificativa

A elaboração de uma Política de Segurança da Informação, bem como sua posterior implementação e divulgação é justificado pela situação atual da instituição.

A instituição A, em questão, entrou no mundo da informática, de forma empírica, como tantas outras instituições públicas e privadas. A informática, inicialmente, era utilizada como apoio à atividade fim, relegada a atividade de bastidores que servia para agilizar os processamentos antes feitos em papel, calculadoras, máquinas de escrever. Os processos foram sendo informatizados pelas mesmas pessoas responsáveis pelas áreas fim, sem metodologia, sem a formalidade e métodos hoje existentes. Os processos de segurança se limitavam a sistemas anti-virus e regras de uso de equipamentos escritas em avisos afixados nas portas das salas de computadores e iniciativas isoladas sem padrão. Os cuidados com as informações armazenadas eram muito mais intuitivas do que baseados em normas e boas práticas.

Esta situação perdurou por muitos anos, até que os vazamentos de informações confidenciais, os cybers ataques (ataques, represálias ou intrusão ilícita num computador ou numa rede), a proliferação de Malwares (software malicioso destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações), as indisponibilidades constantes e o surgimento de profissionais especializados em roubar as informações das organizações, conhecidos como crackers, obrigou as empresas a seguirem as práticas adotadas pelo mercado para protegerem suas informações, sob risco de comprometer todo o negócio da empresa, a ter que parar sua atividade fim por perda ou vazamento de informações. A instituição A, aqui estudada, seguiu este caminho e, como é comum no serviço público, pretende iniciar um processo através da implementação da Política de segurança da informação com algum atraso, mas com a vantagem de já poder implementá-la de maneira científica, controlada e de acordo com normas e orientação profissional.

Os dados da Empresa A estão armazenados, na maior parte, em um datacenter pertencente a outra empresa, também pública, que presta serviços de T.I. a este e vários outros órgãos. Esta tem sua própria política de segurança já implementada e consolidada, o que garante boa parte da segurança necessária aos dados da instituição A. É necessário que a própria instituição A tenha sua política de segurança de modo que tanto sua informação localizada, armazenada em sua sede, quanto a informação armazenada em terceiros, sigam as mesmas regras de segurança, com base em um documento único. Esta política própria somada à política da terceirizada atual e eventuais outros terceiros prestadores de serviço, garantirá um nível de segurança bem maior do que o atual sistema empírico baseado na experiência e construído de modo isolado e não integrado.

1.4 Metodologia

O processo de preparação do presente documento caracterizou-se pela análise de documentos, normas, artigos e pelas etapas descritas a seguir:

- Elaboração da Política de Segurança da Informação baseada na norma ABNT ISO/IEC 27002 – Código de Prática para a Gestão da Segurança da Informação, versão 2005.
- Utilização do modelo conhecido como “Plan-Do-Check-Act” (PDCA) e a abordagem da norma ABNT ISO/IEC 27001 para estruturar os processos necessários para a implementação da política de segurança na instituição A.
- Utilização de técnicas e processos para as fases de planejamento, de execução e de controle baseados na metodologia de gerenciamentos de projetos do PMI (Project Management Institute); definidos no PMBOK, versão 4th Edition – Português.
- Utilização do ciclo de vida de serviço definido nas recomendações e boas práticas da ITIL (Information Technology Infrastructure Library), notadamente em relação ao estágio de transição de serviço. Essas diretrizes são úteis para definição e planejamento quanto à inserção da nova política e serviços correlatos no ambiente de produção da organização.
- Elaboração de diretrizes quanto a divulgação da Política de Segurança da Informação na instituição adotando como documento de referência o Plano de Divulgação de Segurança de Informação do DECEA (Departamento de Controle do Espaço Aéreo). Algumas práticas definidas neste documento foram adaptadas para a instituição A.
- Utilização da bibliografia e artigos técnicos disponíveis, notadamente o Gartner, http://www.gartner.com/ e o livro Sêmola, Marcos (2003) “Gestão da Segurança da Informação: uma visão executiva”. Estes foram utilizados em apoio às normas formais para uma descrição mais prática voltada ao ambiente operacional e a questões do dia-a-dia da instituição A.

O trabalho tem como principais produtos a Política de Segurança da Informação contida no anexo I e o planejamento para sua entrada em produção contida no item 4 (quatro). As demais seções descrevem as normas, os métodos utilizados, a situação atual da instituição e os resultados esperados após a implantação da política.

2 Normas – Regulamentações - Conceitos

A redação da Política de Segurança da Informação é baseada na ISO/IEC 27002.

A implantação desta política no ambiente de produção é baseada no ciclo PDCA e nas orientações da norma ISO/IEC 27001 que enfatiza o entendimento dos requisitos de segurança, a necessidade de estabelecer uma política de segurança com objetivos claros, a implementação e operação de controles para gerenciar riscos, monitoração de desempenho e melhoria contínua baseada em medições objetivas.

Em apoio às normas ISO/IEC 27001 e 27002 foram utilizados processos e técnicas definidas no PMBOK do PMI (Project Management Institute), tendo também como referência as boas práticas da ITIL (Information Technology Infrastructure Library).

Em relação à medição e indicadores de desempenho, também foi considerada a ISO/IEC 27004 – Gestão da Segurança de Informação – Medição.

A seguir algumas considerações sobre essas normas, boas práticas, conceitos e regulamentos.

2.1 A ISO 27002

A ISO (International Organization for Standardization) é a maior organização mundial para desenvolvimento e publicação de normas. Está sediada em Genebra, Suíça, fundada em 1946. É uma organização não governamental que faz uma ponte entre os setores privado e público. Mais de 160 países integram esta organização, o Brasil é representado na ISO pela ABNT(Associação Brasileira de Normas Técnicas). O Objetivo da ISO é desenvolver e promover normas que possam ser utilizadas por todos os países no mundo.

A ISO 27002, da ABNT, é um código de prática para a gestão da segurança da informação. Compõe centenas de regras e recomendações para a organização, aquisição, desenvolvimento, gestão da segurança da informação, bem como aborda os diferentes aspectos da segurança como a gestão de ativos, segurança física, segurança de recursos humanos, gestão de incidentes, continuidade de negócios e conformidade.

As principais seções da norma ISO 27002 são as seguintes:

- Introdução;
- Objetivo;
- Termos e definições;
- Estrutura da norma;
- Análise/avaliação e tratamento de riscos;
- Política de segurança da informação;
- Organizando a segurança da informação;
- Gestão de ativos;

- Segurança em recursos humanos;
- Segurança física e do ambiente;
- Gerenciamento das operações e comunicações;
- Controle de acessos;
- Aquisição, desenvolvimento e manutenção de sistemas de informação;
- Gestão de incidentes de segurança da informação;
- Gestão da continuidade do negócio;
- Conformidade.

A seção 5 da referida norma trata especificamente da política de segurança da informação, cujo objetivo é: “Prover orientação e apoio da direção para a segurança da informação de acordo cm os requisitos do negócio e com as leis e regulamentações pertinentes.” E continua… “Convém que a direção estabeleça uma clara orientação da política alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio de publicação e manutenção de uma política de segurança para toda a organização”.

Alguns dos aspectos mais relevantes da política de segurança da informação são descritos a seguir:

- Definir o que pode e não ser feito na organização;
- Definir o que é considerado inaceitável dentro da instituição;
- Definir direitos e deveres para as pessoas dentro e fora da instituição que lidam com seus recursos computacionais e informações neles contidos;
- Tudo que descumprir a política é considerado um incidente;
- Define penalidades para aqueles que descumprirem a política.

A norma também cita algumas diretrizes para implementação:

- Definição de Segurança da Informação, suas metas globais, escopo e importância;
- Deve conter uma declaração do comprometimento da Direção alinhado com os objetivos de negócio;
- Estabelece os objetivos de controle, os controles e a estrutura de Gerenciamento de Riscos;
- Breve explanação das políticas, princípios, normas e requisitos de Segurança da Informação;
- Define as responsabilidades gerais e específicas;
- Faz referências à documentação de apoio;
- Convém que a Política de SI seja comunicada através de toda organização para todos os usuários de forma que seja relevante, acessível e compreensível para o leitor;

- Se a Política de SI for divulgada fora da Organização, convém que sejam tomados cuidados para não se revelar informações sensíveis.

A ISO 27002 não é uma norma impositiva, ela faz recomendações de segurança baseada nas melhores práticas de segurança da informação, de forma a servir como referência para que a organização realize a sua implantação de acordo com sua conveniência e necessidade.

2.2 O modelo PDCA

Segundo a ISO/IEC 27001, a organização deve estabelecer, implementar, operar, monitorar, analisar criticamente e melhorar um sistema de gestão de segurança da informação (SGSI) dentro das atividades de negócio da instituição e dos riscos que ela enfrenta.

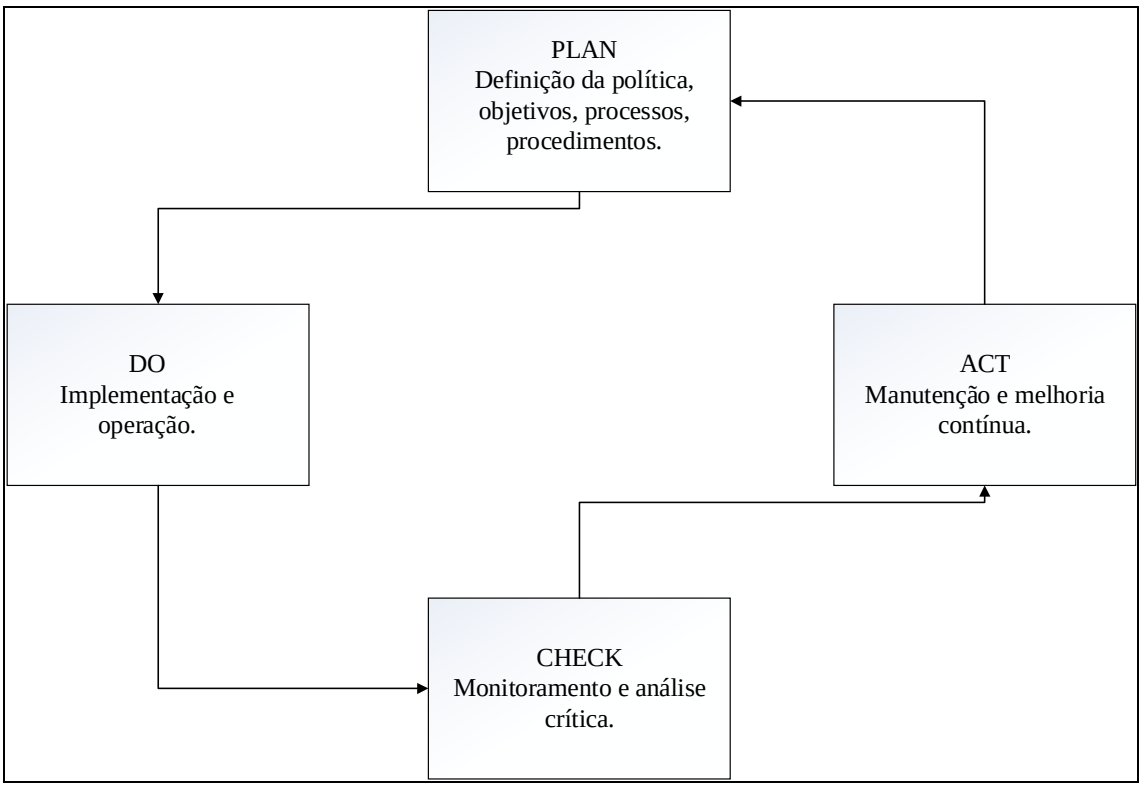

Figura 1. Modelo PDCA aplicado aos processos de segurança da informação

As etapas do modelo são descritas a seguir:

- Plan (Planejar) – estabelecer a política, objetivos, processos e procedimentos relevantes para a gestão de riscos e a melhoria da segurança visando os resultados esperados pela instituição.
- Do (Fazer) – implementar e operar a política, os controles, os processos e os procedimentos.

- Check (Checar) – avaliar e medir desempenho de um processo em relação à política, aos objetivos e a experiência prática, de forma a apresentar resultados para a análise crítica.
- Act (Agir) – executar as ações corretivas e preventivas com base na análise crítica e informações pertinentes, para alcançar a melhoria contínua do sistema de gestão de segurança da informação.

2.3 O PMBOK

Conforme descrito no item anterior a gestão da segurança da informação deve seguir uma abordagem de processo, adotando o modelo "Plan-Do-Check-Act" (PDCA) e visando a melhoria contínua. Porém, alguns processos e técnicas de gerenciamento de projetos são úteis para implementar a política de segurança na instituição. Processos relacionados à gestão de custos, tempo, escopo e demais áreas de gestão de projetos são necessários para a formação de equipes, elaboração de cronogramas, medição de custos, negociação de prazos, contratação de fornecedores, entre outros. Desta forma a instituição deve adotar boas práticas de gestão de projetos em apoio ao ciclo PDCA.

O PMBOK (Project Management Body of Knowledge) é um livro que reúne um conjunto de práticas e processos em gerenciamento de projetos, constituindo a base do conhecimento do PMI (Project Management Institute).

Dentre tantas metodologias e bibliografia sobre gerenciamento de projetos, o PMBOK firmou-se na última década como a mais aceita e difundida no mundo, sendo cada vez mais adotada por instituições públicas e privadas para a condução de seus projetos e capacitação de seus gerentes.

Este livro define que: *"Gerenciamento de projetos é a aplicação de conhecimento, habilidades, ferramentas e técnicas às atividades do projeto a fim de atender aos seus requisitos."* [PMBOK 4th Edition:2008].

O PMBOK também define que: *"O ciclo de vida de um projeto consiste nas fases do mesmo que geralmente são sequenciais e que às vezes se sobrepõem, cujo nome e número são determinados pelas necessidades de gerenciamento e controle da(s) organização(ões) envolvida(as), a natureza do projeto em si e sua área de aplicação."* [PMBOK 4th Edition:2008].

Desta forma, para cada projeto são definidos os processos e técnicas que serão utilizados, não necessariamente todos os processos do PMBOK estarão presentes em cada projeto; pelo contrário apenas os processos relacionados às características de cada trabalho são adotados. Logicamente existem processos que devem ser utilizados em todos os projetos, como por exemplo: o processo *Orientar e Gerenciar a Execução do Projeto*, a execução do escopo proposto é tarefa necessária em qualquer projeto.

Porém dependendo do tamanho, natureza e importância do projeto alguns processos podem não ser adotados, como por exemplo: o processo *Planejar as Aquisições*, caso o projeto não faça aquisições ou compras de material ou serviço; ou ainda o processo *Planejar o Gerenciamento de Riscos*, se não há no projeto uma análise prévia de riscos.

