UNIVERSIDADE ESTADUAL DE MARINGÁ
CENTRO DE TECNOLOGIA
DEPARTAMENTO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

DAIANE MARCELA PICCOLO

Estratégia de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis

Maringá
2013

DAIANE MARCELA PICCOLO

Estratégia de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação do Departamento de Informática, Centro de Tecnologia da Universidade Estadual de Maringá, como requisito parcial para obtenção do título de Mestre em Ciência da Computação.

Orientador: Prof. Dr. Sérgio Roberto Pereira da Silva

Maringá
2013

Dados Internacionais de Catalogação-na-Publicação (CIP)
(Biblioteca Central - UEM, Maringá – PR., Brasil)

P591e

Piccolo, Daiane Marcela
Estratégia de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis / Daiane Marcela Piccolo. -- Maringá, 2013.
108 f. : il., color., figs., tabs.

Orientador: Prof. Dr. Sérgio Roberto Pereira da Silva.
Dissertação (mestrado) - Universidade Estadual de Maringá, Centro de Tecnologia, Departamento de Informática, Programa de Pós-Graduação em Ciência da Computação, 2013.

1. Aplicações móveis. 2. Segurança da informação. 3. Politicas de segurança da informação. I. Silva, Sérgio Roberto Perreira da, orient. II. Universidade Estadual de Maringá. Centro de Tecnologia. Programa de Pós-Graduação em Ciência da Computação. III. Titulo.

CDD 21.ed. 005.3

AHS

FOLHA DE APROVAÇÃO

DAIANE MARCELA PICCOLO

Estratégia de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação do Departamento de Informática, Centro de Tecnologia da Universidade Estadual de Maringá, como requisito parcial para obtenção do título de Mestre em Ciência da Computação pela Banca Examinadora composta pelos membros:

BANCA EXAMINADORA

Profa. Dra. Elisa Hatsue Moriya Huzita
Universidade Estadual de Maringá – DIN/UEM

Profa. Dra. Tania Fatima Calvi Tait
Universidade Estadual de Maringá – DIN/UEM

Prof. Dr. Marcelo Morandini
Universidade de São Paulo – EACH/USP

Aprovada em: 06 de dezembro de 2013.
Local da defesa: Sala 102, Bloco C56, *campus* da Universidade Estadual de Maringá.

AGRADECIMENTOS

Agradeço primeiramente a todos os professores e colaboradores do Programa de Pós-Graduação em Ciência da Computação (PCC-UEM) que contribuíram para a minha formação. Não posso deixar de fazer um agradecimento especial aos meus orientadores Prof. Dr. Sérgio Roberto Pereira da Silva e Profa. Dra. Tania Fatima Calvi Tait que instigaram, auxiliaram e acreditaram no desenvolvimento deste trabalho. Também agradeço aos meus companheiros de estudo, por terem compartilhado essa jornada, e a Maria Inês Davanço, cuja simpatia e eficiência provam que existem pessoas que fazem a diferença em nossas vidas.

Um agradecimento especial ao meu esposo Claudio Munhoz pela paciência e companheirismo.

Estratégia de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis

RESUMO

Com os avanços nas áreas de telecomunicação, computação e miniaturização de computadores, novos produtos tecnológicos foram desenvolvidos e rapidamente tornaram-se pontos-chaves para as novas abordagens de comunicação e estratégias de negócios. E com a situação atual do mundo dos negócios ao qual se tem o crescimento do uso de tecnologias, para diminuir custos e aumentar a produtividade, empresas de desenvolvimento de *software* têm portado suas aplicações para plataformas móveis atendendo o mercado atual. No entanto, à medida que as organizações adquirem as soluções móveis, novos atributos e funcionalidades são identificados para serem apropriados tanto pelo desenvolvimento de *software* para dispositivos móveis como pela segurança da informação, pois novos riscos e desafios incitaram a empresa e gerentes. Entre esses novos riscos e desafios há a necessidade de uma gestão de segurança da informação que aborde as peculiaridades das empresas do contexto de desenvolvimento de software para dispositivos móveis. Neste trabalho, é apresentada uma estratégia de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis que visa auxiliar a segurança da informação protegendo seus principais ativos. Esta estratégia envolve um arcabouço com temáticas que incluem a gestão de projetos, as tecnologias móveis e aspectos de segurança da informação, abordando elementos para garantir a segurança da informação tais como: interpretação da norma ISO 27001, definição do escopo do projeto, elaboração do SGSI, gerenciamento de risco, desenvolvimento e treinamento das normas e procedimentos de segurança e gestão de continuidade do negócio. A avaliação da estratégia seguiu os princípios da engenharia de software experimental sob uma perspectiva de gestores de segurança da informação.

Palavras-chave: Aplicações móveis, Segurança da Informação, Políticas de Segurança da Informação.

ABSTRACT

With advances in the areas of telecommunication, computing and miniaturization of computers new technology products were developed and quickly became key points to new approaches for communication and business strategies. And with the current state of the business world where you have the growing use of technology to reduce costs and increase productivity, software development companies have ported their applications to mobile platforms given the current market. However as organizations acquire mobile solutions, new attributes and features are identified to be suitable for both the development of software for mobile devices like the security of information, as new risks and challenges and urged the company managers. Among these new risks and challenges is the need for information security management to address the peculiarities of companies in the context of software development for mobile devices. This paper presents a strategy for information security in companies developing software for mobile devices that aims to assist information security protecting its main assets. The strategy involves a framework with themes that include project management, mobile technologies and aspects of information security, addressing elements to ensure the security of information such as the interpretation of the ISO 27001 definition of project scope, preparing the SGSI , survey and risk analysis, training and development of standards and procedures for security and business continuity management. The evaluation of the strategy followed the principles of software engineering from the perspective of experimental information security managers.

***Keywords*:** Mobile applications, Information Security, Information Security Policy

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CERT	*Computer Emergency Response Team*
CMMI	*Capability Maturity Model Integration*
CobiT	*Control Objectives for Information and Related Technology*
DOS	*Denial of Service*
EAP	Estrutura Analítica do Projeto
GPGPS	Grupo de Pesquisa de Gerenciamento de Projetos *de Software*
GPS	Gerenciamento de Projetos *de Software*
IP	*Internet Protocol*
MPS-BR	Melhoria de Processos do *Software* Brasileiro
MR-MPS	Modelo de Referência de MPS.BR
PDA	*Personal Digital Assistants*
PDCA	Plan-Do-Check-Act
PMI	*Project Management Institute*
Prince2	*Projetct in Controlled Environments*
SGSI	Sistema de Gestão de Segurança da Informação
SI	Sistema de Informação
SIGP	Sistema da Informação de Gerenciamento de Projetos
SM	Suporte e Manutenção
TI	Tecnologia da Informação

SUMÁRIO

Capítulo

1

Introdução

As empresas desenvolvedoras de software vivem num momento de convergência digital, ao qual um mesmo serviço ou produto está disponível em diversos meios digitais como celular, televisão, *Internet*, entre outros.

Para Cukierman *et al.* (2007), essas novas tecnologias são reputadas como fontes de mudanças radicais e, neste caso, constituem um cenário no qual transformam significativamente várias dimensões da vida moderna. Esse cenário, constituído de múltiplos processos de mobilidade, nasce da soma da computação, telecomunicação e tecnologia e é possibilitado pela conexão móvel.

Krotov e Junglas (2006) e Issac (2006) sustentam que, à medida que os dispositivos móveis foram amplamente adotados pelos indivíduos, as organizações também começaram a adotar esse tipo de tecnologia de diferentes formas. Atualmente, diversas empresas usam as tecnologias móveis para interagir com seus diferentes públicos-alvo como clientes, colaboradores, fornecedores ou acionistas, aproveitando-se da popularização dos telefones celulares, bem como de outros benefícios próprios da tecnologia, obtendo, assim, maior agilidade e produtividade.

Neste cenário, empresas de desenvolvimento de *software* têm portado suas aplicações para plataformas móveis. No entanto, à medida que as organizações adquirem as soluções móveis, novos atributos e funcionalidades são identificados para serem apropriados no desenvolvimento de *software* e na segurança da informação para dispositivos móveis. Esses novos atributos e funcionalidades também caracterizam o contexto móvel mudando até mesmo a maneira como a gestão de segurança da informação deve ser conduzida para garantir

a qualidade dos produtos.

Entretanto, para que empresas de desenvolvimento de software para dispositivos móveis alcancem o sucesso na implantação e no alinhamento estratégico de tecnologias móveis é necessário o emprego de medidas específicas de segurança da informação. Neste sentido, o presente trabalho apresenta uma estratégia de segurança da informação especificando diretrizes a serem seguidas no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança da informação nos projetos de desenvolvimento de software para dispositivos móveis contribuindo com o desenvolvimento de novas aplicações mais seguras.

1.1. Objetivos

O objetivo geral é apresentar uma estratégia de segurança da informação para empresas de desenvolvimento de software para dispositivos móveis com base nas normas ISO 27001, ISO 27002 e políticas de segurança da informação de empresas do setor de TI (Tecnologia da Informação). Desta forma, apoiar a empresa e gerentes sobre os fatores de segurança da informação no planejamento, execução e monitoramento de seus projetos.

1.2. Objetivos Específicos

Para alcançar o objetivo geral, é necessário atingir os objetivos específicos, que são:

- Definir os ativos da empresa que devem ser protegidos e principalmente, qual é o nível de segurança que cada ativo deve ter para que a mesma obtenha sucesso em seus projetos.
- Verificar se a hipótese (H0) “A estratégia de SI para empresas de desenvolvimento de software para dispositivos móveis é ineficiente para o contexto de desenvolvimento de software móvel” é refutada, e as hipóteses (H1)“Os elementos abordados na estratégia de SI para empresa de desenvolvimento de software para dispositivos móveis satisfazem com eficiência a segurança da informação de empresas do contexto móvel” e (H2) “A estratégia de SI para empresa de desenvolvimento de software para dispositivos móveis minimiza os impactos negativos de riscos identificados”, são afirmativas na opinião do grupo de gestores.

- Validar a estratégia de segurança da informação em empresas de desenvolvimento de *software* para dispositivos móveis.

1.3. Justificativa

Pesquisas em tecnologias e aplicações móveis têm crescido e se tornando uma das áreas multidisciplinares com maior representatividade nos últimos anos (Machado; Freitas, 2009; Fouskas *et.* 2005). E com a situação atual do mundo dos negócios ao qual se tem o crescimento do uso de tecnologias, para diminuir custos e aumentar a produtividade, com sistemas cada vez mais interligados cria-se então a necessidade de tornar esta tecnologia segura e confiável.

Neste cenário, modelos, metodologias ou estratégias de gestão envolvendo a segurança da informação para projetos de desenvolvimento de software para dispositivos móveis são alvos de pequena parte das pesquisas, deixando vasto espaço para estudos sobre o assunto. Como pode ser observado, a partir dos trabalhos de Wangham (2007), Boulhosa (2011) e Sima (2006), nos quais os mesmos tratam de segurança da informação em aplicações móveis a partir de ferramentas e protocolos específicos para implementação do software.

Apesar dessas metodologias integrarem aspectos de segurança, suas aplicações não são específicas para a gestão de segurança, ao qual envolva aspectos tanto dos requisitos físicos como lógicos da empresa. Embora uma empresa possa ter as melhores técnicas, softwares ou equipamentos para segurança, somente isso não é suficiente, uma vez que pessoas podem ser facilmente influenciadas, persuadidas, enganadas e convencidas a fornecer informações a pessoas não autorizadas a recebê-las.

Outra justificativa acerca da proposta de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis é que até 2014 o número de aplicativos disponível para *download* em *app stores* para *smartphones* e *tablets* saltará de 200, em 2012, para mais de 1,2 mil em 2014 (Gartner, 2013).

Nesse contexto, uma estratégia de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis é proposta visando definir etapas para subsidiar a empresa e os gerentes de projeto no planejamento, na coordenação, na cooperação, na execução do projeto e no desenvolvimento do *software* móvel.

Dada à relevância das aplicações móveis no cenário atual, na Universidade Estadual de Maringá (UEM) está sendo desenvolvido o projeto M-Aplic – Uma abordagem para gestão de projetos para aplicações móveis, com apoio da Fundação Araucária e como parte das atividades do Grupo de Pesquisa em Gestão de Projetos (GPGPS).

Assim, a estratégia aqui proposta contribui para que o gerente tenha uma visão sobre a segurança das informações, podendo planejar e acompanhar esse item imprescindível para aplicações móveis e podendo compor um dos elementos da abordagem M-Aplic no quesito segurança da informação.

1.4. Metodologia de Desenvolvimento

A metodologia utilizada para o desenvolvimento da proposta de dissertação é composta por quatro fases. Assim, para atender aos objetivos da proposta, é utilizada a metodologia apresentada na Figura 1.1.