Outros conceitos importantes são os de:

- Processo: *"Um processo é um conjunto de ações e atividades inter-relacionadas que são executadas para alcançar um produto, resultado ou serviço predefinido. Cada processo é caracterizado por suas entradas, as ferramentas e as técnicas que podem ser aplicadas e as saídas resultantes."* [PMBOK 4th Edition:2008].
- Fases do Projeto: *"As fases do projeto são divisões de um projeto onde controle adicional é necessário para gerenciar de forma efetiva o término de uma entrega importante. Geralmente as fases são terminadas sequencialmente, mas podem se sobrepor em algumas situações."* [PMBOK 4th Edition:2008].

Por fim para o entendimento da metodologia é necessário a noção do que são as áreas de conhecimento. O PMBOK agrupa os processos por áreas de acordo com determinados critérios, a divisão atual apresenta nove áreas de conhecimento descritas a seguir:

- Gerenciamento de Escopo: conjunto de atividades para determinar e controlar o escopo do projeto e suas mudanças.
- Gerenciamento de Tempo: conjunto de atividades para determinar e controlar o cronograma e prazos do projeto e suas mudanças.
- Gerenciamento de Custo: conjunto de atividades para determinar e controlar os custos do projeto e suas mudanças.
- Gerenciamento da Qualidade: conjunto de atividades para planejar e realizar o controle de qualidade do projeto.
- Gerenciamento de Recursos Humanos: conjunto de atividades para contratação, capacitação, mobilização e gerenciamento dos recursos humanos do projeto.
- Gerenciamento da Comunicação: conjunto de atividades para geração, coleta, distribuição e armazenamento das informações do projeto.
- Gerenciamento de Riscos: conjunto de atividades relacionadas com a identificação, análise e controle dos riscos do projeto.
- Gerenciamento de Aquisições: conjunto de atividades para compra ou aquisições de produtos ou serviços para a realização do projeto.
- Gerenciamento da Integração: conjunto de atividades relacionadas com a integração de todas as áreas e elementos necessários para o gerenciamento do projeto como um todo.

A partir do entendimento das áreas de conhecimento descritas acima, pode-se por fim relacioná-las com os processos definidos no PMBOK. De forma sucinta seguem alguns dos principais processos que podem servir de apoio na implantação da política de segurança da informação:

- Escopo – definir o escopo, verificar o escopo, controlar o escopo.

- Tempo – definir as atividades, desenvolver o cronograma, controlar o cronograma.
- Custo – estimar os custos, determinar o orçamento, controlar os custos.
- Qualidade – planejar a qualidade, realizar o controle da qualidade.
- Recursos Humanos – mobilizar a equipe, desenvolver a equipe, gerenciar a equipe.
- Comunicações – identificar as partes interessadas, planejar as comunicações, distribuir as informações.
- Riscos – identificar os riscos, planejar as respostas aos riscos, monitorar e controlar os riscos.
- Aquisições – planejar as aquisições, realizar as aquisições, administrar as aquisições.

2.4 A ITIL

A ITIL (Information Technology Infrastructure Library) é um conjunto de processos, procedimentos e boas práticas usadas para o gerenciamento de serviços de tecnologia da informação. Tais práticas foram compiladas em cinco livros:

- Estratégia de Serviço – neste livro são tratados os aspectos relacionados ao alinhamento do negócio e da tecnologia da informação.
- Desenho de Serviço – neste livro são tratados processos e arquiteturas necessárias para atender aos requisitos de negócio atuais e futuros.
- Transição de Serviço – neste livro é abordado como é realizada a inserção, em ambiente operacional, de um serviço ou conjunto de serviços.
- Operação de Serviço – neste livro as diretrizes são relacionadas a manter o serviço em operação de acordo com o nível de serviço estabelecido para gerar os resultados esperados.
- Melhoria de Serviço Continuada – as práticas descritas neste livro visam o gerenciamento de melhorias nos processos de Gerenciamento de Serviço de TI, bem como nos próprios serviços de TI implementados na produção.

A ITIL tem um núcleo de condução das atividades que é a estratégia de serviço, que serve de base para os demais livros. Todos os livros são vistos como fases do ciclo de vida dos serviços. A utilização deste modelo no ambiente organizacional pode propiciar vários benefícios, tais como diminuição dos custos operacionais, aumento da eficiência e maior satisfação do cliente, seja ele externo ou interno.

As boas práticas da ITIL servem como técnicas e procedimentos complementares a metodologia de projetos do PMBOK e ao ciclo PDCA, buscando desta forma uma

maneira de integrar de forma eficaz e eficiente pessoas, processos e tecnologias envolvidas tanto na fase de projeto quanto na gestão dos serviços em produção.

- Durante a fase de execução serão observados, principalmente, os processos definidos no livro três, denominado de Transição de Serviço. Durante a implantação os serviços são testados e validados, este livro apresenta uma sequência lógica para esta fase do projeto, tratada no item 4.3.

Este modelo sequencial servirá como referência para colocar os serviços em produção, por exemplo, para cada serviço haverá um planejamento prévio, serão avaliados os equipamentos necessários, softwares necessários, recursos humanos, autorizações e licenças, capacitação e mudança; posteriormente o serviço é validado na produção e avaliado quanto ao desempenho e requisitos. Por fim, o conhecimento adquirido deve ser propagado no corpo técnico e quando necessário para toda a instituição.

A ITIL não dá uma descrição precisa, rígida ou detalhada de como essas atividades devem ser conduzidas, pois cada organização tem suas próprias características, porém o modelo descrito serve de base para a transição dos serviços na produção de maneira mais eficiente. Por exemplo, algumas das atividades pertinentes para a instalação de um novo software na produção:

- Testes para sua validação antes da instalação no ambiente corporativo.
- As equipes técnicas devem ser treinadas antes dos serviços entrarem em produção.
- A quantidade de licenças deve ser adequada.
- Caso necessário o suporte externo e a assistência técnica devem ser previamente contratados.
- Os usuários devem ter as permissões e os perfis corretos.
- Deve ser avaliada a necessidade de treinamento dos usuários.

Porém, a forma como essas atividades serão conduzidas depende muito da instituição em questão e de sua cultura organizacional.

A gestão do conhecimento segue tanto as boas práticas da administração de empresas, bem como as recomendações da ITIL, as quais são mais voltadas ao ambiente e serviços de tecnologia da informação.

Outra questão importante é descrita no livro quatro, que são as diretrizes voltadas à operação dentro dos níveis de serviço estabelecidos junto aos clientes, sendo referência para as atividades do dia-a-dia da instituição.

Por fim, o gerenciamento destes serviços não se encerra ao final do projeto de implantação, persistindo dentro da instituição através de atividades de suporte, manutenção, aprimoramento e capacitação. Portanto, são também necessárias boas práticas em relação a serviços e políticas implantadas na organização, item contemplado no livro cinco da ITIL, que descreve práticas de melhoria contínua.

A definição de serviço pela ITIL: *"Um serviço é um meio de entregar valor aos clientes, facilitando os resultados que os clientes querem alcançar, sem ter que assumir custos ou riscos"* [ITIL V3:2007].

A definição de Gerenciamento de Serviços pela ITIL: *"O Gerenciamento de Serviços é um conjunto de habilidades da organização para fornecer valor para o cliente em forma de serviços"* [ITIL V3:2007].

2.5 A ISO 27004

Esta norma destina-se a ajudar as organizações a definirem métricas e realizarem medições para melhorar sistematicamente a eficácia de seus sistemas de gestão da segurança da informação. São apresentadas várias técnicas para coleta de informação e posterior geração de indicadores de desempenho. Com isso os gestores podem avaliar de forma adequada se os controles alcançam de forma satisfatória os objetivos de controle planejados e dessa forma podem tomar decisões gerenciais, aplicar medidas corretivas e promover a melhoria contínua dos processos dentro da instituição.

Para apoiar a tomada de decisão e avaliar o desempenho dos serviços em produção são necessárias medidas relativas à gestão dos indicadores e a medição da segurança da informação, algumas tarefas relacionadas são listadas a seguir:

- Criar uma cultura e clima dentro da instituição para coleta de dados e para efetuar as medições.
- Interpretar os resultados obtidos em relação às metas estabelecidas e aos referenciais de excelência.
- Aplicar conceitos básicos de matemática e estatística na criação e gestão dos indicadores.
- Definir de forma clara os objetivos da medição da segurança da informação.
- Definir a responsabilidade da direção no apoio ao processo e na análise dos resultados.
- Desenvolver métricas e medições apropriadas; utilizando unidades, periodicidade, métodos e classificações pertinentes a cada indicador.
- Analisar os dados e comunicar os resultados às partes interessadas através de relatórios, gráficos ou tabelas.
- Empregar ferramentas de gestão (Diagrama de Ishikawa, Pareto, Matriz de Probabilidade e Impacto) na elaboração de relatórios e na divulgação dos resultados.
- Implantar e monitorar as ações corretivas necessárias.

3 Implantação da Política de Segurança na Produção

Alguns cuidados devem ser tomados para uma melhor transição dos serviços relacionados com a implantação da nova política de segurança na instituição:

- Planejar cuidadosamente a finalidade, o escopo e o alcance da política de segurança antes de sua implantação.
- Para que a transição de serviços ocorra de forma mais eficiente é aconselhável começar por serviços e práticas mais simples e que tenham um maior benefício para a organização; deixando as tarefas de maior complexidade e menor retorno para serem implementadas por último.
- Evitar colocar na política de segurança qualquer requisito ou exigência que na prática não será seguido.
- Tratar a criação de políticas de segurança como uma mudança da cultura organizacional, tendo um plano de divulgação cuidadosamente criado.

Uma clara compreensão dos objetivos da política de segurança é o ponto de partida para atingi-los com a sua implementação. Se o propósito não é claramente entendido quando está escrito, surgirão problemas para resolver durante a execução.

Não é benéfico ou mesmo prático lidar com todas as formas possíveis de incidentes de segurança, da mesma forma não será possível implementar uma política imune a falhas. É fundamental entender que a implementação deve focar em objetivos realistas.

Os gerentes devem ter a experiência necessária e o senso crítico para avaliar os processos durante a execução e propor as ações corretivas. A alta direção deve participar e fornecer todo o apoio necessário à implantação.

É necessário conhecimento profundo da instituição, suas normas, seus procedimentos e sua cultura organizacional. Toda organização apresenta áreas de maior impacto, que muitas vezes deverão ser priorizadas durante a implantação. Determinadas políticas podem ser implementadas antes em determinado ambiente ou departamento, se estes requerem maior atenção e rapidez em relação à segurança da informação. Caberá aos gestores avaliar e sequenciar a implementação dos serviços da forma mais eficiente para instituição como um todo.

É fundamental o entendimento de que a segurança da informação dentro da instituição é um processo contínuo.

A implementação será realizada observando as técnicas, normas e metodologias descritas na seção anterior. Para uma melhor organização do trabalho foram definidas as seguintes etapas para a implementação da política de segurança:

- Inicialização – composta por um único processo que visa documentar e iniciar formalmente a implementação.
- Planejamento – composta pelos processos necessários para formação de equipes, determinação de responsabilidades, identificação de riscos, elaboração de cronograma de trabalho, determinação do orçamento,

planejamento de aquisições, entre outros. Esta fase engloba a etapa “Plan” do modelo PDCA.

- Execução – composta pelos processos de gerenciamento e execução das atividades planejadas. Esta fase engloba a etapa “Do” do modelo PDCA.
- Monitoração e Controle – composta pelos processos de controle, medição e análise crítica dos serviços implementados. Esta fase engloba as etapas “Check” e “Act” do modelo PDCA.

Cada processo utilizado na implementação da política de segurança apresenta um número determinado de entradas que resultam em um número determinado de saídas. A notação a seguir foi utilizada para a sua representação, que detalhamos nos itens 4.1 a 4.4.

N**ome do Processo**

Descrição do Processo.

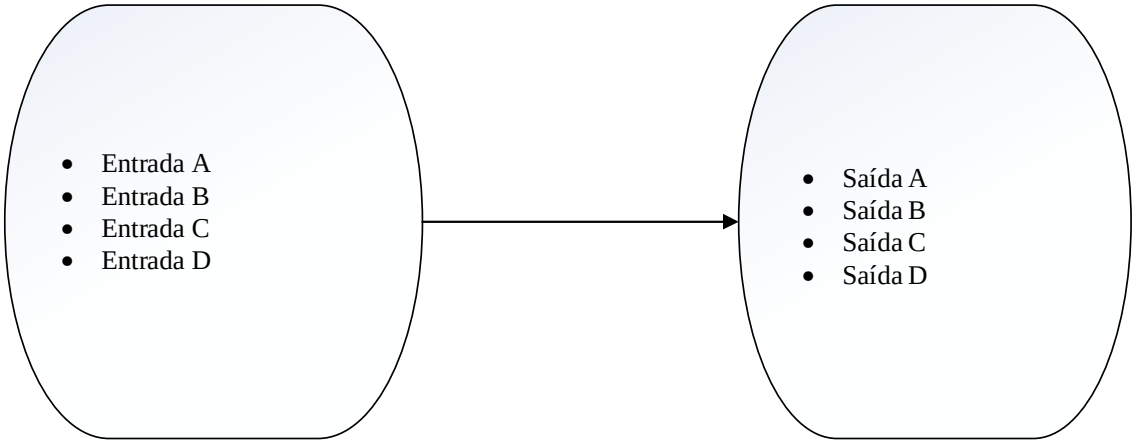

Figura 2. Processo genérico

3.1 Inicialização

Esta fase define o processo necessário para o início da implementação da política de segurança na instituição:

3.1.1 Desenvolver o Termo de Abertura

O início da implementação deve gerar um documento formal que pode ser na forma de um plano ou mesmo de uma ata de reunião, este documento é o Termo de Abertura.

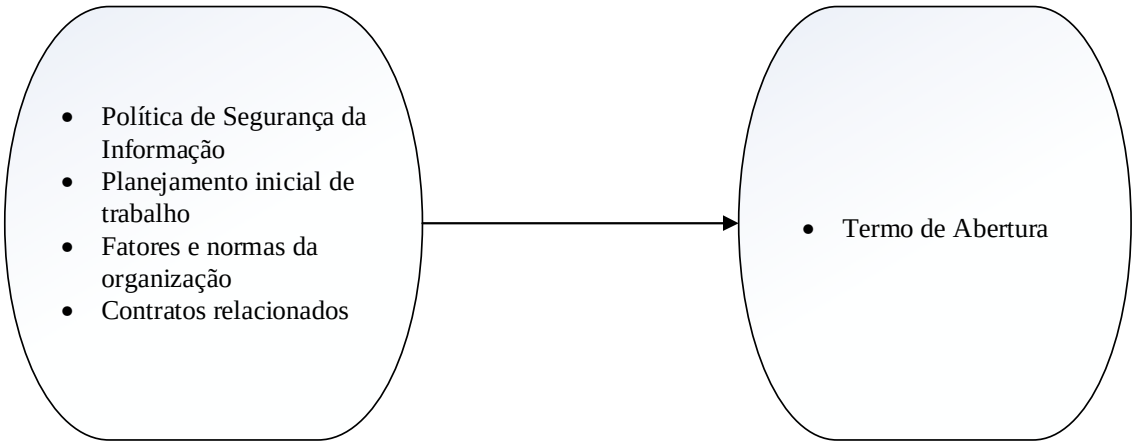

Figura 3. Desenvolver o termo de abertura

No termo de abertura deve ser definido o responsável ou os responsáveis pela implementação da política de segurança. É necessária a participação dos gerentes envolvidos e desejável a participação do diretor da área.