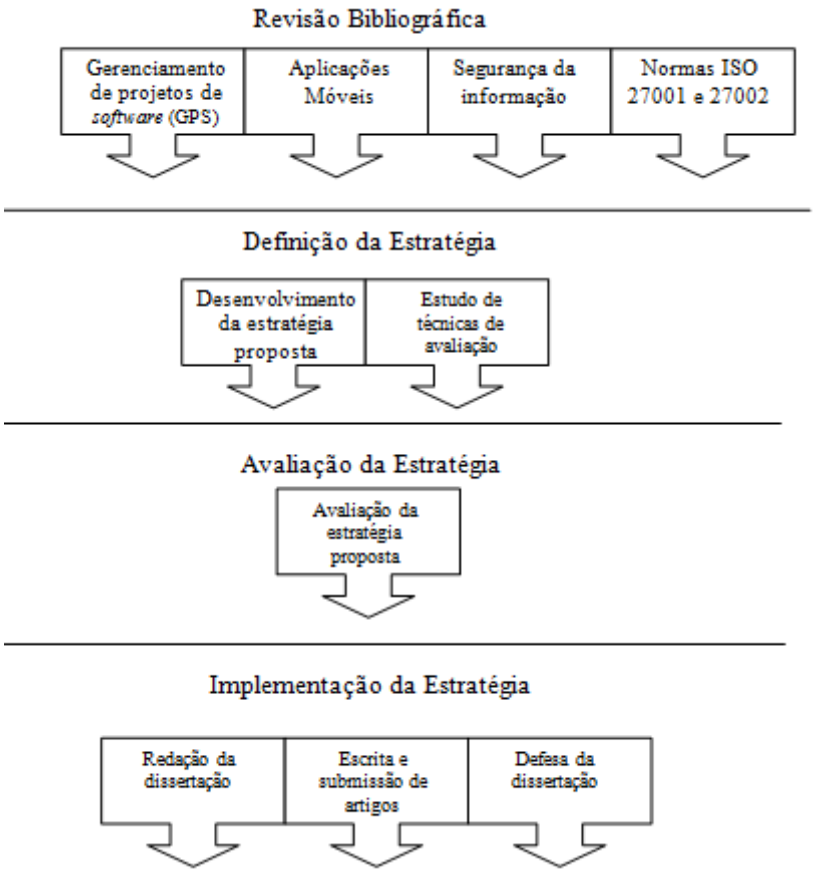

Figura 1.1: Etapas da metodologia de desenvolvimento da pesquisa

- **Revisão Bibliográfica:** envolve a revisão inicial da literatura, que teve como objetivo formar um referencial teórico consistente e visualizar o estado da arte.
- **Definição da Estratégia**: identifica, especifica e defini, com base na etapa anterior, os elementos necessários para uma estratégia de segurança da informação em ambiente de desenvolvimento de *software* para dispositivos móveis.
- **Avaliação da Estratégia:** verifica se a estratégia proposta satisfaz os objetivos de acordo com a avaliação por meio da engenharia de *software* experimental (Mafra e

Travassos, 2006).

- **Redação:** consiste na escrita da dissertação e do artigo, bem com a respectiva defesa da dissertação e submissão do artigo para um evento da área de engenharia de software.

1.5. Organização do Trabalho

Neste capítulo foram apresentados os propósitos e a motivação da proposta de elaboração de uma abordagem de estratégia de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis, bem como orientações sobre como o estudo será conduzido para alcançar o objetivo geral e os objetivos específicos.

O restante do trabalho encontra-se organizado da seguinte forma:

- **Capítulo 2 - Revisão bibliográfica:** apresenta os conceitos relevantes para o desenvolvimento deste trabalho, sendo eles: gerenciamento de projetos de software, computação móvel, dispositivos móveis, aplicações móveis, desafios no desenvolvimento das aplicações móveis, segurança da informação, gestão da segurança da informação e normas de segurança da informação.
- **Capítulo 3 - Bases da estratégia de segurança da informação:** aborda os elementos que subsidiaram a elaboração do arcabouço da estratégia de segurança da informação em empresa de desenvolvimento de software para dispositivos móveis.
- **Capítulo 4 - Estratégia de implementação da segurança da informação:** apresenta os elementos que farão parte do documento de segurança.
- **Capítulo 5 – Avaliação da estratégia:** ilustra o processo de avaliação das bases que alicerçam a proposta da estratégia de segurança da informação.
- **Capítulo 6 – Conclusão:** apresenta as contribuições e os trabalhos futuros identificados a partir do desenvolvimento da estratégia de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis.

A figura 1.2 apresenta a estrutura do trabalho de uma forma mais detalhada.

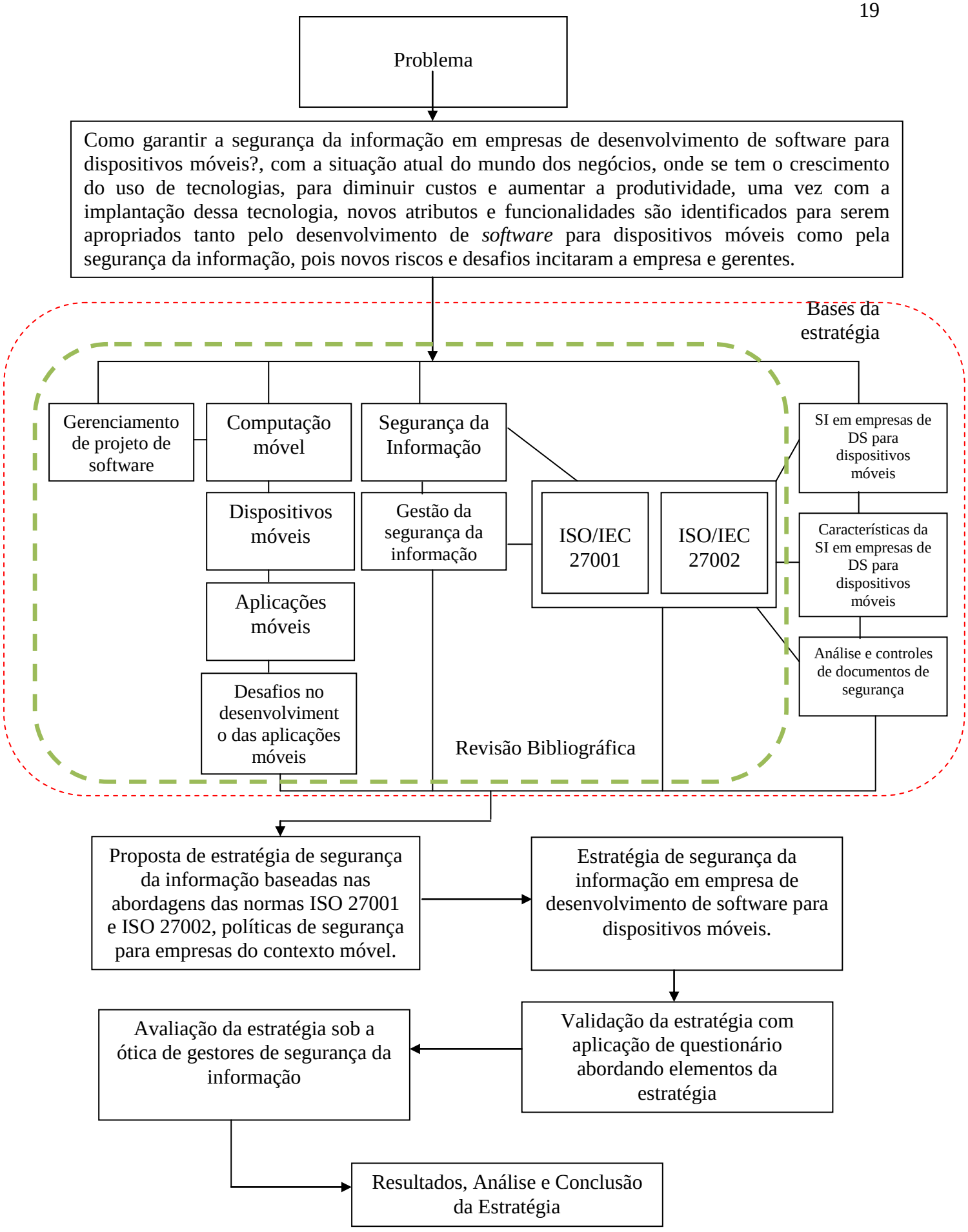

Figura 1.2: Estrutura do trabalho

Capítulo

2

Revisão Bibliográfica

2.1. Considerações Iniciais

Em empresas circulam informações muitas vezes confidenciais que, se forem fornecidas para pessoas não autorizadas, podem afetar no seu sucesso. Porém, se não existir um processo que proteja essas informações e defina quais podem ser fornecidas e para quem, a proteção dessas se torna quase impossível (Rodrigues, 2011).

A área responsável por essa proteção é a da Segurança da Informação, que tem como objetivo manter a confidencialidade, integridade e disponibilidade tanto das informações corporativas quanto das pessoais, trazendo como benefícios a redução dos riscos de vazamentos, fraudes, erros, sabotagens, uso indevido, roubo ou outros problemas que possam comprometer qualquer um dos objetivos acima citados.

Garantir a segurança da informação em projetos de desenvolvimento de software móvel é um fator primordial para o seu sucesso, uma vez, que o crescimento dessa tecnologia aumentou e as organizações têm portado suas aplicações para essa plataforma fazendo com que as empresas de desenvolvimento de *software* mudassem também sua tecnologia.

Neste capítulo é apresentado um estudo sobre os componentes relevantes da proposta de uma estratégia de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis. Os elementos relacionados ao arcabouço e que fornecem subsídios para o desenvolvimento da estratégia foram baseados nos estudos de Andrade (2012), Fontes (2011), Boulhosa (2011), Wangham (2007), Machado (2007), Souza (2007), Sima (2006), Fouskas *20L 20L*. (2005) e são:

- Gerenciamento de projetos de software;

- Computação móvel;
- Dispositivos móveis;
- Aplicações móveis;
- Desafios no desenvolvimento das aplicações móveis;
- Segurança da informação e;
- Gestão de segurança da informação

Desta forma, são abordadas as áreas de gerenciamento de projetos de software, o cenário da tecnologia para aplicações móveis, a segurança da informação em ambiente de desenvolvimento de software e a gestão de segurança da informação.

2.2. Gerenciamento de Projeto de Software

O gerenciamento de um projeto (GP) é o processo de tomar decisões que envolvem o uso de recursos, tanto materiais como humanos, para realizar atividades, temporárias, com o objetivo de fornecer um resultado (Huzita e Tait, 2006). A essência do gerenciamento de um projeto é a elaboração, planejamento, controle e a execução das atividades que definem um projeto específico. O GP é a primeira camada do processo de engenharia de *software*, pois abrange todo o processo de desenvolvimento, do começo ao fim (Pressman, 1995).

O GPS envolve além das etapas de GP (planejamento, avaliação e controle), as etapas do desenvolvimento de um projeto de *software* (técnicas de desenvolvimento, testes e qualidade). Segundo Enami (2006, p.55), "a área de gerência de projetos de *software* possui particularidades que dificultam ainda mais o gerenciamento, tais como: mudança da tecnologia, rodízio de pessoal que possui conhecimento específico sobre a tecnologia e a intangibilidade do software*"*.

A qualidade do GP depende da qualidade do sistema de informações em GP (SIGP), que: fornecerá informações aos *stakeholders* do projeto utilizando-se de fontes formais e informais; irá cobrir o ciclo de vida do desenvolvimento; irá apoiar o SI (Sistema da Informação) da organização interagindo com os SIs de outras áreas da organização; facilitará a tomada de decisão; reduzirá as surpresas ao longo do projeto; e, estará focado nas áreas críticas do projeto.Conforme o PMI (2008, p.6) o gerenciamento de projetos "é a aplicação do conhecimento, habilidades, ferramentas e técnicas às atividades do projeto a fim de atender aos seus requisitos". A aplicação do conhecimento diz respeito aos processos que devem ser

aplicados e integrados para efetivação do gerenciamento de projetos. O PMI (2008, p.37) define processo como sendo "um conjunto de ações e atividades inter-relacionadas realizadas para alcançar um produto, resultado ou serviço pré-especificado". A aplicação das habilidades e ferramentas é feita nas entradas de um processo e resultam em uma ou mais saídas que alimentam outros processos. Os processos estão divididos em cinco grupos de processos de gerenciamento de projetos (PMI, 2008): Iniciação, Planejamento, Execução, Monitoramento, Controle e Encerramento.

Os resultados que um processo produz, geralmente, são consumidos na entrada de outro processo, formando assim, conexões entre os processos, que se pode elevar ao nível dos grupos de processos conforme a Figura 2.1 (PMI, 2008).

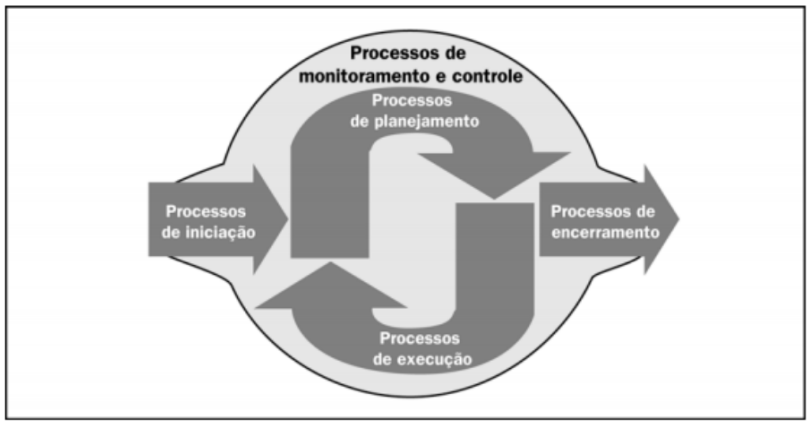

Figura 2.1: Conexão entre os grupos de processos
Fonte: Guia PMBOK®. Um Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos. 3ª edição. Pensilvânia: *Project Management Institute*, 2008.