3.2 Planejamento

Este grupo de processos define os processos necessários para definição do escopo, refina os objetivos e desenvolve o curso para alcançar esses objetivos. Estes processos são listados a seguir:

3.2.1 Definir o escopo

Esse processo é necessário para definir o escopo que será fundamental para condução dos trabalhos e decisões futuras. O escopo deverá conter o detalhamento de todas as áreas abordadas pela política de segurança como gestão da segurança da informação; gestão dos ativos de informação; controle de acesso dos usuários; política de senhas; aquisição de componentes de hardware e software; gestão dos equipamentos; dispositivos móveis; instalação e utilização de softwares; compartilhamento de arquivos; cópias de segurança; uso da internet; uso de correio eletrônico; utilização de antivírus; termo de confidencialidade; desenvolvimento, manutenção e testes de software; descarte de mídias removíveis; segurança em recursos humanos; incidentes de segurança e penalidades.

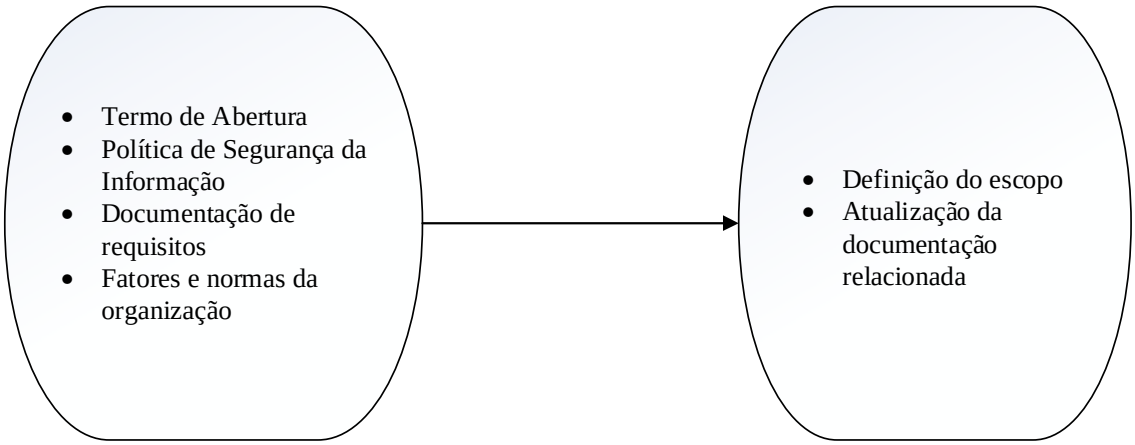

Figura 4. Definir o escopo

3.2.2 Definir as atividades

Esse processo é necessário para definir as atividades necessárias para produzir os produtos esperados pela implementação da política de segurança.

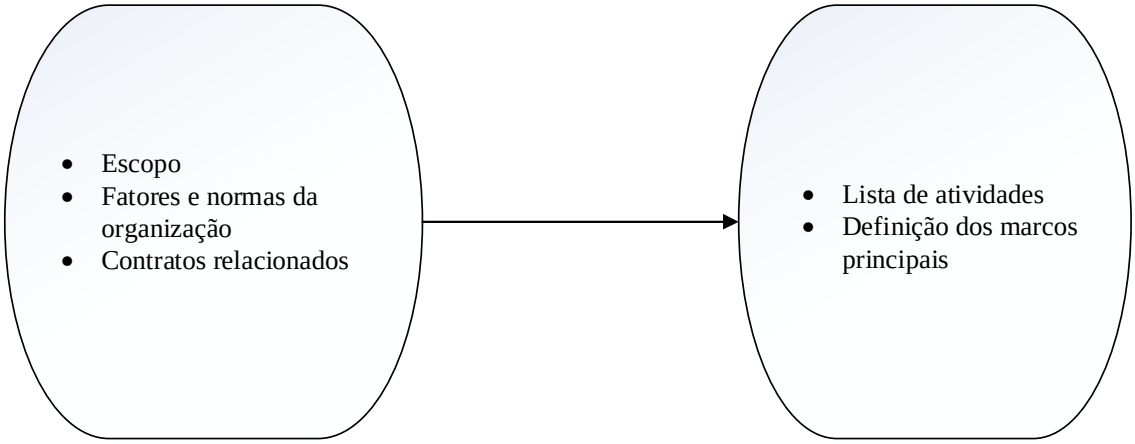

Figura 5. Definir as atividades

Uma lista de atividades elenca as tarefas necessárias para se alcançar determinado produto, como por exemplo:

A Implantação da política de descarte de mídias removíveis tem como atividades:

- Elaboração do procedimento operacional de descarte de mídias removíveis.
- Treinamento dos responsáveis pelo serviço de descarte de mídias.
- Realização de testes e validação do procedimento operacional.
- Divulgação do procedimento operacional de descarte de mídias.
- Implementação da política de descarte de mídias no ambiente de produção.

Incidentes de Segurança tem como atividades:

- Elaboração dos documentos de registro de incidentes de segurança.
- Treinamento dos responsáveis em relação aos procedimentos operacionais.
- Definição das ações e respostas esperadas mediante a gravidade dos incidentes.
- Elaboração de relatórios gerenciais com a medição mensal dos incidentes.

Controle de Acessos dos Usuários tem a seguinte lista de atividades:

- Elaboração do procedimento operacional para permitir a criação e o cancelamento de contas.
- Normatização dos perfis de acesso de cada sistema.
- Elaboração do procedimento operacional para acesso remoto.
- Elaboração do procedimento operacional para acesso externo de usuários.
- Testes e validação dos procedimentos de acesso.
- Implementação do controle de acessos no ambiente de produção.

3.2.3 Estimar os recursos das atividades

Este processo define quais recursos, sejam humanos ou equipamentos, são necessários para cumprir as atividades definidas no processo anterior. Para a implantação da política de segurança serão alocados recursos humanos para as atividades de acordo com a sua complexidade e nível de acesso à informação.

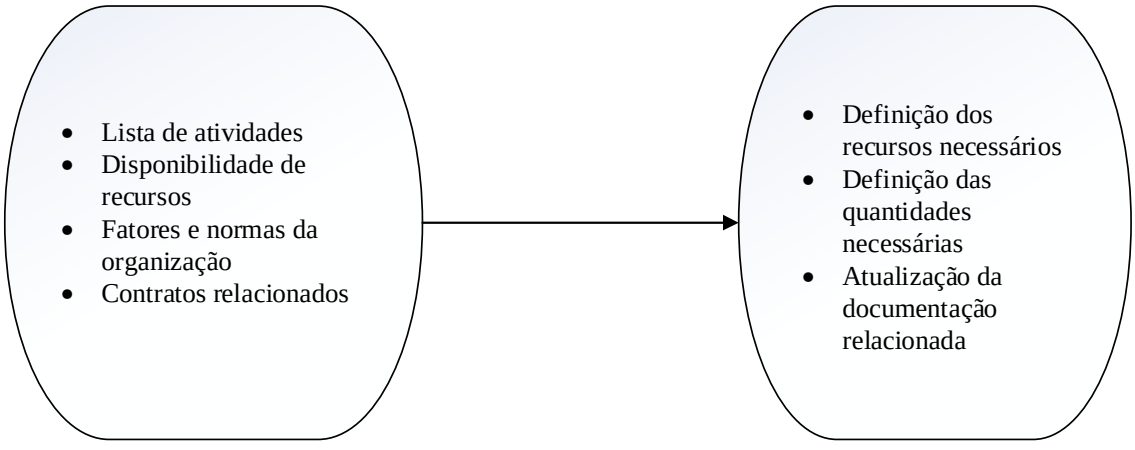

Figura 6. Estimar os recursos das atividades

Para cada atividade deverá existir um responsável pela execução e a supervisão de um gestor da área. Os recursos humanos serão classificados da seguinte forma:

- Técnico – profissional de nível técnico com até cinco anos de experiência.

- Técnico sênior – profissional de nível técnico com mais de cinco anos de experiência.
- Analista – profissional de nível superior com até cinco anos de experiência.
- Analista sênior – profissional de nível superior com mais de cinco anos de experiência.
- Gerente do setor – profissional com até cinco anos de experiência na gestão de pessoas e contratos.
- Assessor do Diretor de T.I. – profissional com mais de cinco anos de experiência na gestão de pessoas e contratos.
- Diretor – profissional responsável pela área de TI.

Excepcionalmente algumas pessoas poderão atingir o nível sênior em período menor que cinco anos, isto devido à proficiência técnica, necessidade da instituição ou habilidades gerenciais acima da média. A seguir os recursos estimados para algumas das atividades previstas no processo anterior:

- Elaboração do procedimento operacional de descarte de mídias removíveis – Analista.
- Treinamento dos responsáveis pelo serviço de descarte de mídias – Técnico sênior.
- Realização de testes e validação do procedimento operacional – Técnico sênior.
- Divulgação do procedimento operacional de descarte de mídias – Gerente do setor.
- Implementação no ambiente de produção da instituição – Técnico sênior.
- Elaboração do procedimento operacional para permitir a criação e o cancelamento de contas – Analista.
- Elaboração do procedimento operacional para acesso remoto – Analista.
- Elaboração do procedimento operacional para acesso externo de contribuintes – Analista sênior.
- Testes e validação dos procedimentos de acesso – Analista.
- Implementação do controle de acessos no ambiente de produção – Analista.

3.2.4 Estimar as durações das atividades

Este processo é necessário para definir os tempos aproximados para completar as atividades. Para isso é necessário que os gestores das áreas analisem as atividades, sempre consultando as pessoas que as executam, para definirem seu tempo aproximado

de execução. Também é necessária a avaliação quanto à disponibilidade de recursos humanos ou equipamentos.

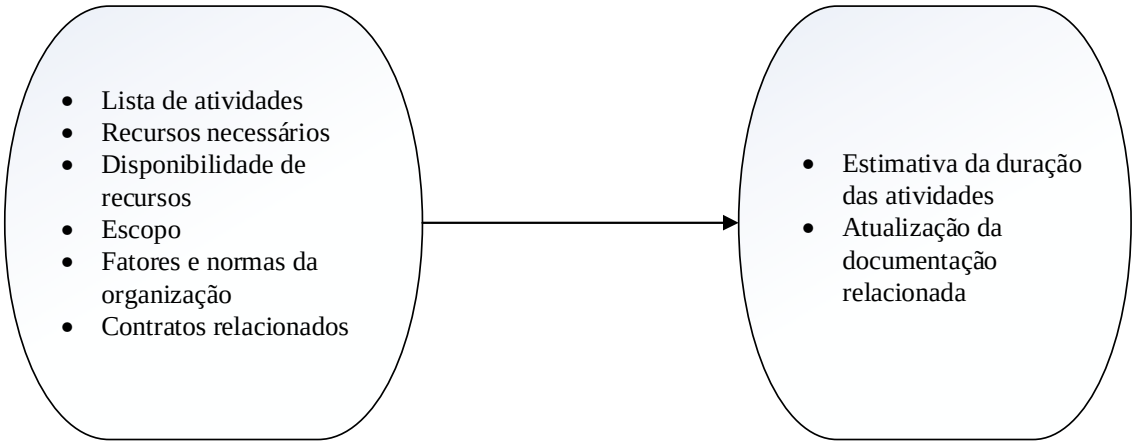

Figura 7. Estimar as durações das atividades

3.2.5 Desenvolver o cronograma

Este processo analisa a sequência das atividades, suas durações, os recursos necessários e as restrições para gerar um cronograma de execução. Este é um dos principais processos da fase de planejamento.

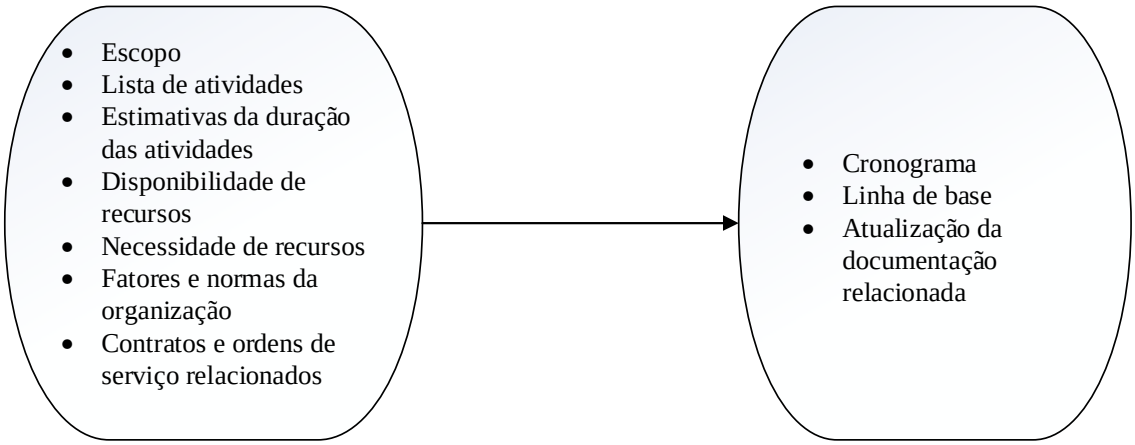

Figura 8. Desenvolver o cronograma

A linha de base ou *baseline* é uma versão específica e inicial do cronograma com as datas de início e término definidas para todas as atividades, neste estágio as tarefas e os recursos já devem ter sido previamente definidos e aprovados. A linha de base serve para o acompanhamento de prazos e marcos durante toda a execução.

A medição deve ser feita sempre avaliando o cronograma realizado comparado ao cronograma programado, definido pela linha de base; de forma a corrigir as distorções, avaliar o desempenho e executar as ações corretivas.

O cronograma também é uma importante ferramenta gerencial, devendo ser enviando para o escritório de projetos e à alta gestão da instituição periodicamente de forma a documentar o progresso da implementação da política de segurança.

Para desenvolver o cronograma a organização utilizará o software especializado em gerenciamento de projetos Microsoft Project, já licenciado para esta instituição.

Os softwares de gerenciamento de projeto apresentam várias formas de visualização do cronograma, sendo que as mais utilizadas são referentes ao diagrama de Gantt:

- Visão tabular – onde o gerente pode escolher quais informações são relevantes e apresentá-las em forma de tabela. Por exemplo, na figura 9 (nove) há nome da tarefa, sua duração, seu início, seu término, as atividades interdependentes e o nome dos recursos.
- Visão gráfica – onde o gerente adota um gráfico para ilustrar o avanço das diferentes etapas do projeto conforme a figura 10 (dez).