Os grupos de processos, porém, de acordo com o PMI (2008, p.40) "raramente são eventos distintos ou únicos; eles são atividades sobrepostas que ocorrem em diversos níveis de intensidade durante todo o projeto" como é mostrado na Figura 2.2.

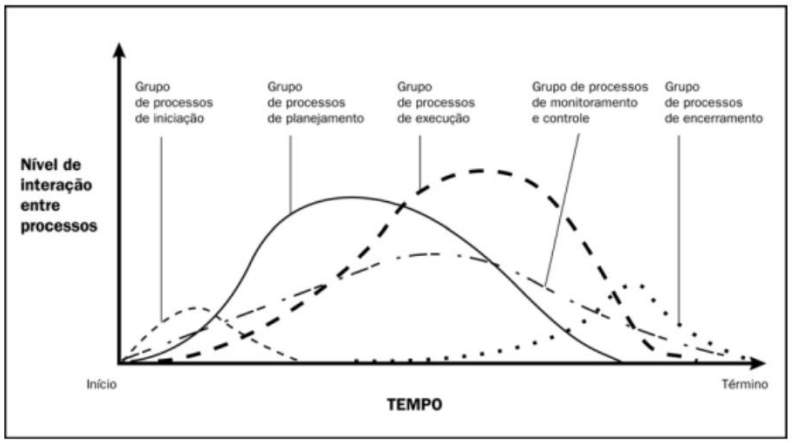

Figura 2.2: Interação entre os grupos de processos
Fonte: Guia PMBOK®. Um Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos. 3ª edição. Pensilvânia: *Project Management Institute*, 2008.

Além da divisão por grupos, os processos também são organizados em nove áreas de conhecimento (PMI, 2008), conforme Figura 2.3.

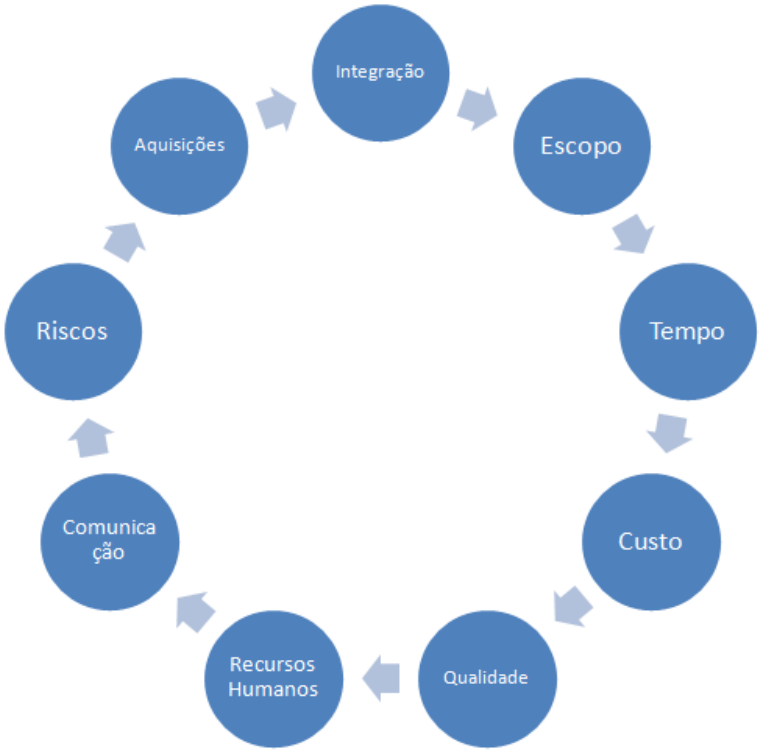

Figura 2.3: Áreas de conhecimento dos grupos de processos

As nove áreas de conhecimento dos grupos de processos apresentado na Figura 2.3, apresentam requisitos para auxiliar as fases do gerenciamento do projeto.

Segundo Enami (2006), dentre os principais padrões e modelos para o gerenciamento do projeto destacam-se os modelos processuais do PMI (*Project Management Institute*), o CMMI (*Capability Maturity Model Integration*) e o MR-MPS (Modelo de Referência de Melhoria de Processos de *Software*), este último também conhecido como MPS.BR (Melhoria de Processo de Software Brasileiro). Fernandes e Abreu (2008) complementam a lista com os modelos PRINCE2 (*Projetct in Controlled Environments*) e CobiT (*Control Objectives for Information and Related Technology*).

No entanto as normas ISO 9001, ISO/IEC 9126 e ISO/IEC 12207 auxiliam o gerente de projetos a obter dados relevantes do ambiente e padronizar o desenvolvimento de software, contribuindo para a gestão de projetos de software (Fernandes e Abreu , 2008).

Os padrões e normas citados por Fernandes e Abreu (2008) e Enami (2006) contribuem para o gerenciamento de projetos de software e possuem aplicabilidade específica conforme a necessidade e objetivo do projeto.

2.3. Computação móvel

Computação móvel pode ser representada como um novo paradigma computacional que permite que usuários desse ambiente tenham acesso a serviços independentemente de sua localização, podendo inclusive, estar em movimento. Mais tecnicamente, é um conceito que envolve processamento, mobilidade e comunicação sem fio. A ideia é ter acesso à informação em qualquer lugar e a qualquer momento.

A computação móvel é caracterizada por três propriedades essenciais: mobilidade, portabilidade e conectividade (Souza, 2007).

Lee, *et.*(2005) classifica o conceito mobilidade como:

> *Capacidade de poder se deslocar ou ser deslocado facilmente. No contexto da computação móvel a mobilidade se refere ao uso pelas pessoas de dispositivos móveis portáteis funcionalmente poderosos que ofereçam capacidade de realizar facilmente um conjunto de funções de aplicação, sendo também capazes de conectar-se, obter dados e fornecê-los a outros usuários, aplicações e sistemas. (Lee; 24L 24L , 2005, p. 56)*

Já o conceito de Portabilidade é definido como a capacidade de ser facilmente transportável (Lee, *et.*, 2005 *apud* Souza, 2007).

> *Para um dispositivo móvel ser portátil, deve ser pequeno e leve (incluindo acessórios), no entanto, essa portabilidade tem consequência limitações como capacidade de memória, armazenamento, poder de processamento e tamanho de tela. Além disso, a portabilidade aumenta o risco de perda ou danos no dispositivo móvel. (Augustin et., 2001, p. 35 apud* Souza, 2007*).*

Ainda segundo Lee, *et.*, (2005) mesmo que muitos dispositivos móveis tenham aplicações independentes, que permitem aos usuários operarem de forma independente durante certo tempo, a sua função primária da conectividade é conectar as pessoas ou sistemas e transmitir e receber informações.

2.4. Dispositivos móveis

A implantação de tecnologias móveis pelas organizações exige uma abordagem estratégica para incorporar aos negócios. A tecnologia móvel precisa ser estudada, compreendida e

incorporada pelas organizações por meio de estratégicas cuidadosamente interpretadas e pesquisadas, visando prover um valor ao negócio e aos envolvidos (Unhelkar, 2009).

As tecnologias móveis possibilitam a ocorrência de interações entre os envolvidos (pessoas, organizações, clientes, fornecedores, etc.) a qualquer hora e em qualquer lugar. Esse paradigma é possível com a implementação de uma infraestrutura adequada que envolve padrões de comunicação móvel e a utilização de dispositivos portáteis (Unhelkar, 2009; Machado; Freitas, 2009), incluindo os celulares, *smartphones*, *Personal Digital Assistants* (PDAs), *palmtops*, *notebooks* e *netbooks*.

Segundo Boulhosa (2011), estes aparelhos estão cada vez mais sofisticados e embutem diversos dispositivos que permitem conexão de banda larga, sensores e funcionalidade de geolocalização, entre outras funções, que nos abre inúmeras oportunidades de exploração.

O desafio para a área de TI é que estes aparelhos estão entrando nas empresas por todos os lados. Impedir seu uso é impossível, mas é necessário criar procedimentos que garantam a segurança e privacidade dos dados considerados críticos para o negócio (Andrade, 2012).

2.5. Aplicações Móveis

Com os avanços nas áreas de telecomunicação, computação e miniaturização de computadores, novos produtos tecnológicos foram desenvolvidos e, rapidamente tornaram-se pontos-chave para as novas abordagens de comunicação e estratégias de negócio (Ali-Hassan *et.*, 2010; Counts *et*., 2006). Neste cenário, têm-se as aplicações móveis que apresentam várias características que agregam funcionalidade aos seus usuários. A primeira delas é a mobilidade, a capacidade de manter voz constante e comunicação de dados enquanto em movimento. Em segundo lugar, está o imediatismo, que permite aos usuários obter conectividade quando necessário, sem considerar a localização e sem uma longa sessão de *login*. Finalmente, localização permite aos usuários obterem informações relevantes para suas localizações atuais.

A combinação dessas características fornece uma grande faixa de possíveis aplicações que podem ser oferecidas aos usuários que utilizam dispositivos móveis, tais como: Comunicações que são as aplicações de comunicações onde incluem aquelas em que o usuário utiliza a rede de comunicação móvel apenas como um canal para acessar mensagens ou informações (e-*mail*, mensagem unificada e acesso à *intranet/Internet)*; Aplicação baseada em localização que é navegação, condições de tráfego de veículos, localização de pessoas e

hospitais, etc; Aplicações verticais que é o gerenciamento de frota, alocação de recursos, etc; Publicidade que são os serviços oferecidos do tipo *push*[1] e Serviço de valor agregado *M-commerce* que está relacionado com a venda a varejo, compra de bilhetes e o *Banking que são os* serviços bancários e Comércio Financeiro.

2.6. Desafios no desenvolvimento das aplicações móveis

O desenvolvimento de software para dispositivos móveis resulta em uma tarefa desafiadora (Boll *et*., 2005; Hosbond, 2005; Varshney &Vetter, 2000 *apud* Souza, 2007) e apresenta muitos desafios diferentes das típicas aplicações convencionais. Ressalta ainda que um dos desafios enfrentados é a falta de padronização e a variedade de modelos, plataformas (Java, Windows Mobile, Symbian, Android e iPhone).

Devido a essa falta de padronização, ao definirmos os requisitos de um projeto de software para dispositivos móveis, é muito importante levar em consideração a variedade de hardware (processadores, memórias, tamanho da tela, etc) e de software (sistemas operacionais e seus recursos) encontrada em dispositivos móveis (Muchow, 2004 *apud* Souza, 2007).

Segundo Alberto Leite, presidente da SupportComm, empresa brasileira especializada no desenvolvimento de aplicativos móveis, em um artigo publicado em abril de 2012, acrescenta que, além da visualização, a forma de processar e de armazenar as aplicações também varia de celular para celular. E tudo isso precisa ser ajustado à grande quantidade de modelos disponíveis no mercado o que torna um grande desafio para os gerentes de projetos.

Esse ambiente de comunicação móvel, associado à combinação complexa de protocolos de rede, faz o projeto de soluções de segurança para aplicações móveis um desafio particular (Josang e Sanderrud, 2003). Portanto, segurança e opções de conectividade sem fios são fatores que também devem ser levados em consideração no desenvolvimento de aplicações móveis.

2.7. Segurança da Informação

Com base na norma NBR ISO/IEC 27002 (ABNT, 2005), “Informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e

[1] *Push* é um sistema de distribuição de conteúdo da Internet em que a informação sai de um servidor para um cliente, com base em uma série de parâmetros estabelecidos pelo cliente, também chamado de "assinatura".

consequentemente necessita ser adequadamente protegido".

A informação é utilizada tanto para administrar internamente a organização como para prever situações de mercado e concorrentes. Por esse motivo, ela é um bem poderoso para a empresa (Carvalho, 2011). Por ser tão importante, a informação necessita ser segura e neste aspecto é necessário analisar a segurança da informação. A geração de informação é algo muito comum para qualquer empresa e a segurança dessas informações é vital também quanto ao caráter estratégico. Para Bluephoenix (2008) a segurança da informação de uma empresa garante, em muitos casos, a continuidade de negócio, incrementa a estabilidade e permite que as pessoas e os bens estejam seguros de ameaças e perigos.

Segundo a norma (ABNT NBR ISO/IEC 27002, 2005) para que se possa garantir a segurança da informação alguns princípios básicos devem ser respeitados, tais como:

- **Confidencialidade:** significa que a informação deve ser protegida contra sua divulgação para pessoas não autorizadas – interna ou externamente. Consiste em proteger a informação contra cópias e distribuição não autorizada. Dessa forma, a informação deve ser confidencial e sua utilização deverá ser feita por pessoas previamente autorizadas.
- **Integridade:** consiste em garantir que a informação gerada não seja modificada sem a devida autorização da(s) pessoa(s) responsável por ela. Isto implica que não deve ser permitido que a informação original sofra nenhum tipo de violação seja ela escrita, alteração de conteúdo, alteração de status, remoção e criação de informações.
- **Autenticidade:** o controle de autenticidade está ligado ao fato da informação que esteja sendo trafegada seja de fato originada do proprietário a ela relacionado. Não deve ser permitida a violação da origem da informação.
- **Disponibilidade:** garantir que a informação esteja disponível às pessoas autorizadas sem nenhum tipo de modificação e sempre que elas necessitarem. Pode ser chamado também de continuidade do serviço.