As tarefas descarte de mídias removíveis e controle de acesso já tiveram suas atividades e recursos definidos nos processos anteriores, desta forma é possível desenvolver seu cronograma conforme as figuras 9 (nove) e 10 (dez).

GRÁFICO DE GANTT

	Modo da	Nome da tarefa	Duração	Início	Término	Predecessoras	Nomes dos recursos
1		**Descarte de Mídias Removíveis**	**17 dias**	**Seg 02/06/14**	**Ter 24/06/14**		
2		Elaboração do Procedimento	3 dias	Seg 02/06/14	Qua 04/06/14		Analista 1
3		Testes e validação do Procedimento	3 dias	Qui 05/06/14	Seg 09/06/14	2	Técnico sênior
4		Treinamento	3 dias	Ter 10/06/14	Qui 12/06/14	3	Técnico sênior
5		Divulgação do Procedimento	5 dias	Sex 13/06/14	Qui 19/06/14	4	Gerente
6		Implementação da Política de descarte	3 dias	Sex 20/06/14	Ter 24/06/14	5	Técnico sênior
7		**Controle de Acessos de Usuários**	**15 dias**	**Seg 09/06/14**	**Sex 27/06/14**		
8		Procedimento criação/cancelamento de contas	3 dias	Seg 09/06/14	Qua 11/06/14		Analista 2
9		Procedimento de acesso remoto	3 dias	Seg 09/06/14	Qua 11/06/14		Analista 3
10		Procedimento de acesso de contribuintes	5 dias	Seg 09/06/14	Sex 13/06/14		Analista sênior
11		Testes e validação dos Procedimentos	5 dias	Seg 16/06/14	Sex 20/06/14	10	Analista 3
12		iImplementação da política de controle de acessos	5 dias	Seg 23/06/14	Sex 27/06/14	11	Analista 3

Figura 9. Representação tabular das tarefas do cronograma

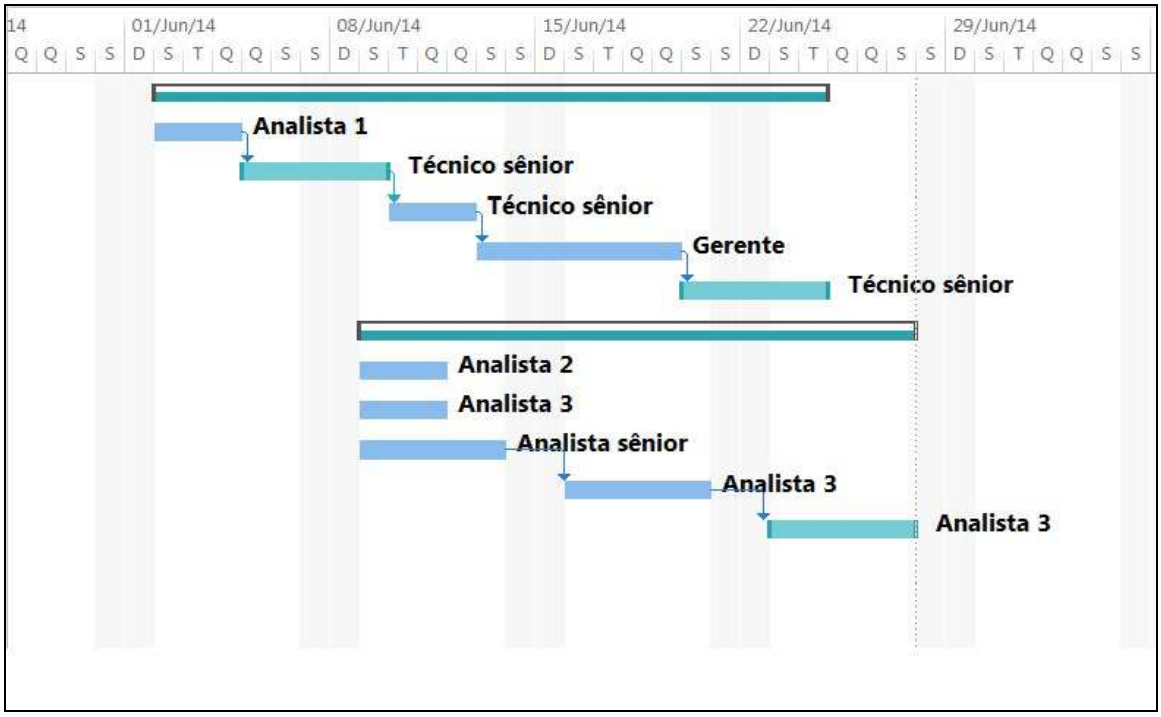

Figura 10. Representação do Gráfico de Gantt das tarefas do cronograma

3.2.6 Determinar o orçamento

É o processo de agregação dos custos estimados das atividades ou pacotes de trabalho para estabelecer o orçamento da implementação da política de segurança na produção.

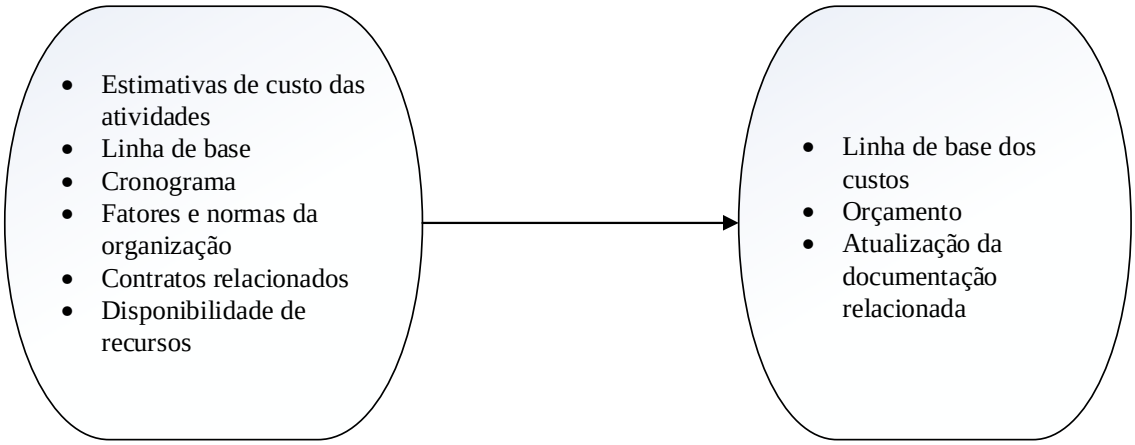

Figura 11. Determinar o orçamento

Para determinar os custos necessários para a implementação na produção a instituição conta com a experiência de gestores que conhecem o ambiente e participaram de projetos semelhantes no passado. Esta opinião especializada será responsável por avaliar os diversos fatores que influenciam os custos como taxas de mão de obra, valor dos equipamentos, inflação, taxa de juros, relação com os fornecedores, fatores de risco, entre outros.

O cronograma elaborado no processo anterior servirá como importante ferramenta para orçar o custo com pessoal, já que os valores de homem/hora são conhecidos para todos os recursos humanos dentro da organização.

Por exemplo, para orçar a atividade de Elaboração do procedimento operacional para permitir a criação e o cancelamento de contas:

- Recurso interno necessário: Analista – R$ 80,00 / hora.
- Duração da tarefa: 16 horas.
- Custo com mão de obra: R$ 1.280,00.

Para orçar a tarefa de Elaboração do procedimento operacional para permitir o acesso de contribuintes:

- Recurso interno necessário: Analista sênior – R$ 100,00 / hora.
- Recurso de suporte externo: Analista de segurança – R$ 120,00 / hora.
- Duração da tarefa: 20 horas com 2 horas previstas de suporte externo.
- Custo com mão de obra: R$ 2.040,00.

Sobre os valores de mão de obra são somados os custos fixos pertinentes e demais despesas que podem ocorrer com equipamentos, hospedagem, alimentação e custos adicionais que possam ser relacionados diretamente com a tarefa em questão.

Depois de realizado todo esse processo para cada atividade definida no cronograma, o gerente terá um orçamento detalhado por atividade que quando totalizado gerará o orçamento total de implementação da política de segurança na produção.

O orçamento realizado será alimentado no sistema de gerenciamento de projetos periodicamente e comparado ao planejado utilizando-se das funções residentes no software.

3.2.7 Identificar os riscos

Processo para determinar quais os riscos podem afetar a implementação e para documentar suas características.

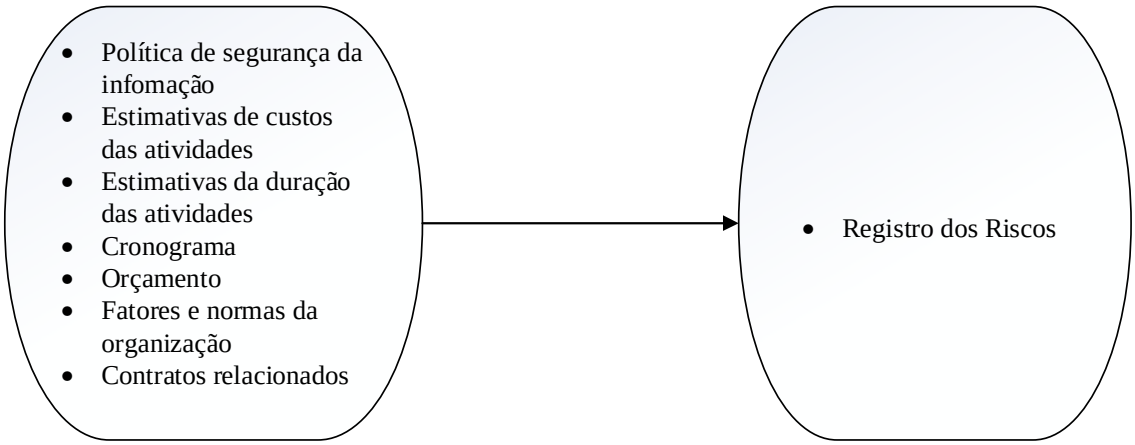

Figura 12. Identificar os riscos

A abordagem focada na prática de controles de risco será sempre mais eficaz na redução de falhas de segurança do que tentar resolver os problemas apenas quando estes ocorrerem.

Alguns **pecados** citados por Sêmola na implementação de uma política de segurança da informação:

- Atribuir exclusivamente à área de tecnológica a segurança da informação;
- Posicionar os responsáveis pela segurança imediatamente abaixo da diretoria de TI;
- Definir investimentos limitados e subestimados a esta atividade;
- Elaborar planos voltados à reatividade;
- Ignorar a interferência da segurança no negócio;
- Tratar as atividades de segurança como despesa e não como investimento;
- Satisfazer-se com ações de segurança isoladas;
- Não cultivar corporativamente a mentalidade de segurança;
- Tratar a segurança como um projeto, com início e fim, e não como um processo contínuo.

O projeto de implementação deverá conter um capítulo de gerenciamento de riscos com a identificação dos riscos e seu ranqueamento quanto à probabilidade de se tornarem problemas, contemplando ações de mitigação de acordo com as boas práticas indicadas pelo PMI.

3.2.8 Planejar as aquisições

É o processo de documentação das decisões de compra e contratação, especificando a abordagem, a forma e os fornecedores em potencial.

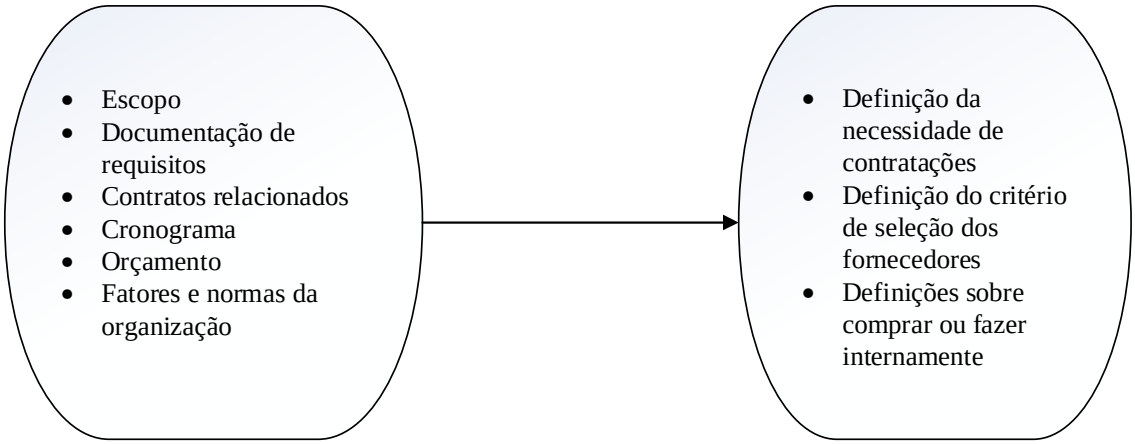

Figura 13. Planejar as aquisições

3.2.9 Definir os perímetros do ambiente de produção

Este processo estuda o ambiente de produção e os ativos que sustentam cada negócio da organização. Este estudo serve para definir os aspectos relevantes da infraestrutura física, tecnológica e humana que tem relação com cada um dos serviços que serão implementados na instituição. As principais saídas deste processo são a definição dos perímetros, dos processos de negócio críticos e de seus gestores responsáveis.

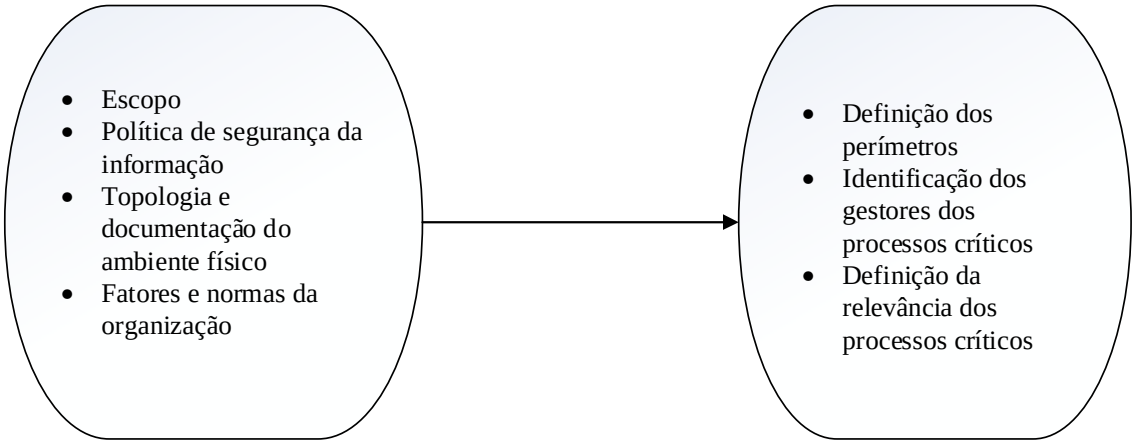

Figura 14. Definição dos perímetros da produção

Este processo se justifica pelo perfil técnico de muitas das atividades necessárias para se atingir a solução de segurança da informação desejada pela instituição.

O ambiente da instituição é bastante complexo e muitas vezes heterogêneo. Além das diversas plataformas de hardware e software, os usuários apresentam níveis de

conhecimento bastante diversos. Todos estes fatores devem ser levados em consideração para a implementação da política de segurança.

É comum nesta etapa a avaliação de plantas baixas do ambiente físico, de inventário de equipamentos, da documentação topológica, dos sistemas e das plataformas existentes. A partir desta documentação e da análise crítica dos gestores mais experientes serão definidos os ambientes de trabalho que existem dentro da instituição.

Estas definições servem para avaliar de forma criteriosa os impactos de um incidente de segurança dentro de cada área da instituição. Por exemplo, um incidente de segurança dentro de um perímetro de testes terá pequena relevância se comparado ao mesmo incidente em um perímetro de produção.

A seguir a definição dos símbolos utilizados para na definição desses perímetros:

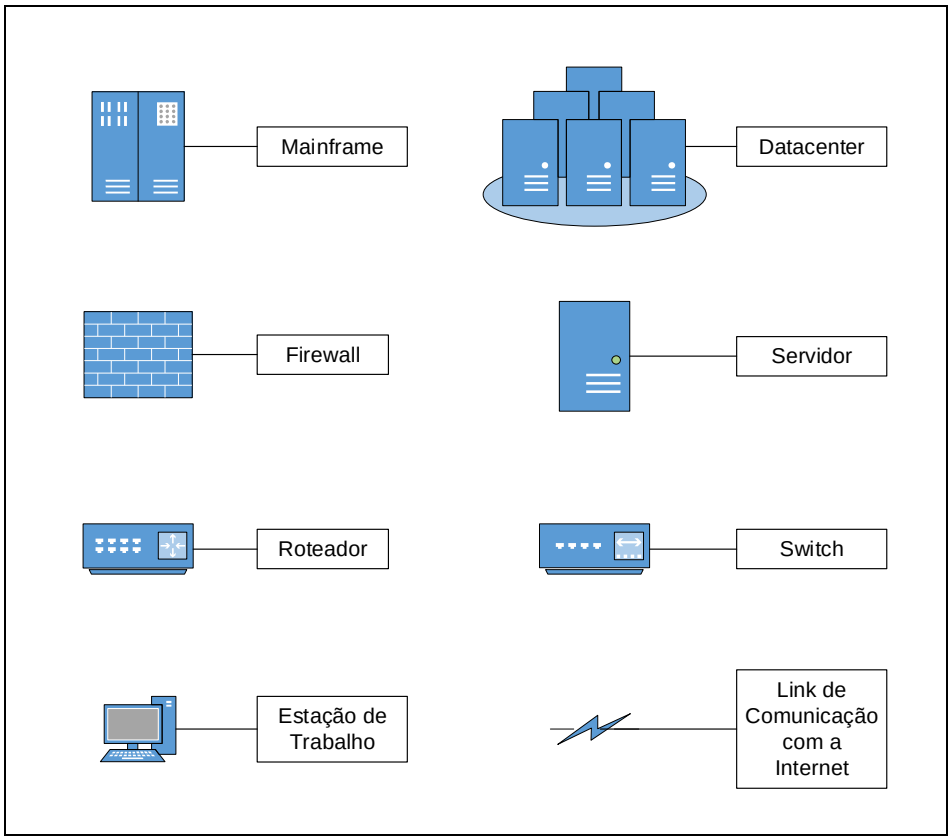

Figura 15. Simbologia utilizada na descrição dos perímetros

É importante entender que existem usuários que acessam tanto servidores mainframe quanto ambientes em baixa plataforma (aplicativos voltados a web) localizados na própria instituição ou externos a ela. Estes equipamentos e suas aplicações na organização podem ser de tecnologias bastante distintas. Os usuários possuem níveis de criticidade de segurança diferentes a serem considerados. A seguir uma representação simplificada do ambiente de produção da instituição:

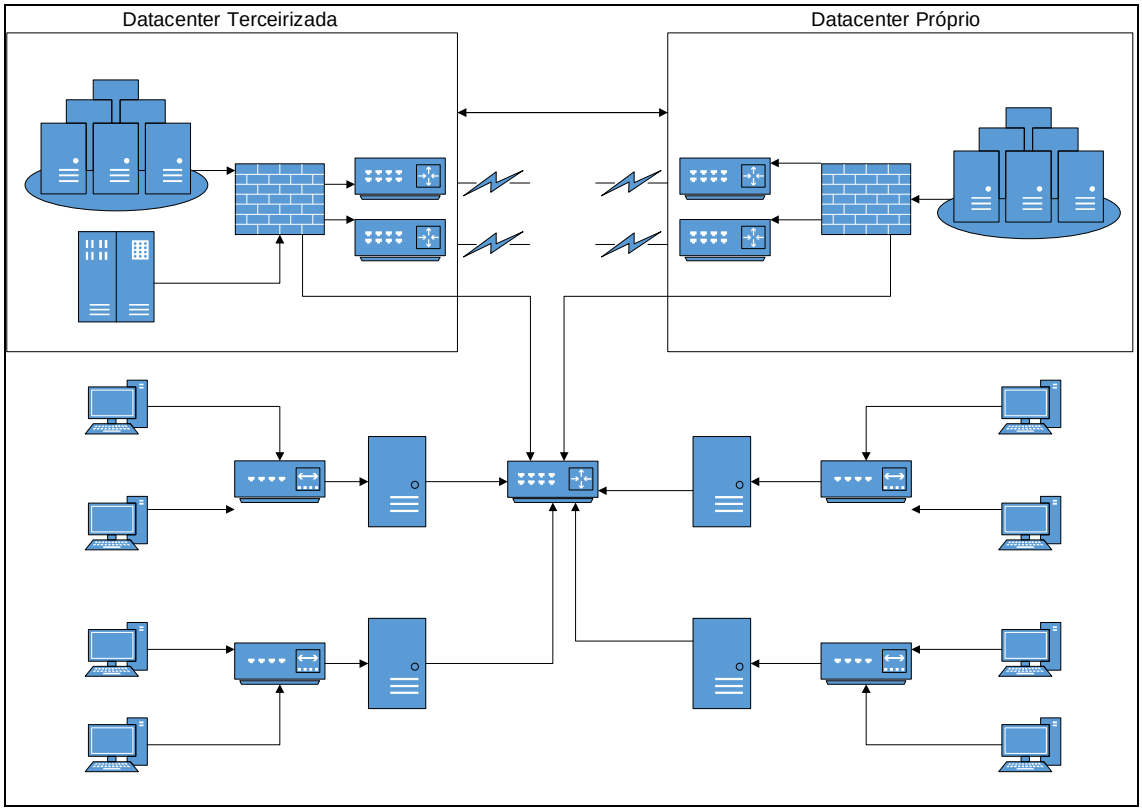

Figura 16. Representação simplificada do ambiente integrado

Conforme representado no diagrama anterior, a partir das estações de trabalho os usuários acessam tanto os servidores mainframe e de aplicativos web localizados na empresa prestadora de serviços de T.I. como os demais servidores localizados no datacenter próprio da instituição. Como existem processos de negócio críticos em servidores mainframe e em servidores do datacenter não é possível caracterizar um ambiente como sendo o mais importante para a organização neste aspecto. Porém a característica predominante dos dados do ambiente terceirizado, por se tratarem de dados transacionais atualizados em tempo integral, nos leva a crer que nível de disponibilidade deste ambiente deva ser bem maior.

Em relação à criticidade pode ser feita distinção quanto a servidores utilizados para testes/homologação e servidores que suportam os processos de negócio da produção. Os servidores de testes são menos críticos para a instituição e consequentemente o impacto de um incidente de segurança nestes servidores deve ser tratado de forma menos crítica do que em um servidor da produção.

O conhecimento mais detalhado da topologia e da infraestrutura será necessário para que os gestores conduzam a implementação da política de segurança de forma otimizada respeitando a criticidade de cada ambiente e de cada tipo de usuário, o que não será feito neste momento. Outros fatores relevantes que devem ser abordados e detalhados no planejamento são o mapeamento dos processos críticos de T.I. e de seus gestores responsáveis.

3.2.10 Elaborar os planos de segurança

Este processo tem como saída os planos de segurança que a instituição utilizará com a implementação da política de segurança.

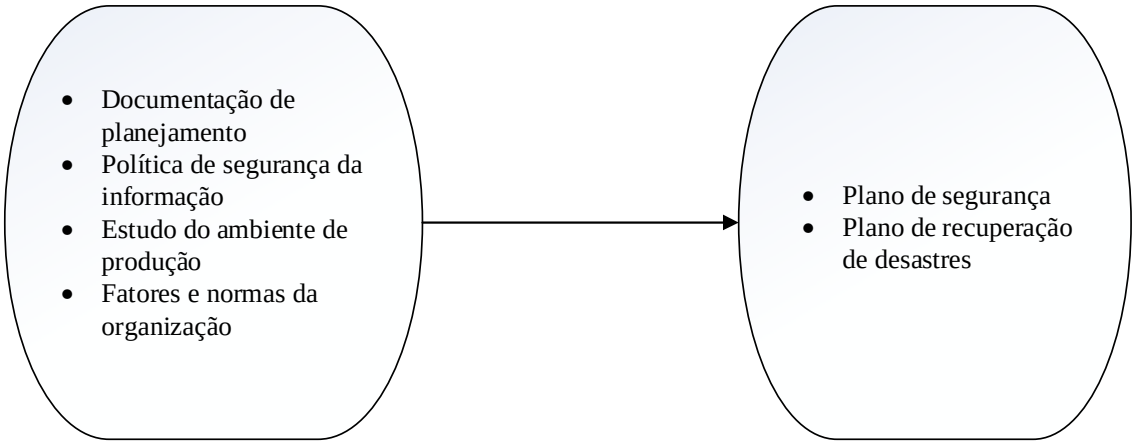

Figura 17. Elaborar os planos de segurança

O plano de segurança utilizará a documentação da etapa de planejamento e a expertise técnica da organização para definir diretrizes a respeito de ameaças, riscos, sensibilidades, impactos e vulnerabilidade física, tecnológica e humana. Este plano deve especificar ações e atividades que deverão ser executadas de forma a atingir os níveis de segurança desejados com a implementação da nova política. Nesta fase podem ser criados grupos ou comitês de segurança que visarão medir os resultados do ambiente de produção, reportar novas necessidades e situações que exponham a segurança da informação dentro da organização.

O plano de recuperação de desastres visa garantir a continuidade de processos cruciais à instituição, com o objetivo de minimizar impactos de um eventual desastre. Este plano deve abordar incidentes de segurança que não possam ser evitados. Os gestores devem analisar os vários objetos de contingência, seja qual for sua natureza. Por exemplo: uma aplicação, um processo de negócio, uma equipe técnica ou um ambiente físico. A partir dessa análise deve ser selecionada a melhor estratégia para se enfrentar cada desastre possível definido no plano de recuperação.

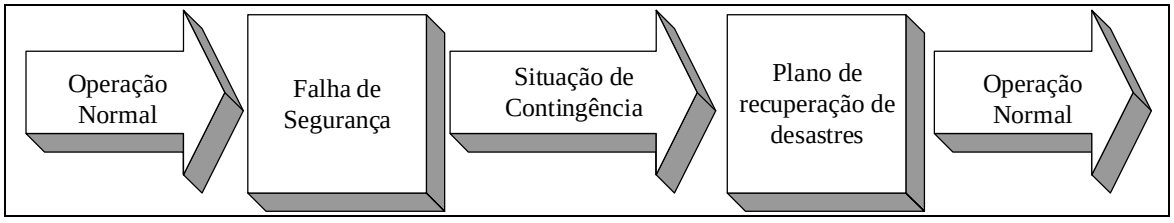

Figura 18. Aplicação do plano de recuperação de desastres

3.3 Execução

O grupo de processos de execução consiste nos processos definidos para realizar a implementação da política de segurança na instituição. Corresponde a etapa “Do” do modelo PDCA. Esta etapa é amplamente baseada nas diretrizes definidas na etapa de planejamento.

3.3.1 Mobilizar a equipe

Este processo tem como objetivo confirmar a disponibilidade dos recursos planejados e obter a equipe necessária para colocar os serviços no ambiente de produção da instituição.

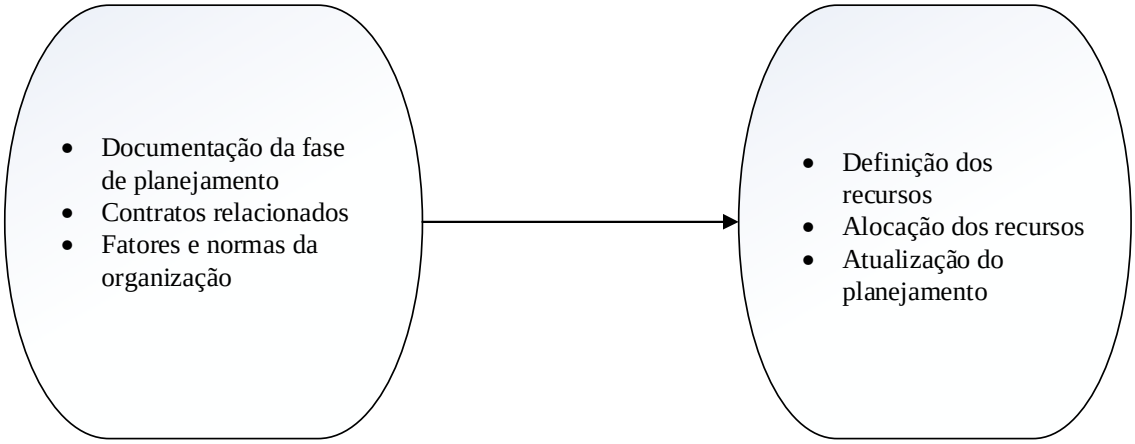

Figura 19. Mobilizar a equipe

Para atingir seus objetivos a instituição pode utilizar recursos externos ao seu corpo técnico. A ISO 27002 destaca alguns aspectos a serem observados em relação aos recursos humanos a serem contatados:

- O objetivo é assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com seus papéis, e reduzir o risco de furto ou roubo, fraude ou mal uso de recursos;
- As responsabilidades pela segurança da informação sejam atribuídas antes da contratação de forma adequada, nas descrições de cargos e nos termos e condições de contratação;
- Todos os candidatos ao emprego, fornecedores e terceiros sejam adequadamente analisados, especialmente em cargos com acesso a informações sensíveis;
- Todos os funcionários, fornecedores, terceiros, usuários de recursos de processamento da informação, assinem acordos sobre seus papéis e responsabilidades pela segurança da informação.