Através da garantia desses serviços, a segurança da informação poderá trazer benefícios relevantes para a organização como, por exemplo: aumentar a produtividade dos usuários através de um ambiente mais organizado, maior controle sobre os recursos de informática e, finalmente, garantir a funcionalidade das aplicações críticas da empresa.

Neste cenário, empresas que desenvolvem ou que estão mudando suas aplicações para dispositivos móveis devem estar cientes dos fatores mais comumente considerados pelas empresas do ramo que é a segurança. Os dispositivos móveis geralmente contêm

informações pessoais que podem ser alvo dos *hackers*, pois não há verificação de segurança.

Assim com a evolução dessa tecnologia móvel, a informação concretizou-se como o ativo mais valioso das empresas, e a segurança dessa informação um fator primordial, pois de uma forma crescente, as organizações, seus sistemas de informações e suas redes de computadores apresentam-se diante de uma série de ameaças, sendo que, algumas vezes, estas ameaças podem resultar em prejuízos para as empresas.

A segurança da informação visa proteger as empresas de um grande número de ameaças para assegurar a continuidade do negócio. Esta segurança é obtida a partir da implementação de uma série de controles, que podem ser políticas, práticas e procedimentos, os quais precisam ser estabelecidos para garantir que os objetivos de segurança específicos da organização sejam atendidos.

O Relatório *Symantec* (28R28.symantec.com.br) no primeiro semestre de 2010 sobre Segurança da Informação nas Empresas mostra que as empresas da América Latina perdem mais de US$ 500 mil por ano em decorrência de ataques virtuais. Outra pesquisa da *Qualibest* (28R28.qualibest.com.br) apontou que mais de 85% dos funcionários no Brasil usam a *internet* da empresa para fins pessoais. Desses, quase 80% usam o e-mail pessoal durante o expediente, mais de 60% fazem pesquisas pessoais em sites de busca, mais de 50% fazem operações com *internet banking* e cerca de 15% utilizam a conexão com a *internet* da empresa para *download* de músicas, jogos e outros *downloads* de interesses pessoais.

2.7.1 Ameaças e ataques

As ameaças ao sistema de informação estão relacionadas com a quebra dos quatro princípios básicos da segurança da informação: Confiabilidade, Integridade, Autenticidade e Disponibilidade.

Uma ameaça consiste em uma possível violação de um sistema computacional e pode ser acidental ou intencional (Pinheiro, 2007). Uma ameaça acidental é aquela que não foi planejada. Pode ser, por exemplo, uma falha no hardware ou no software. Já uma ameaça intencional, como o nome diz, está associada à intencionalidade premeditada.

Por ameaças entendem-se também os elementos que tem a condição de explorar a vulnerabilidades e causar problemas severos aos ativos de uma empresa (Módul, 2011; Souza, 2011). Dentre as várias classificações na literatura, podemos citar as seguintes:

Naturais - condições da natureza que podem causar danos, como por exemplo: enchentes, incêndio e terremotos.

Intencionais: propositais como vírus de computador, espionagem, fraude, vandalismo,

roubo entre outros.

Involuntárias: originadas por falhas não intencionais dos usuários como acidentes, erros, falta de conhecimento dos ativos.

Um ataque ocorre quando uma ameaça intencional é realizada. Os ataques ocorrem por motivos diversos. Variam desde a pura curiosidade, passando pelo interesse em adquirir maior conhecimento sobre os sistemas, até o extremo, envolvendo ganhos financeiros, extorsão, chantagem de algum tipo, espionagem industrial, venda de informações confidenciais e, ferir a imagem de um governo ou uma determinada empresa ou serviço. Três aspectos que um sistema de informação deve atender para evitar a concretização das ameaças e ataques: Prevenção, Detecção e Recuperação.

2.7.2. Prevenção

Segundo Fontes (2011), as organizações e os indivíduos podem prevenir seus sistemas contras ameaças e ataques de muitas maneiras, tais como:

Proteção de hardware: normalmente chamada de segurança física, impede acessos físicos não autorizados à infraestrutura da rede, prevenindo roubos de dados, desligamento de equipamentos e demais danos quando se está fisicamente no local.

Proteção de arquivos e dados: proporcionada pela autenticação, controle de acesso e sistemas antivírus. No processo de autenticação, é verificada a identidade do usuário; o controle de acesso disponibiliza apenas as transações pertinentes ao usuário e os programas antivírus garantem a proteção do sistema contra programas maliciosos;

Proteção de perímetro: ferramentas de firewall e *routers* cuidam desse aspecto, mantendo a rede protegida contra tentativas de intrusão (interna e externa à rede).

2.7.3. Detecção

Segundo Turbam (2007), os controles de detecção de intrusões alertam os responsáveis pela segurança sobre qualquer sinal de invasão ou mudança suspeita no comportamento da rede que possa significar um padrão de ataque. Os avisos podem ser via e-mail, mensagem no console de gerência, celular, etc. A instalação desses controles é necessária, mas não o suficiente, pois também é necessário responder a questões como as seguintes: *"Os controles foram instalados conforme pretendido? Eles são eficazes? Ocorreu alguma brecha de segurança? Nesse caso, quais as ações necessárias para evitar que ocorram novamente?"*.

Ressalta ainda que essas questões devem ser respondidas por observadores

independentes e imparciais.

> Tais observadores executam a tarefa de auditoria de sistemas de informação ao qual periodicamente devem-se analisar os componentes críticos do sistema a procura de mudanças suspeitas. Esse processo pode ser realizado por ferramentas que procuram, por exemplo, modificações no tamanho dos arquivos de senhas, usuários inativos, etc. (Turban, 2007, p. 45).

2.7.4. Recuperação

A melhor defesa é estar preparado para diversas eventualidades. Um elemento importante em qualquer sistema de segurança é um plano de recuperação de acidentes. A destruição dos recursos de computação de uma organização pode provocar danos significativos (Turban, 2007; Potter; Rainer, pag. 454.). Assim, algumas medidas podem ser tomadas, tais como:

Cópia de segurança dos dados (Backup): manter sempre atualizados e testados os arquivos de segurança em mídia confiável e separados física e logicamente dos servidores;

Aplicativos de Backup: ferramentas que proporcionam a recuperação rápida e confiável dos dados atualizados em caso da perda das informações originais do sistema;

Backup de hardware: a existência de hardware reserva, fornecimento autônomo de energia, linhas de dados redundantes, etc., podem ser justificados levando-se em conta o custo da indisponibilidade dos sistemas.

2.7.5. Vulnerabilidades

Segundo Nakamura (2002, p.29-89), vulnerabilidades são deficiências de diversas origens, as quais muitas vezes, não são identificadas a tempo ou, mesmo quando isso ocorre, não são devidamente tratadas de modo a evitar um ataque.

Moreira (2001 apud Souza, 2007), afirma que a vulnerabilidade é o ponto onde poderá acontecer um ataque, ou seja, o ponto onde uma fraqueza ou deficiência de segurança poderá ser explorada, causando assim um incidente de segurança.

> A vulnerabilidade é o ponto onde qualquer sistema é suscetível a um ataque, ou seja, é uma condição encontrada em determinados recursos, processos, configurações, etc. Condição causada muitas vezes pela ausência ou ineficiência das medidas de proteção utilizadas de salvaguardar os bens da empresa. (Moreira, 2001, p. 22 apud Souza, 2007)

As vulnerabilidades podem ter origens diversas como apresentado na lista sugerida por Semôla (Semôla, 2003, p.48 – 49).

Agentes da natureza, umidade, poeira, poluição e calor podem causar danos aos ativos. Deve-se levar em consideração também fatores geográficos que possam resultar em ameaças. Por exemplo, instalações próximas a rios que causam inundações.

- **Hardware:** falha no dimensionamento do equipamento a ser utilizado, problemas de projeto e manutenção.
- **Software:** falhas no desenvolvimento que permitem a inclusão e execução de softwares com códigos maliciosos.
- **Mídias de armazenamento:** falhas de fabricação ou estocagem de CD-ROM, disco rígido, DVD-ROM entre outros.
- **Meios de comunicação:** problemas no cabeamento, antenas de rádio inadequadas entre outros problemas na infraestrutura de comunicação.
- **Humanas:** relativas aos danos que o ser humano pode causar às informações quando de espionagem, má utilização e acidentes derivados da falta de treinamento, insatisfação com o trabalho, erros dentre outros fatores.

2.7.6. Riscos

Os riscos podem ser definidos como a probabilidade da ocorrência de um determinado evento sem a pretensão de invocá-lo e que após sua concretização resulte em um impacto positivo ou negativo (Heldman, 2006; PMI 2008 apud Andrade, 2012).

Entretanto, Módulo (2007) diz que os riscos são as possibilidades das ameaças explorarem as vulnerabilidades, ocasionando danos ou perdas de dados, proporcionando prejuízos aos negócios da empresa e que acabam por afetar os princípios de confidencialidade, integridade e disponibilidade.

Existem diversas formas de se analisar os riscos e por intermédio de um estudo classificar as informações em categorias permitindo avaliar o impacto que uma ameaça pode trazer.

A norma NBR 27001 descreve os controles de segurança requeridos no ambiente organizacional e preconiza que os sistemas de gestão de segurança da informação devem se focar na gestão de riscos a fim de atingir os seguintes objetivos:

- identificar o valor e analisar eventuais fraquezas dos ativos de informação;
- permitir que a gerência tome decisões fundamentadas sobre a gestão do risco, eventualmente justificando despesas alocadas a este fim; e
- incrementar a informação organizacional sobre os sistemas de tecnologia da

informação a fim de melhorar sua segurança.

O processo de gestão de riscos é definido por oito atividades que são apresentados na norma ISO/IEC 27005:2008 que tem por objetivo fornecer as diretrizes para o processo de Gestão de Riscos de Segurança da Informação e são apresentadas na Figura 2.4.

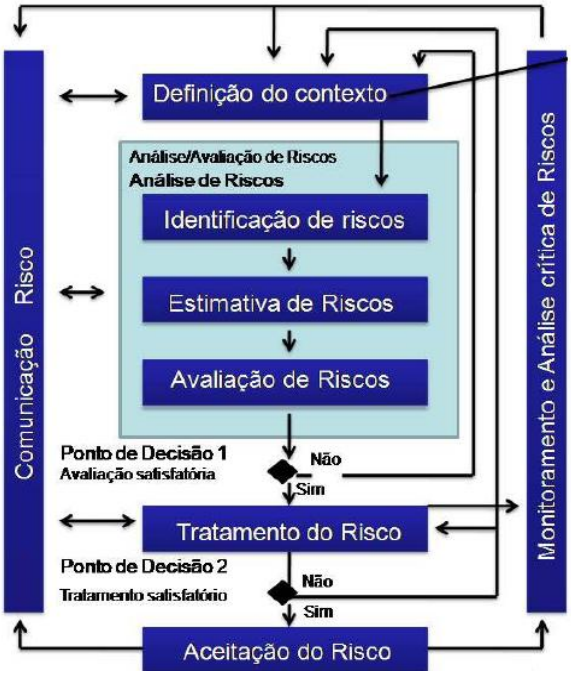

Figura 2.4: Processo de gestão de riscos de segurança da informação
Fonte: ABNT NBR ISO/IEC 27005, 2008

Para cada etapa da norma são propostas diretrizes para implementação que serão brevemente descritas a seguir (ABNT NBR ISO/IEC 27005, 2008).

- **Definição do contexto:** Definir o escopo e limites que serão levados em consideração na gestão de riscos.

Deverão ser descritos os processos que fazem parte do escopo, garantindo a identificação dos ativos relevantes para a gestão dos riscos. Além disso, a definição do contexto inclui determinar os critérios gerais de aceitação dos riscos para a organização e as responsabilidades para a gestão de riscos. É nessa definição do escopo e limites que a política de segurança da informação é considerada.

- **Análise/Avaliação dos riscos de segurança da informação:** Este item apresenta todo processo de análise e avaliação dos riscos de segurança da informação, tais como:

1 - Identificação de riscos:

Identificar os eventos que possam ter impacto negativo nos negócios da organização.

Devem ser identificados os ativos, suas vulnerabilidades e as ameaças que podem causar danos aos ativos. Identificar as consequências que as perdas de confidencialidade, de integridade e de disponibilidade podem ter sobre os ativos.

2 - Estimativa de riscos:

Atribuir valor ao impacto que um risco pode ter e a probabilidade de sua ocorrência, de forma qualitativa ou quantitativa. Estimar o risco através da combinação entre a probabilidade de um cenário de incidente e suas consequências.

3 - Avaliação de riscos:

Determinar a prioridade de cada risco através de uma comparação entre o nível estimado do risco e o nível aceitável estabelecido pela organização.

O ponto de decisão 1, visto na Figura 2.4, verifica se a avaliação dos riscos foi satisfatória, conforme os critérios estabelecidos pela organização. Caso não seja satisfatória, a atividade pode ser reiniciada de forma que se possa revisar, aprofundar e detalhar ainda mais a avaliação, assegurando que os riscos possam ser adequadamente avaliados.