3.3.2 Divulgar a política de segurança

O objetivo deste processo é divulgar a política de segurança em conformidade com os objetivos estratégicos e com o plano de divulgação da segurança da informação.

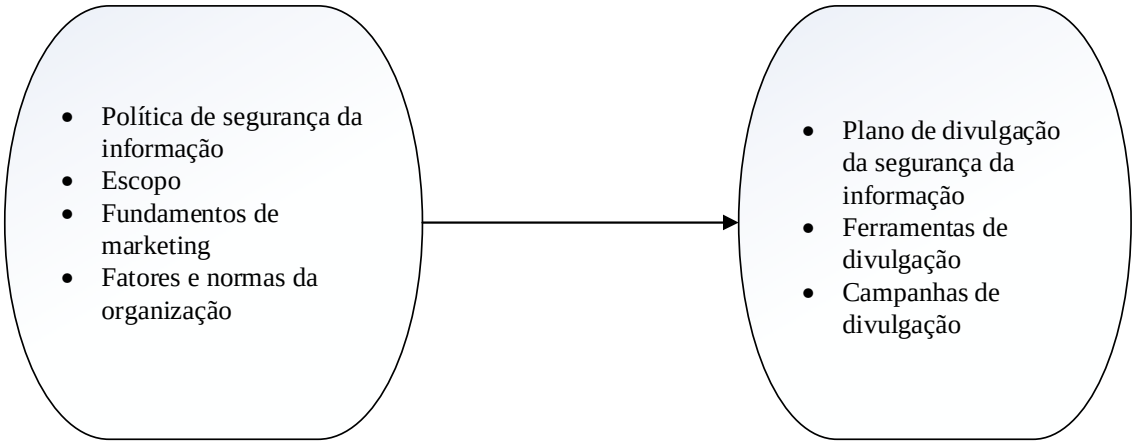

Figura 20. Divulgar a política de segurança

Após a formulação da política de segurança torna-se essencial a incorporação de ações estratégicas de comunicação para sua divulgação. Com o apoio e comprometimento das pessoas responsáveis pela informação fica mais fácil implementá-las e aprimorá-las dentro da instituição.

Nesse contexto, a elaboração de um plano de divulgação se faz necessária para definir as campanhas e ferramentas que serão utilizadas para treinar e educar as pessoas envolvidas. Desta forma a instituição espera prover um meio de aprendizado para que os riscos de incidentes de segurança atinjam um nível aceitável.

O plano de divulgação deve ser elaborado de forma a conter o detalhamento dos seguintes tópicos:

- Pesquisa inicial – deverá ser realizada uma pesquisa com todo o efetivo da instituição abordando o tema segurança da informação, com o objetivo de avaliar o atual nível de conhecimento e disseminar os principais conceitos.
- Página eletrônica de segurança da informação – esta página tem como propósito estabelecer uma plataforma de informação no meio digital em relação a segurança, assim como criar um canal de comunicação entre os usuários e os responsáveis pela implementação da política.
- Simpósio interno sobre segurança da informação – este evento visa divulgar as ações necessárias para a implementação da política de segurança no ambiente da instituição, bem como promover a conscientização das pessoas para a importância do tema de forma a obter um comportamento favorável para a sua entrada no ambiente de produção.
- Dia da segurança da informação – o gestor de cada departamento deverá agendar um dia de eventos de segurança da informação, contendo

palestras, mesa-redonda, fórum e jogos, para incentivar as boas práticas de segurança definidas na política e documentos complementares.

- Treinamento em segurança da informação – durante a vigência do plano de divulgação estarão disponíveis palestras em pelo menos três níveis de conhecimento para educar todo o corpo efetivo da instituição.
- Cartilha da segurança da informação – este documento deve ser distribuído para todo o corpo da instituição, devendo ser elaborado em linguagem simples e contendo algumas das principais práticas de segurança desejáveis.
- Envio de e-mails marketing sobre as notícias de segurança da informação – cada serviço implementado e cada mudança no ambiente de produção deve ser informada através de e-mail.
- Cartazes em lugares estratégicos sobre segurança da informação – estes cartazes devem abordar de forma simples e diretas práticas sobre os seguintes tópicos: senha, vírus, correio eletrônico, pirataria, reporte de incidentes, internet e política de segurança.

O plano de divulgação de segurança de informação do DECEA (Departamento de Controle do Espaço Aéreo), utilizado como referência para o presente trabalho, estabeleceu um grupo de “slogans” que serve de base para a elaboração dos cartazes, da cartilha e dos e-mails de marketing:

- “A informação é um ativo valioso para o sucesso da missão de sua instituição. Contribua, proteja este ativo.
- A internet é uma porta de entrada que pode ocasionar acesso indevido e vazamento de informações. Utilize-a de forma segura!!!
- Atenção às mensagens de Correio Eletrônico com assuntos importantes para o seu trabalho. Correntes, piadas, cartões... Delete esta idéia!!!
- Conhecer os riscos é o primeiro passo para planejar a continuidade operacional dos processos de sua área.
- Não deixe que toda a proteção oferecida por sua instituição seja colocada em risco. Proteja o seu computador portátil ou estação de trabalho.
- Otimize o seu tempo, utilize somente as informações necessárias para o desempenho de suas funções.
- Prevenir é muito melhor que remediar. Armazene as informações referentes ao seu trabalho na rede.
- Quantas pessoas possuem a chave de sua casa? E quantas têm a sua senha de acesso. Proteja-se.
- Riscos, falhas e incidentes de segurança da informação podem ser evitados com a sua ajuda. Como? Reportando na página de segurança da informação da instituição.

- Evite que o e-mail jogue contra você. Fique atento a arquivos grandes, suspeitos e adote boas práticas de uso.
- Não deixe que um vírus de computador acabe com o trabalho de uma semana inteira. Utilize o antivírus antes de abrir arquivos de mídias removíveis.
- Não seja surpreendido pela presença de programas de computadores irregulares. Instale apenas programas legais autorizados." [PCA_7-18, 2012]

O plano de divulgação será disponibilizado para todos os gestores de departamento, o qual deve indicar quais colaboradores devem participar de cada treinamento ou palestras disponíveis.

A instituição manterá o plano e as campanhas de divulgação atualizadas:

- As ferramentas como os e-mails de marketing e a página eletrônica de segurança da informação persistirão mesmo após a implementação da política de segurança no ambiente de produção.
- A cartilha de segurança deve ser revisada e distribuída a cada ano.
- Novos cartazes devem ser elaborados sempre que existir uma mudança significativa no ambiente de produção.
- Novas pesquisas devem ser realizadas para medir o grau de conhecimento sobre as políticas implementadas.
- Deve ser criada e revisada semestralmente uma agenda contendo a programação de treinamentos e palestras disponíveis no período.

3.3.3 Orientar e gerenciar a execução

É o processo que consiste na realização do trabalho definido na fase de planejamento para atingir os objetivos da instituição.

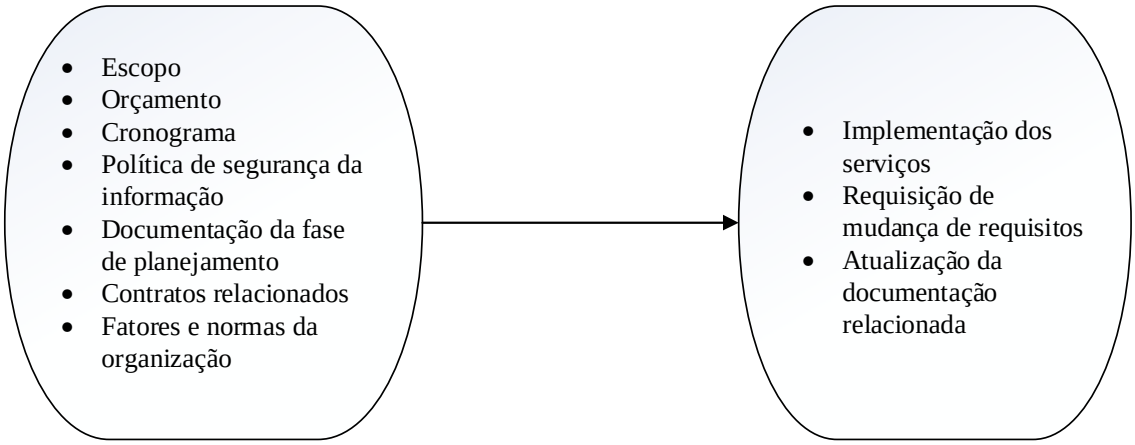

Figura 21. Orientar e gerenciar a execução

As principais atividades desta fase são:

- Executar as atividades previstas no planejamento.
- Implementar os padrões e os métodos desejados.
- Gerenciar fornecedores.
- Obter, gerenciar e usar recursos, inclusive softwares, materiais, ferramentas, equipamentos e instalações.
- Estabelecer e gerenciar os canais de comunicação, tanto externos quanto internos à equipe técnica.
- Gerar informações sobre o andamento da implementação.
- Fazer previsões e correções nos custos, no cronograma e no planejamento.
- Gerenciar riscos e implementar respostas aos riscos.
- Emitir solicitações de mudanças nos requisitos.

A nova política de segurança entrará em produção de forma que seus serviços estejam alinhados com os requisitos e com os objetivos da organização. Para atingir estas diretrizes os gestores devem seguir boas práticas referentes à gestão de mudança; à gestão de configuração e ativo de serviço; à gestão do conhecimento; à gestão de liberação e implantação; à gestão de validação e avaliação do serviço.

O gerenciamento de mudanças para as operações de TI é fundamental para melhorar a disponibilidade, o desempenho e o rendimento. Seus principais objetivos são minimizar o impacto da mudança, ter sucesso na primeira tentativa e diminuir os riscos da implementação. Esta abordagem vai gerar retorno financeiro direto para a instituição, proporcionando realização antecipada de benefícios (ou remoção de riscos), com economia de tempo e dinheiro. A gestão de mudança é considerada essencial para manter o equilíbrio necessário entre a necessidade de mudar e o impacto da mudança.

O objetivo da gestão do conhecimento é desenvolver uma melhor gestão de tomada de decisão, garantindo que informações confiáveis e seguras estejam sempre disponíveis. Para isto o gestor deve saber quem está usando o serviço, o estado atual deste serviço na instituição, quais as dificuldades enfrentadas pelos usuários e os benefícios esperados depois de concluída a implementação. A gestão do conhecimento é especialmente significativa dentro da transição para a nova política de segurança, já que o seu conhecimento relevante e adequado é um dos elementos-chave para o sucesso da sua implementação.

A gestão de configuração e ativo de serviço tem como objetivo principal reunir a informação necessária, de forma não redundante, dos componentes de TI e de como eles se relacionam. A razão para isto é assegurar que a informação relevante esteja disponível para todos os outros processos da implementação da política de segurança. Essa gestão visa obter uma base sólida para o gerenciamento de incidentes, gerenciamento de problemas e gerenciamento de mudanças para possibilitar a liberação dos serviços de forma segura e dentro do cronograma previsto. Os gestores devem verificar se os registros de configuração estão coerentes em relação à infraestrutura e

corrigir eventuais distorções. Devem proteger a integridade dos ativos de serviços e itens de configuração ao longo de seu ciclo de vida e fornecer informações precisas para apoiar a gestão de negócios e serviços.

O gerenciamento de liberação e implantação deve desenvolver a capacidade de testar, entregar e liberar para a produção os serviços especificados pela nova política de segurança. Estas práticas visam garantir que todo o novo hardware ou software seja identificável, seguro, autorizado e que suas versões instaladas sejam testadas. Os pacotes de liberação devem ser instalados, testados e implementados de forma eficiente e as habilidades e os conhecimentos devem ser transferidos para a operação e para o pessoal de apoio. Os serviços novos ou alterados precisam atender aos níveis de excelência desejados.

O objetivo da validação e avaliação é garantir que um serviço irá fornecer o valor e os resultados esperados pela organização, contribuindo para a garantia da qualidade. A realização de testes de validação é vital no gerenciamento de uma nova política de segurança e tem sido muitas vezes o diferencial entre serviços implementados de maneira eficiente e ineficiente. Se os serviços não são testados de forma criteriosa então a sua introdução no ambiente operacional trará aumento nos incidentes, como falhas em elementos de serviço e desencontros entre o que se queria e que foi entregue. Outra consequência da ausência de uma gestão de validação é o acréscimo em custos, uma vez que os erros são mais caros para corrigir na produção do que se encontrados em ambiente de testes.

Por exemplo, na implementação do serviço de controle de acessos haverá um planejamento definido pelo gestor responsável, onde serão avaliados os recursos humanos, os equipamentos, o software necessário, as autorizações e as licenças. A equipe formada será avaliada quanto à necessidade de capacitação e treinamento. Será definido o ambiente e quais testes são necessários para avaliar de forma adequada os requisitos e o desempenho. Caso a avaliação seja positiva, o serviço será liberado para a produção, tendo a aprovação do gestor competente. Depois de instalado no ambiente operacional da instituição o serviço de controle de acessos passará por mais avaliações de forma a medir se o desempenho na produção não apresenta distorção em relação ao desempenho em ambiente de testes. Caso necessário, serão efetuadas ações corretivas ou alteração de requisitos, sendo que sua documentação e seus procedimentos devem ser revisados de acordo. O conhecimento adquirido deve ser difundido para o corpo técnico e quando necessário para toda a instituição.

A implementação dos demais serviços definidos na política de segurança da informação devem seguir as mesmas diretrizes definidas neste processo e na fase de planejamento.

3.4 Monitoração e Controle

O grupo de processos de monitoração e controle consiste nos processos definidos para acompanhamento, revisão e ajuste dos serviços implementados pela política de segurança. Esta fase corresponde às etapas “Check” e “Act” do modelo

PDCA, incluindo a coleta, a medição e a avaliação da medição, com o objetivo de efetuar melhorias nos processos.

O monitoramento fornece a instituição uma compreensão clara do estado das mudanças implementadas, de forma a identificar áreas que possam requerer atenção especial.

O controle é baseado em ações corretivas e preventivas para definir as ações necessárias para se atingir o desempenho planejado.

Algumas atividades realizadas nessa etapa:

- Monitoramento dos diversos controles implementados, medindo sua eficiência e propondo mudanças nas variáveis que afetam o nível de risco do negócio;
- Projetar o retorno do investimento, por meio de medições objetivas que permitam avaliar os resultados alcançados e viabilizar novas demandas;
- Garantir a adequação do negócio às regras e padrões instituídos;
- Manter plano de recuperação de desastres que garantam a continuidade operacional do negócio;
- Administrar os controles implementados e estar preparado para a adequação em virtude de mudança de cenário ou variáveis internas e externas;
- Atualizar o Plano de Segurança pelo menos uma vez ao ano ou em período menor caso necessário, adequando-o às necessidades da instituição e à evolução tecnológica.

3.4.1 Controlar os custos

Processo que controla e atualiza o orçamento durante a implementação dos serviços definidos na fase de planejamento. Também gerencia as mudanças necessárias que surgirem na fase de execução.

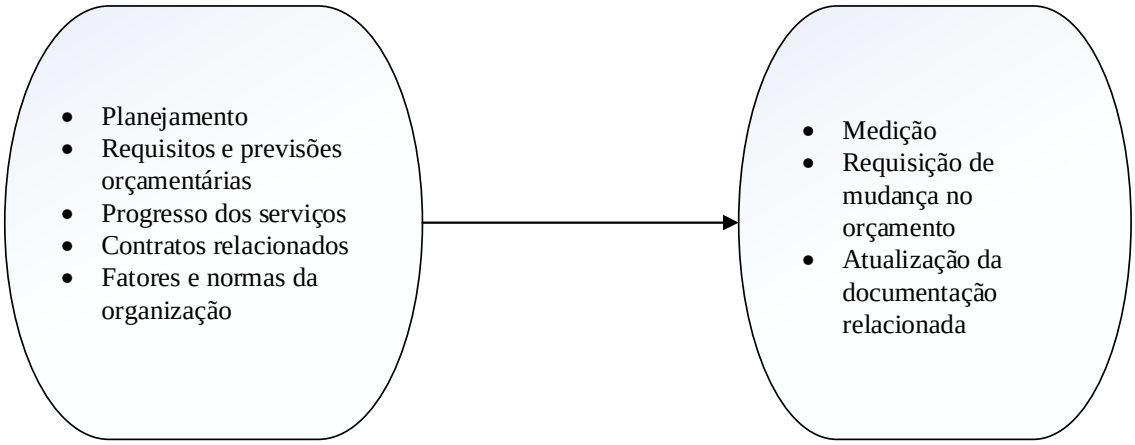

Figura 22. Controlar os custos

A atualização do orçamento requer o registro dos custos reais gastos até a data. É essencial a comparação entre o custo orçado e o realizado. Os relatórios de desempenho devem apresentar as medições realizadas em comparação ao orçamento inicial. Acréscimos e alterações devem ser analisados, aprovados e documentados.

3.4.2 Controlar o escopo

Controla o escopo definido na fase de planejamento e gerencia as mudanças feitas na fase de execução ou na operação normal dos serviços.

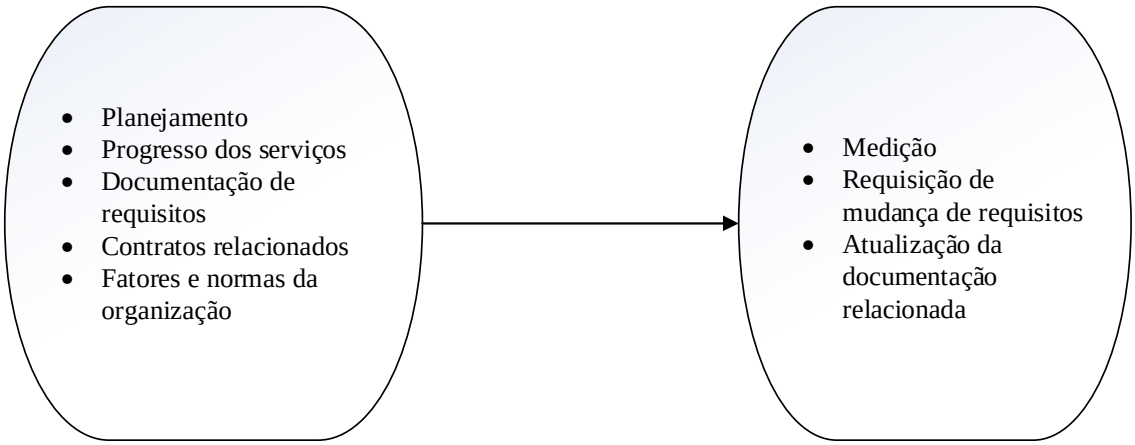

Figura 23. Controlar o escopo

Um cuidado essencial na gestão da política de segurança é o controle de solicitações de mudança ou de inclusão de funcionalidades. Estas solicitações devem ser analisadas de forma criteriosa de forma a impedir um desvio de foco e um aumento improdutivo do escopo. Os gestores devem avaliar o impacto financeiro, o tempo necessário e o benefício que cada mudança gerará para a instituição. As mudanças devem ser discutidas, aprovadas e documentadas por meio de formulários padronizados.

3.4.3 Controlar o cronograma

É o processo que controla o progresso dos serviços em implementação em relação ao que foi planejado. Também gerencia as mudanças feitas na fase de execução.

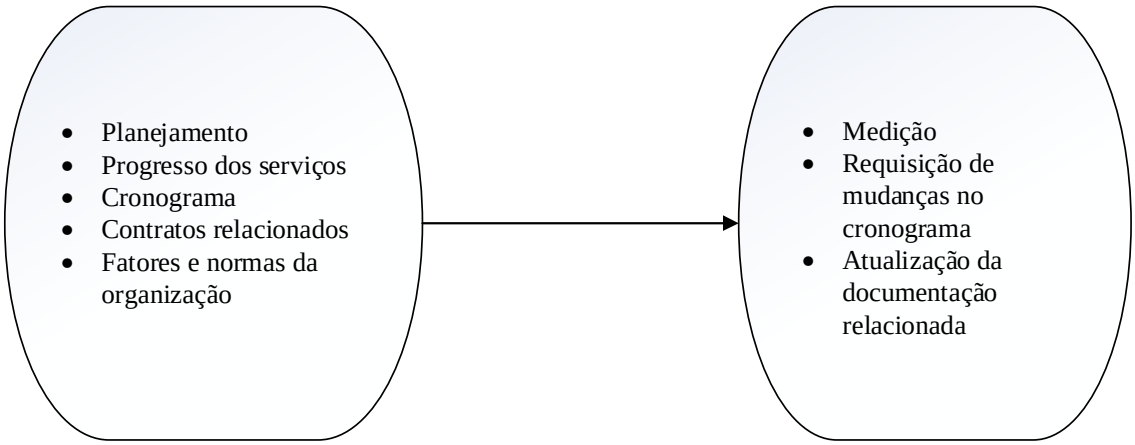

Figura 24. Controlar o cronograma

Uma parte importante do controle de prazos é definir qual a melhor ação corretiva para cada situação ou atraso. Por exemplo, um grande atraso em uma atividade que não esteja no caminho crítico pode ter impacto irrelevante na conclusão das tarefas, enquanto que um pequeno atraso em uma atividade crucial pode exigir ação imediata.

A instituição utilizará software de gerenciamento de projetos Microsoft Project de forma a facilitar a comparação entre os prazos programados e os realizados. Uma cópia atualizada do cronograma deverá ser disponibilizada nos relatórios de acompanhamento e desempenho destinados ao escritório de projetos e à alta gerência.

3.4.4 Implementar métricas e indicadores

É o processo que define quais medições e indicadores devem ser implementados, visando o desempenho planejado e a melhoria contínua dos processos.

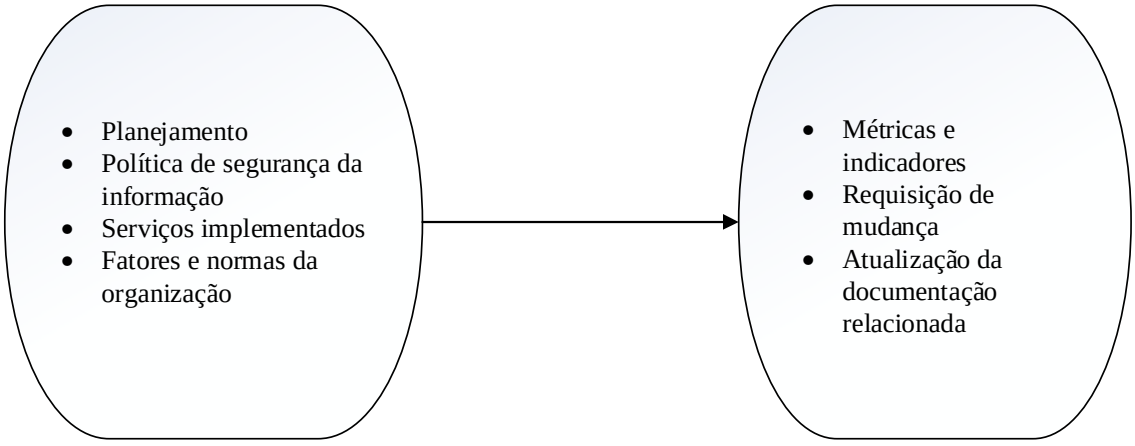

Figura 25. Implementar métricas e indicadores

Nesta etapa os gestores devem utilizar o planejamento atualizado, a política de segurança, as normas da instituição e sua expertise para a definição dos seguintes fatores:

- Serviços que serão objeto de medição.

- Técnicas que serão utilizadas para a coleta de dados.
- Técnicas que serão utilizadas para a análise dos dados coletados.

Por exemplo, um serviço que será medido é referente às cópias de segurança ou “backups”. Este serviço visa restaurar dados, arquivos, mensagens de correio eletrônico, imagem de estações de trabalho, entre outros.

Para medir a eficiência deste serviço o ideal é a criação de um indicador que avalie aspectos relevantes como integridade dos dados e tempo de restauração. As métricas devem ser estabelecidas de forma a atender os padrões definidos no planejamento. Por exemplo, a partir do recebimento da solicitação de um usuário a cópia de segurança deve ser disponibilizada seguindo os parâmetros de tempo definidos:

- Para um arquivo a restauração deve ser executada em até duas horas.
- Para as mensagens de correio eletrônico a restauração deve ser executada em até quatro horas.
- Para a imagem de uma máquina a restauração deve ser executada em até oito horas.

Os tempos envolvem não só o processo de restauração em si, mas todo o período necessário para a conclusão da tarefa, que inclui desde a mobilização dos recursos até o registro de execução do serviço.

A definição de métricas e indicadores permite não apenas a monitoração e o controle dos serviços, mas também a sua melhoria. A partir de uma análise dos dados coletados é possível adotar medidas corretivas de forma a aperfeiçoar os processos, conforme a representação a seguir:

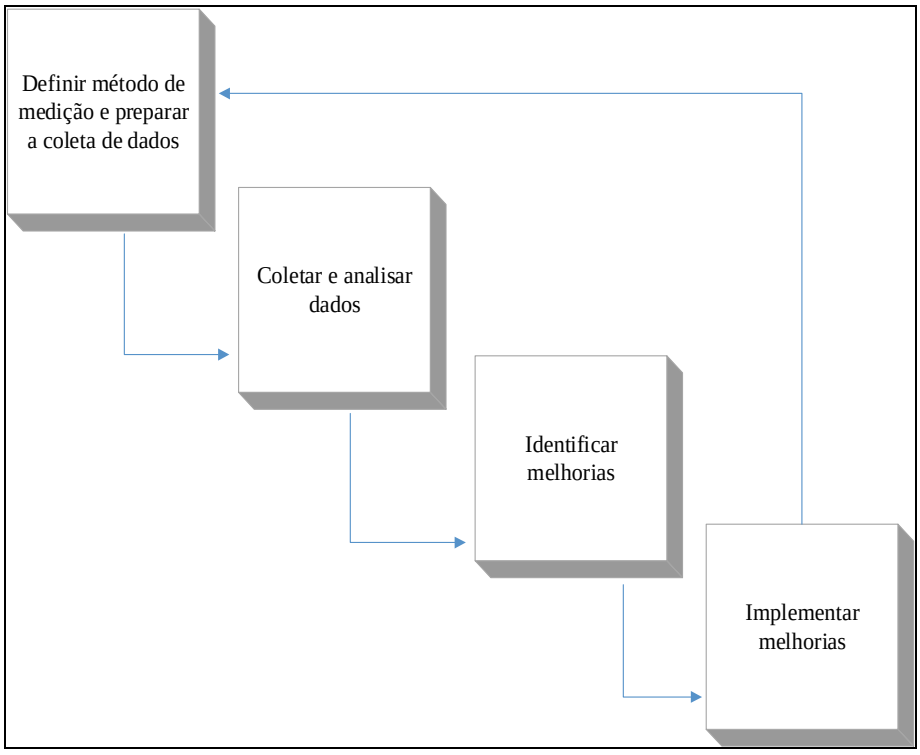

Figura 26. Implementação prática de métricas e indicadores

3.4.5 Reportar desempenho

É o processo de coleta e distribuição de informações sobre o desempenho, as medições e as previsões sobre o progresso dos serviços da política de segurança.

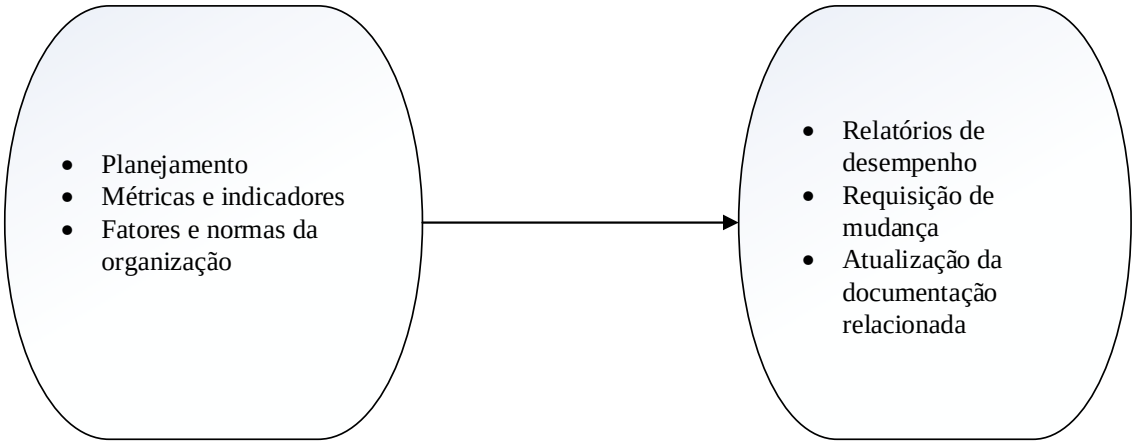

Figura 27. Reportar desempenho

A partir das métricas e indicadores criados os gestores reportarão o desempenho dos serviços através de relatórios periódicos. Por exemplo, em relação às cópias de segurança pode ser feita a medição do número de restauração das cópias com sucesso em relação ao número total de solicitações. A figura a seguir mostra uma sugestão de gráfico para indicar o desempenho deste serviço.