- **Tratamento do risco:** Implementar controles para reduzir, reter, evitar ou transferir os riscos. Se o tratamento do risco não for satisfatório, ou seja, não resultar em um nível de risco residual que seja aceitável, deve-se iniciar novamente a atividade ou o processo até que os riscos residuais sejam explicitamente aceitos pelos gestores da organização. Esta iteração se dá no ponto de decisão 2, como visto na figura 2.4.
- **Aceitação do risco:** Registrar formalmente a aprovação dos planos de tratamento do risco e os riscos residuais resultantes, juntamente com a responsabilidade pela decisão.
- **Comunicação do risco:** Desenvolver planos de comunicação dos riscos para assegurar que todos tenham consciência sobre os riscos e controles a serem adotados.
- **Monitoramento e análise crítica de riscos:** Monitorar continuamente os riscos e seus fatores a fim de identificar eventuais mudanças no contexto. Certificar que o processo de gestão de riscos de segurança da informação e as atividades relacionadas permaneçam apropriados nas circunstâncias presentes.

A norma ISO/IEC 27005 não inclui uma metodologia específica para a gestão de riscos de segurança da informação, cabendo a cada organização definir a melhor abordagem conforme o contexto na qual está inserida.

Criada para apoiar o entendimento das especificações e conceitos estabelecidos pela norma ISO/IEC 27001, esta norma define as melhores práticas em gestão de riscos de segurança da informação e podem ser aplicadas a organizações de todos os portes e segmentos.

2.7.7. Ataques

Existem muitos métodos de ataque a recursos de computação, e novos métodos aparecem regularmente.

Coletar informações da ocorrência dos tipos de ataques é um passo necessário para dar início a um plano de ação de segurança da informação (Hatch, 2003, p.225 apud Souza, 2007), os ataques podem ter origem nas ameaças descritas na seção 2.7.1 deste trabalho. A Tabela 2.1 apresenta uma lista de ataques comuns:

Tabela 2.1: Tipos de ataques comuns

Método	Definição
Vírus	Instruções secretas inseridas em programas (ou dados) que são executadas inocentemente durante as tarefas normais. As instruções secretas podem destruir ou alterar dados, bem como se espalhar dentro do sistema ou para outros sistemas de computador.
Worm	Software que não precisa ser executado para ser utilizado. Fornece informações que são transmitidas a *hackers* de modo imperceptível ao usuário.
Cavalo de Tróia	Um programa ilegal, contido dentro de outro programa, que permanece "dormindo" até que um evento específico ocorra, o que aciona o programa ilegal para ser ativado e causar danos.
Denial of Service (DoS)	Ataque de negação de serviço, responsável por sobrecarregar servidores com grande volume de informação, causando a parada do sistema operacional, provocando o preenchimento da memória do computador e a sobrecarga de operações do processador.
Packet Sniffing	Um programa que procura senhas ou conteúdo em um pacote de dados enquanto passam pela Internet.
Cracker de senha	Um programa que tenta adivinhar senhas.
Portas dos fundos	Os invasores de um sistema criam vários pontos de entrada; mesmo que você descubra e feche um, eles ainda podem entrar pelos outros.
Apples maliciosos	Pequenos programas em JAVA que se aproveitam dos recursos do seu computador, modificam seus arquivos, enviam e-mails falsos, etc.
Salami slicing	Um programa destinado a extrair pequenas quantidades de dinheiro de diversas transações maiores, de modo que a quantidade tirada não seja

	imediatamente aparente.
Scan	Também conhecido como Port Scanning, analisa portas IP que possuem serviços associados, como por exemplo, telnet.
Invasão	Um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
Web	Um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
Fraude	Qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro. Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.

Fonte: Adaptado de Turban, 2005

Entre os anos de 1999 a 2012 foram reportados ao CERT.br - Centro de Estudo, Respostas e Tratamento de Incidentes de Segurança no Brasil – vários incidentes com relação a ataques em empresas através dos métodos apresentados na tabela 2.1.

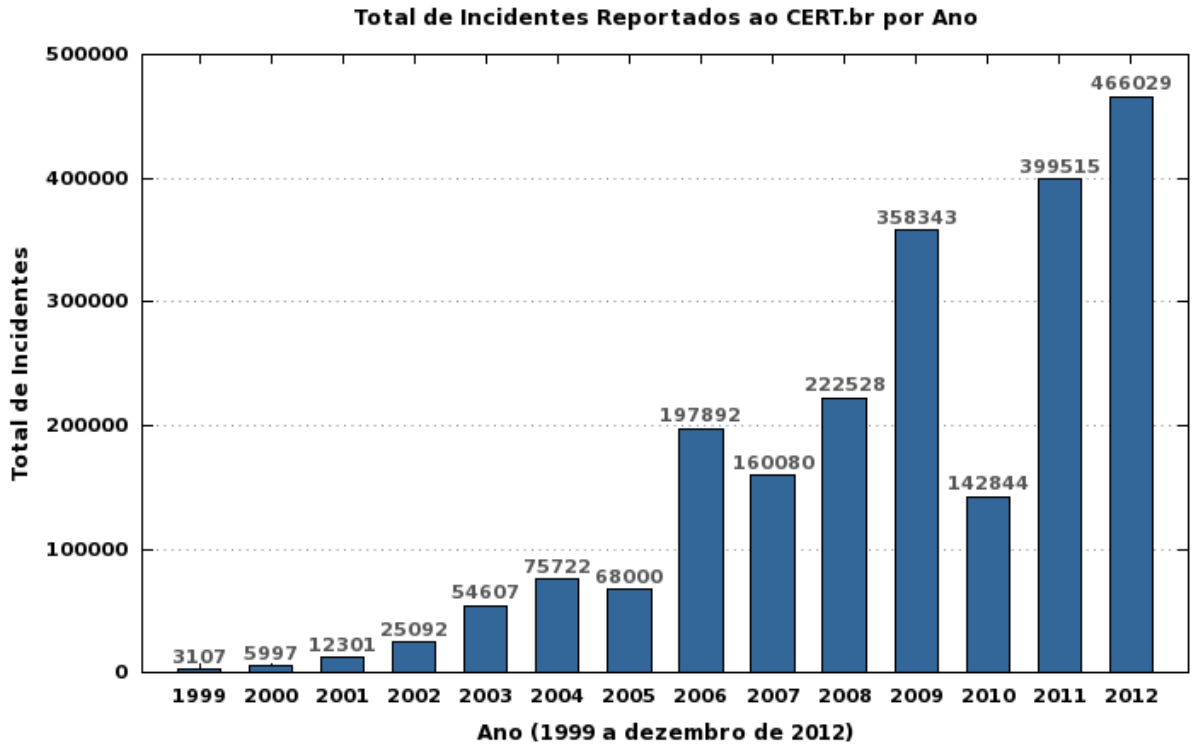

Figura 2.5: Totais de incidentes de segurança reportadas ao CERT

Fonte: CERT.br. Disponível em http://www.cert.br/stats/incidentes. Acesso: 10 mar. 2013.

Segundo a CERT e como apresentado na Figura 2.5 o total de notificações recebidas em 2012 foi de 466.029, este número foi 17% maior que o total de 2011. Nesse cenário, a quantidade de incidentes de segurança por si só motiva as empresas a pensarem a implantar segurança em seus negócios, visto que muitas informações são críticas. Algumas delas são secretas e possuem alto valor estratégico.

A implantação de segurança através de uma estratégia pode auxiliar as empresas nas

mudanças culturais e organizacionais relacionadas à segurança da informação.

2.8. Gestão de Segurança da Informação

Segundo (Fontes, 2011) o processo de segurança da informação existe para possibilitar que a organização utilize de maneira confiável os recursos que suportam as informações necessárias para as suas atividades estratégicas, táticas e operacionais.

Thomas Peltier define a segurança da informação dando ênfase na proteção dos recursos:

> *Segurança da informação direciona e suporta a organização para proteção de seus recursos de informação intencional ou não intencional divulgação indevida, modificação não autorizada, destruição não desejada, ou negação de serviço através da implantação de controles de segurança definidos em políticas e procedimentos. (Peltier, 2004, p.9).*

Peltier continua indicando que segurança da informação está ligada fortemente aos objetivos do negócio. Para Peltier a segurança da informação não deve existir para ela mesma; a segurança da informação deve existir para atender à organização e aos seus objetivos de negócios.

A NBR ISO/IEC 27002:2005 reforça que segurança da informação é importante para o setor público e para o setor privado.

Por sua vez a norma ISO/IEC 27001:2006 orienta sobre a maneira de implantação de um SGSI (Sistema de Gestão de Segurança da Informação).

Em relação ao processo de gestão da segurança da informação a NBR ISO/IEC 27001:2006 provê um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI) conforme as necessidades da organização.

2.9. Normas ISO/IEC 27001:2006 e ISO/IEC 27002:2005

A norma ISO 27001 (ABNT ISO 27001, 2006) provê e apresenta requisitos para que a organização possa estruturar um sistema de gestão de segurança da informação (SGSI). Por sua vez, a norma ISO 27002 (ABNT ISO 27002, 2005) é um conjunto de boas práticas que podem ser aplicadas por um SGSI.

Segundo Souza (2007) o conjunto destas duas normas pode ser descritos como: i) um

método estruturado reconhecido internacionalmente para segurança da informação; ii) um processo definido para avaliar, manter e gerenciar a segurança da informação; iii) um grupo completo de controles contendo as melhores práticas a serem adotadas por empresas (ABNT ISO 27001, 2005).

2.9.1. Norma ISO 27001 – Sistema de Gestão de Segurança da Informação (SGSI)

Esta Norma foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). A adoção de um SGSI deve ser uma decisão estratégica para uma organização. A especificação e a implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos empregados e tamanho e estrutura da organização.

O SGSI pode ser simplesmente definido como um comitê multidisciplinar que tem como principal responsabilidade estabelecer políticas de segurança, multiplicar o conhecimento envolvido e também determinar os responsáveis e as medidas cabíveis dentro de seus limites de atuação (ABNT ISO 27001, 2005).

Esta Norma adota o modelo conhecido como "*Plan-Do-Check-Act*" (PDCA), apresentado na Figura 2.6, que é aplicado para estruturar todos os processos do SGSI.

- ***Plan* (planejar) (estabelecer o SGSI):** Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.
- ***Do* (fazer) (implementar e operar o SGSI):** Implementar e operar a política, controles, processos e procedimentos do SGSI.
- ***Check* (checar) (monitorar e analisar criticamente o SGSI):** Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.
- ***Act* (agir) (manter e melhorar o SGSI):** Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI. A figura 2.6 apresenta o relacionamento do modelo PDCA com as etapas do SGSI.

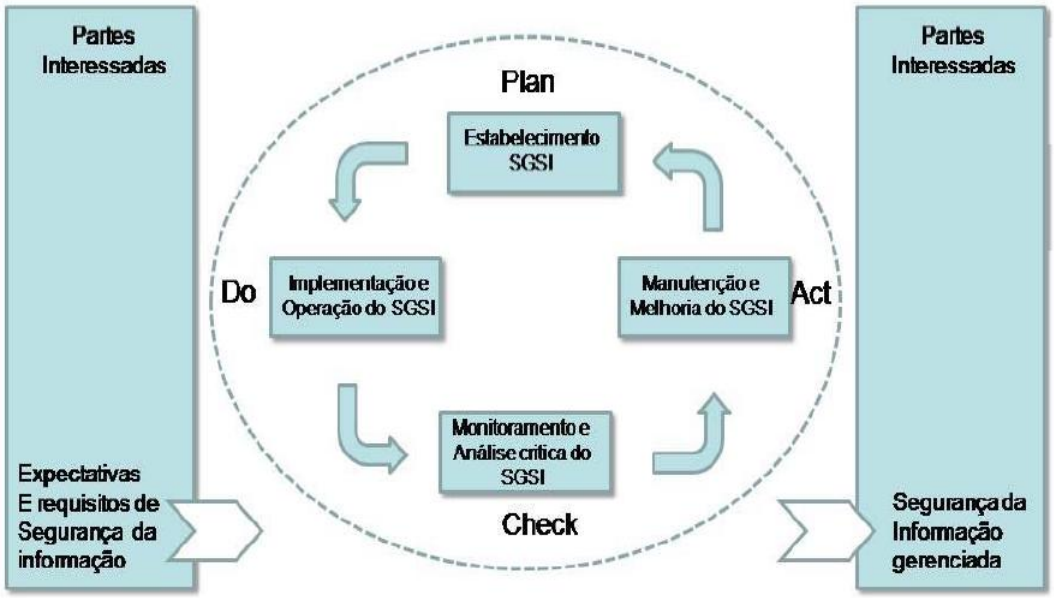

Figura 2.6: Modelo do PDCA

Fonte: NBR ISO/IEC 27001:2006

Com a alta direção compromissada e o treinamento eficaz dos colaboradores, é possível se reduzir o número de ameaças que exploram eventuais vulnerabilidades. Na Tabela 2.2 apresentam-se os requisitos existentes na Norma ISO 27001 para auxiliar a implantação do SGSI na organização.

Tabela 2.2: Requisitos da Norma ISO 27001

Nº	**Requisito**	**Descrição**
1	Escopo	Abrangência da Norma
2	Referência Normativa	Normas e padrões relacionados à norma 27001
3	Termos e definições	Termos e definições relacionados à segurança da informação
4	Sistema de Gestão de Segurança de Informação	Referente à criação, implementação, monitoramento e melhoria do SGSI, também trata de documentação e de registros de informações.
5	Responsabilidade da Direção	Definições de responsabilidades, treinamento e provisão de recursos do SGSI.
6	Auditorias Internas	Auditorias internas realizadas por pessoal treinado e comprometido com o SGSI
7	Análise crítica do SGSI	Análise realizada pelo corpo diretivo da organização das ações efetuadas pelo SGSI
8	Melhoria do SGSI	Trata das ações corretivas e preventivas efetuadas pelo

SGSI

Fonte: Adaptado de (ABNT ISO 27001, 2006)

2.9.2. Norma ISO 27002 – Código de Prática para SGSI

Essa norma foi baseada na norma britânica BS 17799-1:1999 (ABNT ISO 17799, 2005) sendo aplicada como um documento de referência, que é chamada de guia de melhores práticas.

A ISO 27001 é uma norma que apresenta requisitos de segurança para a organização, ou seja, cria um sistema de segurança (SGSI) dentro da empresa. Isso em nenhum momento garante segurança, com um sistema desses implementado, a organização consegue "ver" o problema de segurança facilmente. A ISO 27002, contem todos os controles que tem na ISO 27001 só que com explicações e exemplos de implementação.

A norma é composta por 16 (dezesseis) capítulos, numerados de 0 (zero) à 15 (quinze) e são consideradas 11 (onze) seções de controles de segurança da informação. Cada seção é composta por um número variado de categorias principais de segurança da informação e cada categoria possui certo número de controles. Estes controles, apresentados na tabela 2.3, são elementos que definem o que a norma considera importante para um processo de segurança da informação na organização e devem ser os elementos considerados para as políticas de segurança da informação das organizações.

Existem 133 (centro e trinta e três) controles explícitos nesta norma. Estes controles, de maneira isolada ou agrupada, ou considerando outros controles não descritos nesta norma, são os elementos considerados nesta pesquisa para a identificação da estratégia de segurança da informação de uma organização tomando por base elementos comuns existentes em políticas de organizações afins.

Tabela 2.3: Controles da Norma ISO 27002

Item	Controles	Descrição
[C01]	Política de Segurança	São as normas desenvolvidas que consideram as responsabilidades, punições e autoridades
[C02]	Política Organizacional	Estrutura da gerencia da segurança
[C03]	Classificação e Controle dos Ativos de Informação	Classificação, registro e controle dos ativos
[C04]	Segurança em Pessoas	Foco do risco decorrente de atos decorrentes de ações das pessoas
[C05]	Segurança Física e do ambiente	Levantamento da necessidade de definição das áreas de circulação restrita e de se proteger equipamentos e infraestrutura de TI
[C06]	Gerenciamento de Operações e Comunicações	Aborda temas relacionados à: procedimentos operacionais, homologação e implantação de sistemas, entre outras.
[C07]	Controle de Acesso	Controle do acesso aos sistemas, definição de competências e responsabilidades.
[C08]	Desenvolvimento da Segurança de Sistemas	Requisitos para os sistemas, criptografia, arquivos e desenvolvimento e suporte de sistemas.
[C9]	Gestão de incidentes de segurança	Notificação de vulnerabilidades, ocorrências de segurança e gestão de incidentes.
[C10]	Gestão da continuidade do negócio	Reforço na necessidade de ter um plano de continuidade e contingência.
[C11]	Conformidade	Referente à necessidade de observar os requisitos legais, como a propriedade intelectual.

Fonte: Adaptado de (ABNT ISO 27002, 2005)

Esta norma considera que controles adicionais e recomendações não incluídas nessa norma podem ser necessários.

> *A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados onde necessários, para garantir que os objetivos de negócio e de segurança da organização sejam atendidos. (ABNT, 2005, p.x)*

2.10. Trabalhos relacionados

Esta seção apresenta três trabalhos relacionados com o tema de pesquisa e constitui a fonte precípua para elaborar uma estratégia de segurança da informação em empresas de desenvolvimento de software para aplicações móveis. Os trabalhos definem, respectivamente, modelo de planejamento para iniciativas de adoção de tecnologias móveis na interação entre organização e indivíduo (Machado, 2007), um roteiro para sistematizar e orientar pesquisas relacionadas a negócios móveis (Fouskas *41L al.*, 2005) e alinhamento da gestão de segurança da informação com as áreas de negócio: uma avaliação da contribuição das diretrizes da norma NBR ISO/IEC 27002:2005 (Fontes, 2011).

2.10.1. Análise dos trabalhos relacionados

Machado (2007) propõe em seu trabalho um modelo para planejamento das iniciativas de adoção de tecnologias móveis pelas organizações na interação com seus públicos-alvo. O modelo aborda as principais questões, impactos e riscos sobre adoção e uso organizacional de tecnologias móveis, bem como a percepção de especialistas sobre o que deve ser considerado pelas organizações ao planejar projetos de mobilidade e como os gestores planejam seus projetos de mobilidade.

A pesquisa realizada pelo autor limitou-se a grandes organizações e foi concentrada em apenas uma forma de tecnologia móvel (SMS corporativo). Outro aspecto desse trabalho refere-se à validação do modelo. O autor não aplicou as técnicas de validação ou experimentação, propondo a aderência do modelo em casos reais como trabalhos futuros. Por conseguinte, o modelo elaborado não contempla técnicas de segurança da informação, apenas o planejamento da adoção dessas tecnologias.

Figura 2.7: Modelo teórico do planejamento da adoção de iniciativas móveis na interação entre organização e indivíduo (Machado, 2007).

Fouskas *et al.* (2005) propõem um *roadmap* para sistematizar e orientar a pesquisa de negócios móveis em uma perspectiva metodológica e interdisciplinar, envolvendo interessados das áreas acadêmica e industrial. A Figura 2.8 ilustra esquematicamente as dimensões de pesquisa abordadas no *roadmap* e organizadas em quatro dimensões.

O trabalho de Foukas *et al.* (2005) contribui e estabelece diretrizes para identificar os desafios na adoção e uso das tecnologias móveis aos negócios. Contudo, a área de negócios móveis é dinâmica e alguns dos desafios identificados, tais como infraestrutura, treinamento, tecnologia, políticas e regulamentações devem ser revisadas, pois desde a elaboração do *roadmap* a área de mobilidade evoluiu.

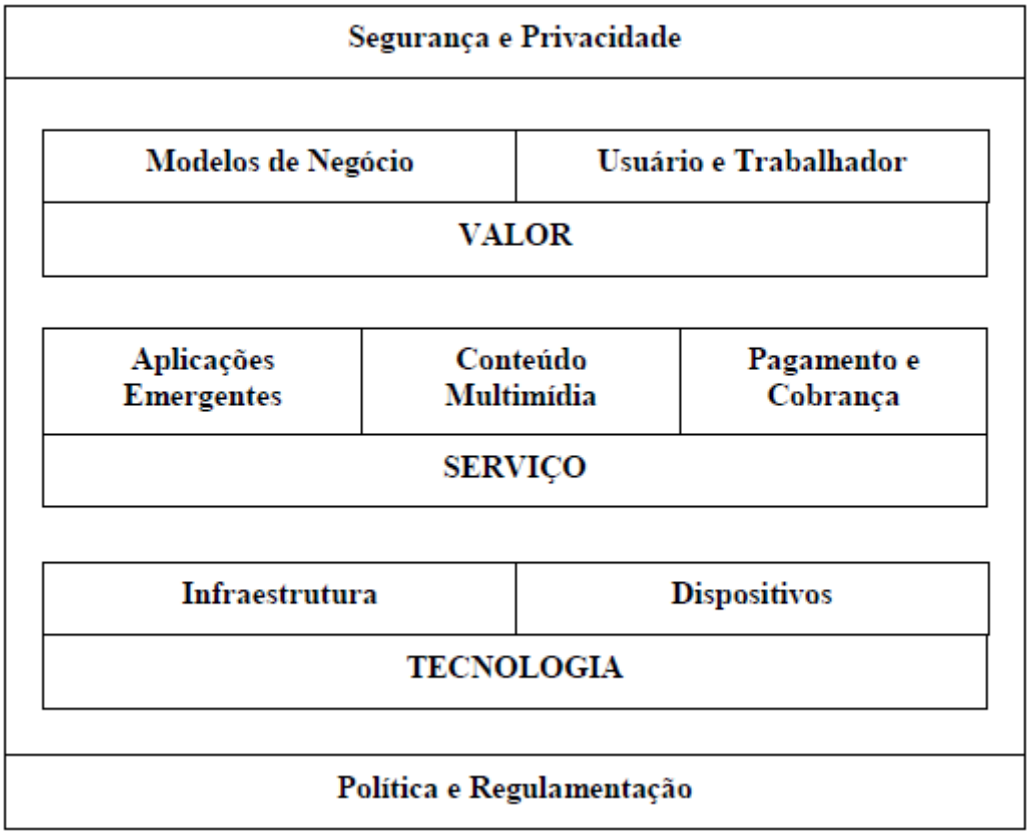

Figura 2.8. Dimensões de pesquisa do roadmap (Foukas et al., 2005, p. 359)

Fontes (2011) em seu trabalho busca identificar os elementos que devem compor um padrão mínimo para a política de segurança da informação de uma organização. No entanto, não trata de questões específicas de segurança da informação em empresas de desenvolvimento de software para aplicações móveis. Outro aspecto, é que o trabalho não apresenta técnica de validação, e sim, propõe aplicação futura em uma empresa.

2.11. Considerações Finais

A gestão de segurança da informação possui desafios que podem ser superados ao adotar técnicas que atendam as necessidades de um determinado contexto de aplicação. O desenvolvimento de software para dispositivos móveis é um exemplo de contexto específico e que exige uma estratégia que satisfaça suas bases e princípios.

Neste capítulo foram apresentados os componentes que fundamentam o arcabouço de uma estratégia de segurança da informação em empresa de desenvolvimento de software para dispositivos móveis com base nos trabalhos de Machado (2011), Fouskas *et al*. (2005) e Fontes (2011). Dentre os componentes estão os conceitos de gerenciamento de projetos, que apresenta áreas que auxiliam a elaboração de projetos; tecnologias, dispositivos e aplicações

móveis, ao qual aborda os desafios enfrentados por essa tecnologia; requisitos de segurança da informação, auxiliando na definição de ferramentas, normas e procedimentos para desenvolvimento de diretrizes de segurança. No próximo capítulo são discutidas as bases da construção da estratégia de segurança.

Capítulo

3

Bases da Estratégia de Segurança da Informação

3.1. Considerações iniciais

A massificação das tecnologias digitais móveis é uma das forças tecnológicas recentes mais importantes (Machado, 2007). Além da rápida disseminação entre as pessoas, as empresas vêm, cada vez mais, adotando esse tipo de tecnologia para atender a atual situação de mercado, embora nem sempre considerando todos os aspectos e riscos envolvidos nesse tipo de iniciativa. Como observado no Capítulo 2 na seção 2.6, às tecnologias móveis apresentam características próprias, introduzindo novas dimensões que as diferenciam das tecnologias convencionais, requerendo assim novas abordagens sobre sua adoção e uso.

No entanto, pesquisas visando explorar e entender os riscos e os desafios de segurança nas empresas de desenvolvimento de software para dispositivos móveis sob a percepção dos gerentes e especialistas em gestão de segurança da informação tem sido pouco retratado por autores, dentre eles: Andrade (2012), Fontes (2011), Boulhosa (2011), Wangham (2007), Machado (2007), Souza (2007), Sima (2006) e Fouskas *et al.* (2005).

Este capítulo apresenta as bases para uma estratégia de segurança da informação em empresa de desenvolvimento de software para dispositivos móveis visando identificar os principais desafios e riscos que as empresas podem enfrentar com a adoção dessa tecnologia, bem como apresentar soluções para minimizar o impacto desses riscos a essas empresas.

3.2. Segurança da informação nas aplicações móveis

Para Rodrigues, (2011) a maioria das empresas peca em segurança quando investe muito em software e hardware e esquece dos processos e do treinamento de pessoal. *"As pessoas devem conhecer a importância das políticas de segurança da empresa, o valor das informações e o impacto que o fornecimento de uma informação confidencial para alguém não autorizado pode causar"* (Rodrigues, 2011, p.58).

Como dito anteriormente, em empresas circulam muitas informações confidenciais que podem ser fornecidas para pessoas indevidas, causando danos irreparáveis. Geralmente, as pessoas que trabalham em um projeto não têm como mensurar o valor que uma informação tem para a organização e muito menos o impacto que a disponibilização da mesma para pessoas não autorizadas pode causar. Por esse motivo é importante que exista um processo que identifique, categorize e proteja todas as informações de um projeto.

Em projetos de desenvolvimento de software para dispositivos móveis, conforme descrito na Seção 2.6, são apresentados vários desafios para a empresa e os gerentes de projetos, pois se trata de uma tecnologia que possui suas próprias características, limitações e ameaças.

Dentre os vários desafios abordados destaca-se a segurança da informação, na qual estão relacionados riscos que se não gerenciados podem influenciar diretamente no projeto.

Os riscos associados a esses projetos são diferentes dos enfrentados por projetos clássicos, (Andrade, 2012). Na Tabela 3.1 têm-se os riscos mais incidentes e relevantes em projetos de desenvolvimento de software para dispositivos móveis.

Tabela 3.1: Riscos identificados em GPS para dispositivos móveis (Andrade, 2012)

Grupo	ID	Risco
Geral	**R01**	Rotatividade interna e externa de recursos humanos por motivos salariais e melhores condições de trabalho.
	R02	Assédio de recursos humanos pela concorrência por motivos de mão de obra qualificada.
	R03	Exposição de dados sigilosos ou aplicações estratégicas da empresa.
	R04	Alteração de escopo do projeto.
	R05	Mudança de plataforma e ferramentas de desenvolvimento.
	R06	Imperícia em definir e avaliar os processos organizacionais para o desenvolvimento e a implantação das aplicações móveis.
	R07	Mau uso do dispositivo móvel pela equipe de desenvolvimento e pelos usuários finais.
Específico	**R08**	Instalação de software não autorizado que prejudique o desempenho do dispositivo móvel na execução da aplicação.
	R09	Danos involuntários ao dispositivo móvel.