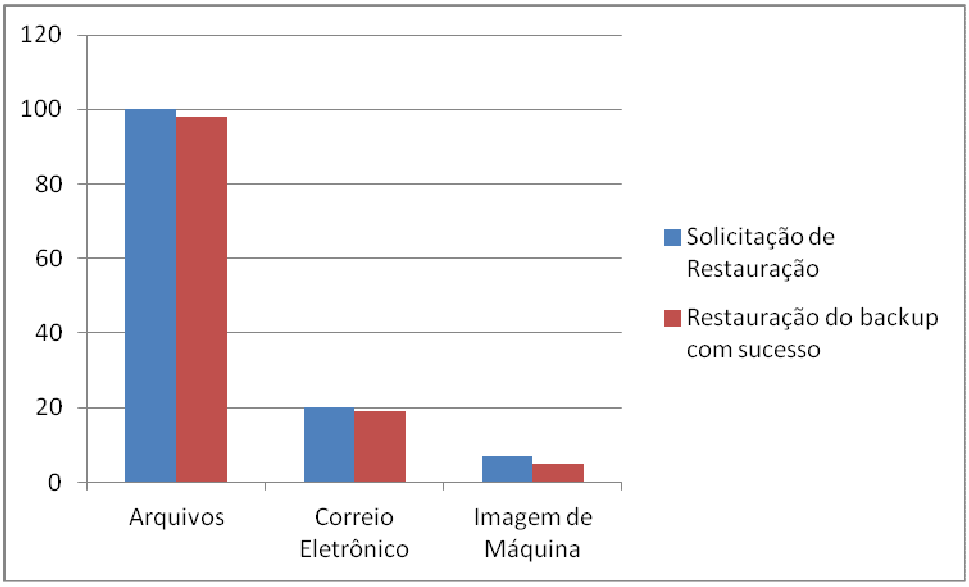

Figura 28. Desempenho do serviço de cópias de segurança ou "backups"

Em relatórios direcionados a alta gerência ou a diretoria é mais eficiente à apresentação de indicadores, que podem ser compreendidos de forma mais rápida e intuitiva. Utilizando os mesmos dados do gráfico anterior segue a representação de um indicador para a análise de sucesso de backup. Este indicador, criado de forma

exemplificada, apresenta o desempenho do serviço através de porcentagem, sendo o número 1 equivalente a 100 %.

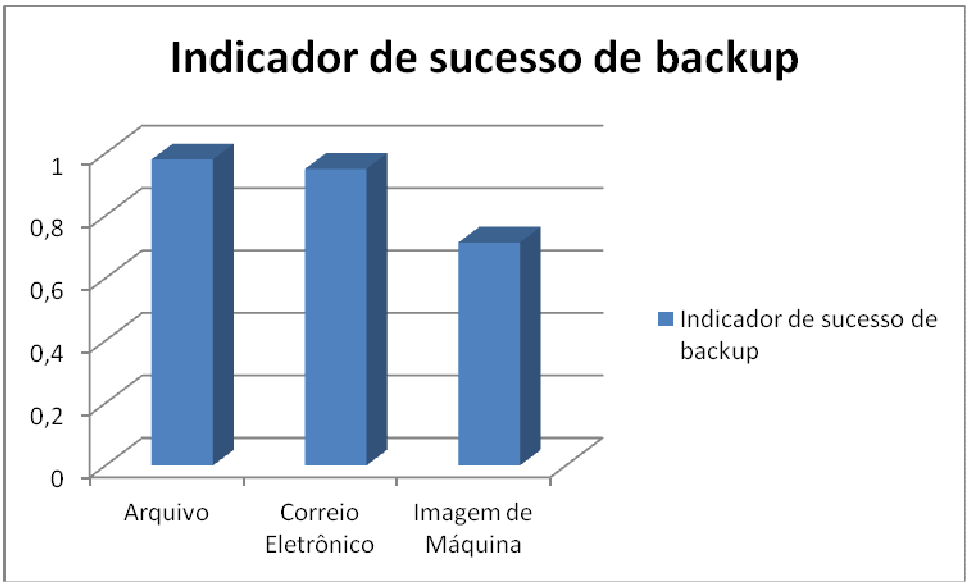

Figura 29. Indicador de sucesso do serviço de cópias de segurança ou "backups"

A partir da figura anterior é possível verificar que o desempenho das cópias de segurança da imagem de máquinas encontra-se em nível baixo. É aconselhável, em uma situação como esta, que os gestores solicitem mais informações para entender as causas deste desvio. Após análise desses dados e das informações coletadas podem ser definidas as ações corretivas necessárias para que o serviço atinja o nível de excelência definido no planejamento.

3.4.6 Monitorar e controlar os riscos

Este processo é responsável pelo acompanhamento dos planos de segurança, monitoramento dos riscos identificados, identificação de novos riscos e avaliação do impacto destes riscos na instituição.

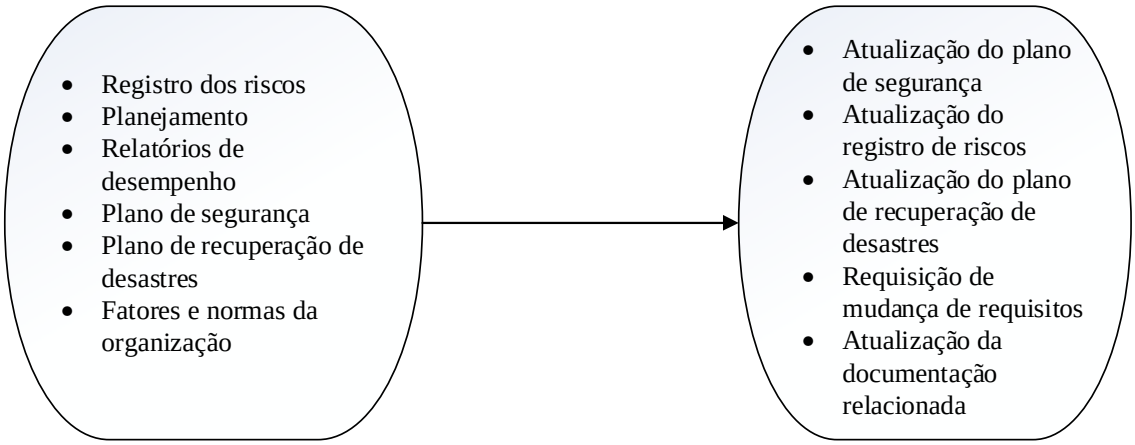

Figura 30. Monitorar e controlar os riscos

Segundo o Gartner alguns cuidados essenciais para o gerenciamento dos riscos são:

- Não criar expectativas irreais.
- Definir os controles de risco direcionados aos problemas principais é sempre mais eficaz do que tentar resolver todos os problemas possíveis.
- Planejamento ruim é uma grande fonte de improdutividade.

Outro cuidado nesta etapa é em relação aos planos de contingência que não podem ser testados. Procedimentos definidos nestes planos de segurança muitas vezes só são colocados em prática quando da ocorrência de uma falha de segurança. Por exemplo, o plano de recuperação de desastres aborda a recuperação de servidores em caso de incêndio, logicamente esta situação não será testada previamente. Desta forma sempre que uma situação de contingência é aplicada na produção os planos e procedimentos devem ser atualizados e corrigidos de acordo com a situação enfrentada.

A atualização dos planos de segurança e da documentação gerada no planejamento é outro fator que determina o sucesso de uma política de controle de riscos. Muitas vezes as situações são contornadas de forma diferente da inicialmente prevista, porém não há atualização dos procedimentos pertinentes. Nestes casos uma falha de segurança que se repita poderá ser tratada conforme um procedimento desatualizado, gerando perda de produtividade.

As situações de risco devem ser periodicamente discutidas e analisadas pelos gestores responsáveis e pelo corpo técnico, o gerenciamento dos riscos é mais eficiente quando praticado de forma mais frequente.

4 A Política de Segurança da Informação

Vide Anexo I

5 Resultados esperados

Diminuir a vulnerabilidade, controlar os riscos, estabelecer um procedimento único para concessão e retirada de acessos automática, retirar processos manuais, instituir a cultura da segurança nas rotinas diárias, são alguns dos resultados esperados.

Estabelecer um plano de continuidade de negócios, com o objetivo de descrever as medidas a serem tomadas pela instituição, para fazer com que seus processos vitais funcionem plenamente o mais rápido possível.

Instituir a gestão de incidentes de segurança para propiciar a melhoria dos sistemas e processos.

Instituir a auditoria de sistemas para verificar a eficácia dos controles e procedimentos de segurança existentes, a eficiência dos processos em uso, a correta utilização dos recursos disponíveis, assessorando a administração na elaboração de planos e definição de metas, apontando deficiências e irregularidades que possam comprometer a segurança e o desempenho organizacional.

Alinhar a Segurança de TI com a Segurança do Negócio e assegurar que a Informação seja gerenciada de forma eficaz em todos os Serviços.

Para que a instituição atinja os resultados esperados é necessário um acompanhamento criterioso dos serviços. Por exemplo, a organização deve desenvolver um “check-list” para certificar que a política de segurança atingiu os objetivos planejados. Os seguintes itens não esgotam as possibilidades, porém cobrem a maior parte dos serviços definidos na política de segurança:

- A política de segurança pode ser facilmente acessada por todos os funcionários.
- A política de segurança é revisada no mínimo anualmente.
- Consultas frequentes são realizadas nas principais áreas de negócio da instituição para verificar a necessidade de novos requisitos de segurança.
- A avaliação de risco é documentada e os resultados têm colaborado com o desenvolvimento da política.
- Os funcionários estão cientes e treinados no uso da política através de cursos e treinamentos.
- O Plano de segurança foi posto em prática, incluindo a identificação, classificação e impacto dos riscos.
- Controles de acesso para áreas restritas têm sido documentados, aprovados e estão sujeitos à atualização constante.
- Os procedimentos para a proteção e monitoramento do equipamento externo a instituição estão documentados e aprovados.
- Os procedimentos para o descarte e a reutilização de mídias removíveis foram aprovados.
- É possível demonstrar que os procedimentos operacionais estão sendo seguidos.

- São realizados planos e campanhas de sensibilização (e-mails, cartazes, conteúdo da intranet, entre outros).
- Os administradores de rede estão cientes da política de segurança e seguem seus procedimentos.
- Existem registros que podem indicar que cópias de segurança estão disponíveis e que os procedimentos de recuperação foram testados.
- Uma política de controle de correio eletrônico foi aprovada e implementada.
- Sistemas de informação da organização não podem ser acessados sem registro que possa indicar o usuário do serviço.
- Registros de configuração e testes devem indicar que as comunicações wireless são protegidas com o mesmo nível de segurança das comunicações por meio físico de transmissão.
- Controle de mudanças é documento em registros, contendo a aceitação e a documentação de teste, planejamento e migração.
- Os funcionários com funções de segurança da informação ou responsabilidades acerca de informações essenciais à instituição assinaram um termo afirmando que eles entendem seus papéis, responsabilidades e a política de segurança.

Caso as afirmações anteriores e outras que possam figurar no “check-list” possam ser avaliadas de forma positiva é possível concluir que os resultados esperados com a implementação da política de segurança da informação foram atingidos.

6 Conclusão

Uma boa política de segurança da informação é aquela que atende às necessidades e particularidades de cada instituição ou empresa e não aquela que contenha todos os requisitos e boas práticas da literatura disponível. Ela deve conter aqueles requisitos suficientes para garantir que atenderá os níveis de segurança exigidos pela criticidade dos dados que se deseja proteger e disponibilizar, aplicando-se os métodos e recomendações de boas práticas que a maturidade daquele ambiente suporte e garanta sua continuidade.

Neste trabalho elaborarmos uma política de segurança da informação ampla o suficiente para atender às necessidades da instituição analisada, porém insuficiente para ser aplicada numa grande empresa de T.I. À medida que a maturidade avança novas versões devem ser pensadas e implementadas, dentro da metodologia e arquitetura definidas, de modo muito menos traumático como é a primeira implementação de tal política.

As fases e os controles da implementação aqui discutidos, com metodologia de gerência de projetos recomendados pelo PMBOK, os métodos de análise de processos com base no PDCA e as boas práticas de transição de serviços previstas pela ITIL e demais literaturas sobre o assunto ainda que não contemplados na sua amplitude acreditamos ser o mais indicado pois evita a personificação dos processos, as decisões empíricas e pessoais que poderiam ficar à mercê das mudanças políticas ou realocação dos recursos envolvidos.

Além dos aspectos técnicos e boas práticas recomendadas pelas instituições pesquisadas, levou-se em consideração para a elaboração das práticas aqui propostas, o fator humano como um risco relevante, senão o principal. Some-se a isto a cultura organizacional do ambiente público, com características extremamente conservadoras que podem potencializar estes aspectos. Características naturais, como resistência a mudanças de comportamento, sensação de exclusão do processo, falta de compreensão do objetivo, desmotivação, devem ser mitigados ou eliminados antes que se tornem problemas.

Este trabalho, embora elaborado com o foco numa certa instituição pública, pode servir de orientação para quem pretende iniciar um processo de implementação de uma política mínima de segurança da informação, pois não há a necessidade de reconstruir os processos, basta seguir os processos aqui identificados e adaptar ao momento e ao ambiente onde se pretende aplicar.

Assim, acreditamos ter atingido o objetivo inicial ao propor um método prático para a implementação de uma política de segurança da informação, ao mesmo tempo que propõe um modelo de documento (anexo I) que poderá ser adaptado, evoluir e ser detalhado por meio de documentos e normas adicionais, num processo contínuo e necessário para que se tenha a política de segurança da informação implementada como um projeto e sustentada como um processo de gestão, garantindo os requisitos básicos de segurança aqui estudados.

7 Referências

Heiser, Jay (2012). Planning Information Security and Risk Management Policy. Gartner, http://www.gartner.com/.

Mcmillan, Rob (2012). How to craft and plan Your Security Policy. Gartner, http://www.gartner.com/.

Scholtz, Tom (2014). Prepare for the Security Implications of Engagement Initiatives. Gartner, http://www.gartner.com/.

Mcmillan, Rob (2013). Use a Structured Approach to Communicate Your Security Strategy. Gartner, http://www.gartner.com/.

Sêmola, Marcos (2003) “Gestão da Segurança da Informação: uma visão executiva”, Editora Campus, RJ, Brasil.

Moreira, Nilton (2001) “Segurança Mínima: Uma visão corporativa da segurança de informações”, Editora Axcelbooks, RJ, Brasil.

ABNT NBR ISO 27002:2005 Tecnologia da informação – Técnicas de segurança – Código de prática para gestão da segurança da informação.

ABNT NBR ISO 27001:2006 Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação — Requisitos

ABNT NBR ISO 27004:2010 Tecnologia da informação – Técnicas de segurança – Gestão da segurança da informação — Medição

PMBOK quarta edição (2008) “Um guia do conhecimento em gerenciamento de projetos (Guia PMBOK)”, Project Management Institute, Pensilvânia, Estados Unidos.

ITIL Version 3 (2007) “Service Transition”, Office of Government Commerce, Reino Unido.

PCA7-18 (2012) “Plano de Divulgação da Informação do Departamento de Controle do Espaço Áereo” Ministério da Defesa e Comando da Aeronáutica, Brasil..