	R10	Comportamento instável do dispositivo móvel devido à presença de vírus.
	R11	Obsolescência programada dos dispositivos móveis.
	R12	Limitação das capacidades de processamento. Armazenamento e durabilidade dos dispositivos móveis ao executar as aplicações corporativas.
	R13	Incompatibilidade dos dispositivos móveis com as aplicações corporativas (especificações técnicas).
	R14	Perda ou roubo do dispositivo móvel.
	R15	Desalinhamento dos processos móveis com a estratégia da empresa (processos específicos em relação à mobilidade).
	R16	Redefinição de processos organizacionais existentes para o desenvolvimento e a implantação das aplicações móveis.
	R17	Mudança de layout das aplicações móveis (usabilidade, escolha do tipo do teclado, touch ou multitouch).
	R18	Problema de convergência entre aplicações móveis e sistemas organizacionais, ou seja, na integração entre sistemas internos ou externos.
	R19	Limitação de cobertura de sinal das operadoras de dados.
	R20	Limitação de largura de banda das operadoras de dados.
	R21	Ausência ou baixa interoperabilidade dos padrões de comunicação móvel.
	R22	Baixa qualidade de conexão dos dispositivos e das operadoras de dados.

Fonte: Andrade (2012)

Os riscos identificados por Andrade (2012) são organizados em dois grupos: gerais e específicos, no qual os riscos específicos correspondem aos riscos associados especificamente com o contexto de desenvolvimento de software para dispositivos móveis e os riscos gerais correspondem aos riscos comuns em projetos de desenvolvimento de software.

No entanto, esses riscos precisam ser gerenciados. Deve ser feita uma análise criteriosa, pois, dependendo da informação que seja divulgada indevidamente, esta poderá inviabilizar a continuidade do projeto. Todas as informações, independentemente da categoria na qual se enquadram, precisam ser identificadas e avaliadas quanto à probabilidade de serem disponibilizadas indevidamente, e quanto ao impacto que essa disponibilização poderá causar.

Os riscos identificados na Tabela 3.1 sustentam a particularidade do gerenciamento da segurança da informação, pois estão relacionados diretamente com os requisitos físicos e lógicos da segurança da empresa. Os requisitos físicos estão relacionados com algo que possa danificar a parte física da segurança e os requisitos lógicos estão relacionados com a segurança de dados e informações. Por exemplo, os riscos [R1], [R2], [R7], [R9] e [R14] estão diretamente ligados com os requisitos físicos de segurança da empresa, pois trata da gestão de pessoas envolvendo a grande rotatividade de pessoas dentro da empresa, pessoas

que já não faz parte da equipe e que mantém informações, acesso as dependências da empresa e ativos de uso particular da empresa.

No entanto, os riscos [R3], [R5], [R10], [R11], [R12], [R13], [R15], [R16], [R17], [R18], [R19], [R20], [R21] e [R22] estão relacionados com os requisitos lógicos de segurança da empresa, pois estão diretamente ligados aos ativos de informações e dados que, se expostos, podem trazer impactos prejudiciais à empresa.

Após essa identificação, os riscos deverão ser priorizados e classificados. A partir dessa lista deverá ser criado um plano de resposta aos riscos, no qual estarão às estratégias de mitigação e contingência dos riscos considerados mais críticos para o projeto auxiliando a empresa e o gerente de projetos na gestão de segurança da informação.

3.3. Desafios da segurança da informação em projetos de desenvolvimento de software para dispositivos móveis

Os desafios da segurança da informação em projetos de desenvolvimento de software para dispositivos móveis podem ser resultados da ocorrência de riscos proporcionados pela complexidade das tecnologias e negócios móveis e da necessidade de ligá-las com múltiplas áreas de conhecimento, condições e contextos.

No entanto, os riscos identificados por Andrade, (2012) caracterizam grandes desafios para a segurança da informação, pois fica clara a diferença entre gerenciar os riscos em um projeto clássico de software e um projeto de software no contexto móvel quando divididos em geral e específicos.

A Figura 3.2 ilustra os riscos categorizados em quatro grupos que afetam a segurança da informação da empresa apresentados no diagrama de Ishikawa, também conhecido como diagrama de espinha de peixe ou causa e efeito, é uma ferramenta gráfica que ilustra como diversos fatores podem estar ligados a problemas ou efeitos potenciais (PMI, 2008).

Originalmente utilizado no controle da qualidade de processos, o diagrama de Ishikawa se alastrou pelas mais diversas áreas e segmentos profissionais. Segundo o PMI (2008) trata-se de uma ferramenta utilizada na gestão de qualidade, mas também é aplicada nas atividades de identificação e análise de riscos. Seu formato simplificado é composto por uma estrutura principal (seta horizontal), pelas causas (linhas ou setas) e pelo efeito (caixa com a descrição do problema). As causas são ligadas a estrutura principal que por sua vez é apontada para o efeito. Extensões do diagrama também são aplicadas e abrangem subcausas e categorias. As subcausas são definidas como as causas potenciais que podem contribuir com

uma causa específica e as categorias são o agrupamento de causas a partir de fatores relacionados ao efeito.

Os riscos e suas relações são representados respectivamente pelos componentes **causas** e **subcausas** e os desafios, gerados pela incidência dos riscos, são representados pelo componente **efeito**.

Os grupos foram divididos em: Infraestrutura e Pessoal (relacionada diretamente com a segurança física), Equipamento e Informação (relacionada com a segurança lógica).

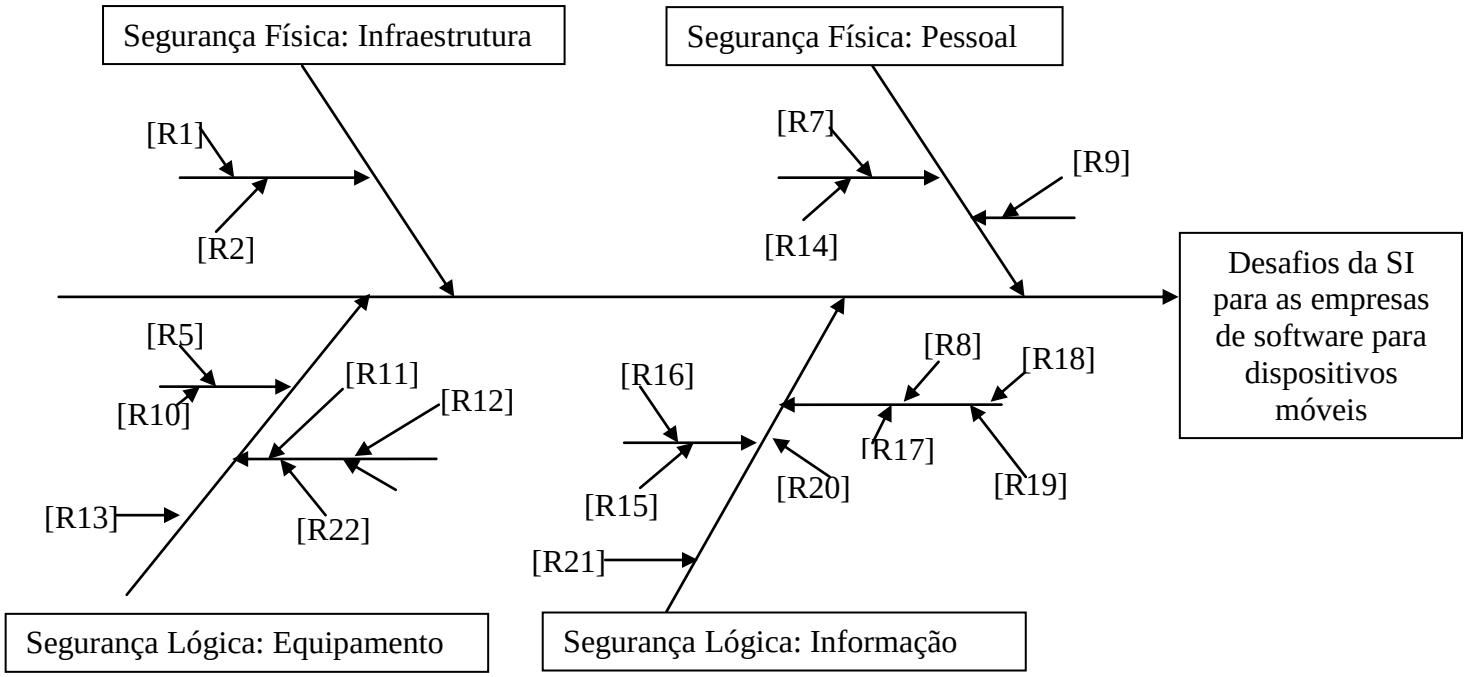

Figura 3.2: Diagrama de Ishikawa aplicado na SI para o GPS para dispositivos móveis

As categorias definidas na Figura 3.2 não seguem nenhum padrão estabelecido e sim formas de identificação de riscos para um melhor gerenciamento no impacto que os mesmos podem causar às empresas com relação à segurança da informação.

Uma análise mais apurada da Figura 3.2 permite observar que o diagrama foi dividido em Infraestrutura e Pessoal ao qual está associada diretamente a segurança física da empresa. As categorias Equipamentos e Informação estão relacionadas à segurança lógica que apresentam riscos que impactam diretamente no desenvolvimento do projeto afetando dados e informações da empresa.

A Tabela 3.3 apresenta os impactos que os riscos associados ao desenvolvimento de software para dispositivos móveis afetam na segurança da informação da empresa.

Tabela 3.3: Impactos dos riscos a segurança da informação em empresa de desenvolvimento de software para dispositivos móveis (elaborada pelo autor)

Requisitos de Segurança		**Riscos**	**Impacto na Segurança da Informação**
Físico	**Infraestrutura**	[R01] [R02]	As mudanças na composição da equipe do projeto impactam não somente no tempo de conclusão do projeto, mas também na segurança da informação, pois com a rotatividade de pessoas pode fazer com que informações importantes do projeto sejam divulgadas indevidamente.
	Pessoal	[R07] [R09] [R14]	Perda, roubo ou danos nos dispositivos móveis pelo uso inadequado, impactam diretamente na segurança da informação, pois informações importantes da empresa podem estar contidas no dispositivo.
Lógico	**Equipamentos**	[R05] [R10] [R11] [R12] [R13] [R22]	As mudanças de tecnologias fazem com que novas ferramentas e plataformas de desenvolvimento sejam adquiridas, com isso necessitando de novas instalações de softwares e hardwares, no que impacta na segurança dos dados, pois devido a alta demanda de serviços no desenvolvimento das aplicações móveis e pensando no prazo do projeto qualquer pessoa pode realizar instalações software e hardware não autorizado prejudicando a segurança das informações.
		[R08]	Com a redefinição de

	Informações	[R15] [R16] [R17] [R18] [R19] [R20] [R21]	processos organizacionais existentes para o desenvolvimento, implantação das aplicações móveis, o desempenho e testes dos softwares móveis podem ser prejudicados com a presença de aplicativos maliciosos ou não autorizados nos dispositivos móveis prejudicando a segurança dos dados gerados na empresa.

O impacto que esses riscos podem causar à empresa é irreparável, neste cenário a análise de riscos, como descrito na Seção 2.7.6 se concentra em ativos, ameaças e vulnerabilidades. Como apresentados na Tabela 3.3 vários riscos podem afetar os ativos da empresa através das ameaças e vulnerabilidades burlando a segurança da informação. No entanto, Tsoumas e Tryfonas (2004) reforçam a importância da automação da gestão da segurança da informação a fim de dar vazão à complexidade e variabilidade dos elementos da segurança.

3.4. Características da segurança da informação em empresas de desenvolvimento de software para dispositivos móveis

O desenvolvimento de software para dispositivos móveis é caracterizado por uma série de incertezas e desafios que envolvem desde a concepção das aplicações e serviços (Foukas *et al.*, 2005 *apud* Andrade, 2012) até a segurança da informação.

A partir do levantamento bibliográfico dos autores Andrade (2012), Fontes (2011), Boulhosa (2011), Wangham (2007), Machado (2007), Souza (2007), Sima (2006) e Fouskas *et al.* (2005), dos desafios e riscos que impactam a segurança da informação envolvendo os requisitos físicos e lógicos de segurança da empresa com adoção de e uso de tecnologias móveis e de desenvolvimento de software para dispositivos móveis fez-se necessário realizar uma pesquisa de campo com o objetivo de identificar e ratificar evidências que comprovassem os relatos e estudos da literatura sobre os desafios e riscos sob a ótica gerencial da segurança da informação no desenvolvimento de aplicações móveis.

Para o desenvolvimento da estratégia foram analisados 15 (quinze) documentos de segurança da informação de empresas do segmento de Tecnologia da Informação (TI). Na solicitação do documento foi informado que o nome da empresa é sigiloso. As 15 empresas estão distribuídas em quatro segmentos de TI conforme apresentado na figura 3.3.

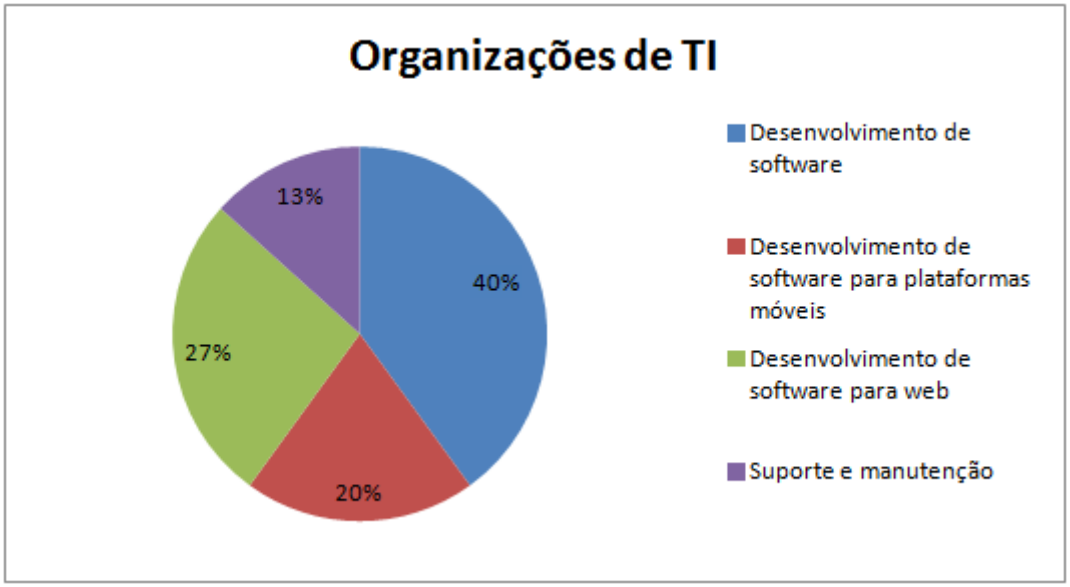

Figura 3.3: Percentual das organizações pesquisadas por segmento de negócios

A análise foi realizada para verificar os tópicos triviais que as empresas tratam com relação à política de segurança e identificar as diferenças dos documentos.

No entanto, a análise foi dividida entre as empresas do segmento de desenvolvimento de software para dispositivos móveis e demais empresas do setor de TI, podendo realizar uma análise mais apurada dos requisitos e controles abordados nos documentos de segurança das empresas dos dois segmentos.

Todas as empresas analisadas estão no mercado há mais de 10 anos e possui um documento de segurança pelo menos há cinco anos, o que fortalece a pesquisa para uma melhor análise para desenvolvimento de uma estratégia para empresas de desenvolvimento de software para dispositivos móveis.

Uma resposta interessante em todas as empresas pesquisadas foi o fato de tomarem como base a Norma ISO 27002. Tal fato reforça o estudo em questão, uma vez que essa norma foi tomada como base para análise dos controles da estratégia de segurança da informação apresentada neste trabalho.

3.5. Análise dos controles dos documentos de segurança da informação

Conforme descrito na seção 2.9.2 deste trabalho, a norma ISO 27002 define 133 controles para gestão de segurança da informação.

Para análise e definição da estratégia foi definido que um controle seria referenciado quando fosse citado pelo menos por 60% das empresas. As empresas foram divididas em dois segmentos: "Segmento 1", no qual são as empresas de desenvolvimento de software do contexto móvel, totalizando três empresas e "Segmento 2", ao qual são classificadas as empresas do segmento de desenvolvimento de software no contexto clássico, desenvolvimento de software para web e empresas de suporte e manutenção no total de 12 empresas.

Os controles foram classificados por lógico e físico. A Tabela 3.4 apresenta os controles da norma e a sua referência pelas empresas quanto do documento de segurança da informação do segmento software no contexto móvel.

Tabela 3.4: Classificação dos controles das empresas do "Segmento 1"

Controles em comum dos documentos de segurança	Percentual de empresas	Controle referente a norma ISO 27002
Requisitos físicos		
Proteção do prédio	100%	Segurança física e do ambiente
Monitoramento de entradas de pessoas na empresa	66%	Segurança física e do ambiente
Proteção da infraestrutura	100%	Gestão da continuidade do negócio
Perda do dispositivo móvel	66%	Classificação e controle dos ativos de informação
Requisitos lógicos		
Cópias de segurança	100%	Controle de acesso
Monitoramento de uso de softwares	66%	Segurança física e do ambiente
Instalação de hardware e softwares não autorizados	66%	Segurança física e do ambiente
Uso de dispositivos portáteis e móveis	100%	Classificação e controle dos ativos de informação
Testes e simulações nos dispositivos móveis	100%	Segurança física e do ambiente
Acesso à rede para uso de dispositivos móveis	66%	Segurança física e do ambiente

Conscientização e treinamento	66%	Política organizacional
Uso de e-mail pessoal e corporativo	100%	Gerenciamento de operações e comunicações
Uso de softwares de comunicação	100%	Gerenciamento de operações e comunicações
Segurança da rede	100%	Gerenciamento de operações e comunicações
Transporte das informações	66%	Gerenciamento de operações e comunicações
Controle de senha	100%	Controle de acesso

Para uma análise mais apurada dos dados, a tabela 3.5 apresenta os controles utilizados pelas empresas quanto do documento de segurança da informação das empresas do "Segmento 2" .

Tabela 3.5: Classificação dos controles das empresas do "Segmento 2"

Controles em comum dos documentos de segurança	**Percentual de empresas**	**Controle referente a norma ISO 27002**
Requisitos físicos		
Proteção da infraestrutura	100%	Segurança física e do ambiente
Proteção de equipamento	100%	Segurança física e do ambiente
Controle de entrada e saída de pessoas na empresa	100%	Gestão de continuidade do negócio
Requisitos lógicos		
Cópias de segurança	100%	Controle de acesso
Treinamento	70%	Controle de acesso
Uso de softwares de comunicação	80%	Segurança física e do ambiente
Autenticação e senha	90%	Política organizacional
Combate a vírus	100%	Gerenciamento de operações e comunicações
Controle do sistema (documentação)	100%	Gerenciamento de operações e comunicações

Observa-se que as empresas do "Segmento 1" adotou características específicas dos controles de segurança da informação com relação às empresas do "Segmento 2". Na Tabela 3.6 é possível analisar a veracidade das proposições definidas no plano do levantamento exploratório.

Tabela 3.6: Controles comum e específico das empresas de desenvolvimento do "Segmento 1" e "Segmento 2"

Controles para segurança da informação	
Comum (contexto clássico e móvel)	• Proteção da infraestrutura • Monitoramento de entrada e saída de pessoas • Cópias de segurança • Treinamento • Uso de softwares de comunicação • Controle de senha
Específico (contexto móvel)	• Monitoramento de uso de softwares • Uso de dispositivos portáteis e móveis • Acesso à rede para uso de dispositivos móveis • Uso de e-mail pessoal e corporativo • Segurança da rede • Transmissão das informações • Testes e simulações nos dispositivos móveis

A Tabela 3.6 apresenta os controles similares entre os documentos de segurança da informação das empresas, no item Comum ("Segmento 1" e "Segmento 2") e os controles específicos das empresas do contexto móvel, podendo verificar as diferenças de alguns requisitos de segurança entre as empresas. Além dos controles analisados, todos os documentos apresentam os seguintes requisitos: apresentação, objetivos, abrangência da norma, regras gerais do documento e gerenciamento dos riscos, inventário dos ativos, as penalidades (caso do não cumprimento das regras), divulgação do documento de segurança e plano de continuidade do negócio, no qual são requisitos importantes e básicos para formulação de um documento de segurança.

No entanto, um fato interessante é que os documentos foram desenvolvidos, mas não há um acompanhamento das regras e procedimentos estabelecidos, pois não existe um comitê especifico para a segurança da informação. Esse fato ocorre em todas as empresas pesquisadas nos dois segmentos.

Nas empresas do "Segmento 1" um fato importante é que o documento foi divulgado apenas uma vez e não existe atualização do mesmo. Ou seja, poucas pessoas tem conhecimento das regras e procedimentos de segurança, o que resulta nos problemas que foram abordados pelas empresas classificados na Tabela 3.7.

Tabela 3.7: Problemas enfrentados pelas empresas

#	Problemas	Descrição
[P1]	Acesso restrito em áreas críticas das empresas	Não existe restrição ao acesso de pessoas em áreas críticas da empresa, ou seja, todos tem acesso a todos os setores, o que impacta diretamente na segurança de dados e informações.
[P2]	Uso de dispositivos móveis	Não existe o controle do uso dos dispositivos móveis na empresa, já que a empresa utiliza os mesmos para uso específico, nos quais são realizados testes e simulações das aplicações, no entanto, o uso particular não é controlado, assim esses aparelhos ficam interligados diretamente na rede da empresa.
[P3]	Uso de emails	O uso de emails dentro da empresa é totalmente livre, todos utilizam seus emails pessoais para enviar e receber informações importantes da empresa.
[P4]	Instalação de software e hardware	Todos têm acesso diretamente à instalação de software e hardware, caso alguém necessite de algum aplicativo a instalação é realizada sem nenhuma restrição, o que está afetando os equipamentos com relação à segurança.
[P5]	Acesso a redes sociais	Não existe controle de acesso a softwares, sistemas e internet. Assim o uso dessas aplicações é livre, o que está causando sérios problemas com relação à divulgação de informações importantes da empresa.
[P6]	Compartilhamento de dados e informações na rede	A rede da empresa é aberta, onde dados e informações são trafegadas com facilidade, tanto informações da empresa e pessoal.

A tabela 3.7 apresentou os problemas expostos de forma geral pelas empresas do "Segmento 1", no entanto nem todos os problemas foram abordados por todas as empresas.

O problema [P1] "Acesso restrito em áreas críticas da empresa" foi destacado por duas empresas, os problemas [P2] "Uso de dispositivos móveis", [P3] "Uso de emails", [P4] "Instalação de software e hardware" e [P5] "Acesso a redes sociais" foram abordados pelas três empresas, no qual as mesmas ressaltam que existe uma dificuldade grande com relação ao controle dos problemas [P2], [P3] e [P4], uma vez que a atualização e acesso a dados acontecem constantemente e controlar o uso de email, a instalação a software e acesso aos dispositivos móveis podem atrasar as atividades do projeto. Por fim, o problema [P6] foi destacado por uma empresa, em que a mesma teve prejuízos com saídas de informações

indevidas da empresa por meio da rede.

Pode-se observar que as empresas adotaram o documento de segurança, no entanto, estão enfrentando dificuldades na aplicação do mesmo.

Neste cenário, é essencial o desenvolvimento de uma estratégia de segurança da informação para suprir as deficiências de segurança enfrentadas pelas empresas de desenvolvimento de software para dispositivos móveis, uma vez que é uma tecnologia que vem crescendo constantemente aumentando os riscos e desafios para a empresa. Mas, se existir um documento que apresente técnicas e procedimentos de segurança, abordando requisitos de proteção, o impacto negativos dos riscos podem ser menores.

3.6. Considerações finais

A segurança da informação em empresas de desenvolvimento de software para dispositivos móveis exige uma atenção em alguns pontos em específico, tais como, a identificação e ocorrência de riscos e maior precisão no planejamento da política de segurança da informação. Esses pontos permitem conduzir a segurança das informações com maior eficácia, não somente em alguns ativos e sim em todos ativos da empresa desde a infraestrutura até o desenvolvimento final do software.

Da compreensão desses conteúdos, é possível observar diferentes problemas abordados nas empresas do contexto clássico e móvel. Este capítulo apresentou alguns dos principais riscos e desafios da segurança da informação encontrados em empresas de desenvolvimento de software para dispositivos móveis e foi baseado na literatura com análises de documentos de segurança da informação de empresas.

Capítulo

4

Estratégia de Implantação de Segurança da Informação

4.1. Considerações iniciais

Com os riscos e desafios da segurança da informação em empresas de desenvolvimento de software para dispositivos móveis, a estratégia proposta nesta dissertação tem como objetivo orientar o processo de implantação de uma estratégia de segurança da informação em um ambiente organizacional de desenvolvimento de software para dispositivos móveis abordando elementos de segurança envolvendo ativos físicos e lógicos da empresa. Tal estratégia é baseada nos requisitos e controles das normas ISO 27001, ISO 27002 e análise de documentos de segurança da informação de empresas do setor de TI.

As duas normas apresentam requistos de segurança para todo tipo de empresa, no entanto, os requisitos e controles utilizados para a proposta desta dissertação foram implementados com base nas características e desafios das empresas de aplicações móveis descritas no Capítulo 3.

Conforme descrito nas seções 2.9.1 e 2.9.2, as Normas ISO não citam quais linhas de trabalho devem ser adotadas. Apenas apresenta requisitos e controles para que uma organização possa estruturar um SGSI. Portanto com o crescimento da tecnologia móvel, em que empresas de desenvolvimento de software estão adotando essa tecnologia com o intuito de suprir a alta demanda vinda dos usuários, elaborou-se uma estratégia com o objetivo de proporcionar um método lógico para implantar segurança da informação em empresas de desenvolvimento de software para aplicações móveis cuidando da infraestrutura da empresa e do ciclo de vida do projeto. Na Figura 4.1 apresenta-se a estratégia proposta para implantação da segurança da informação em empresas de desenvolvimento de software para aplicações móveis.

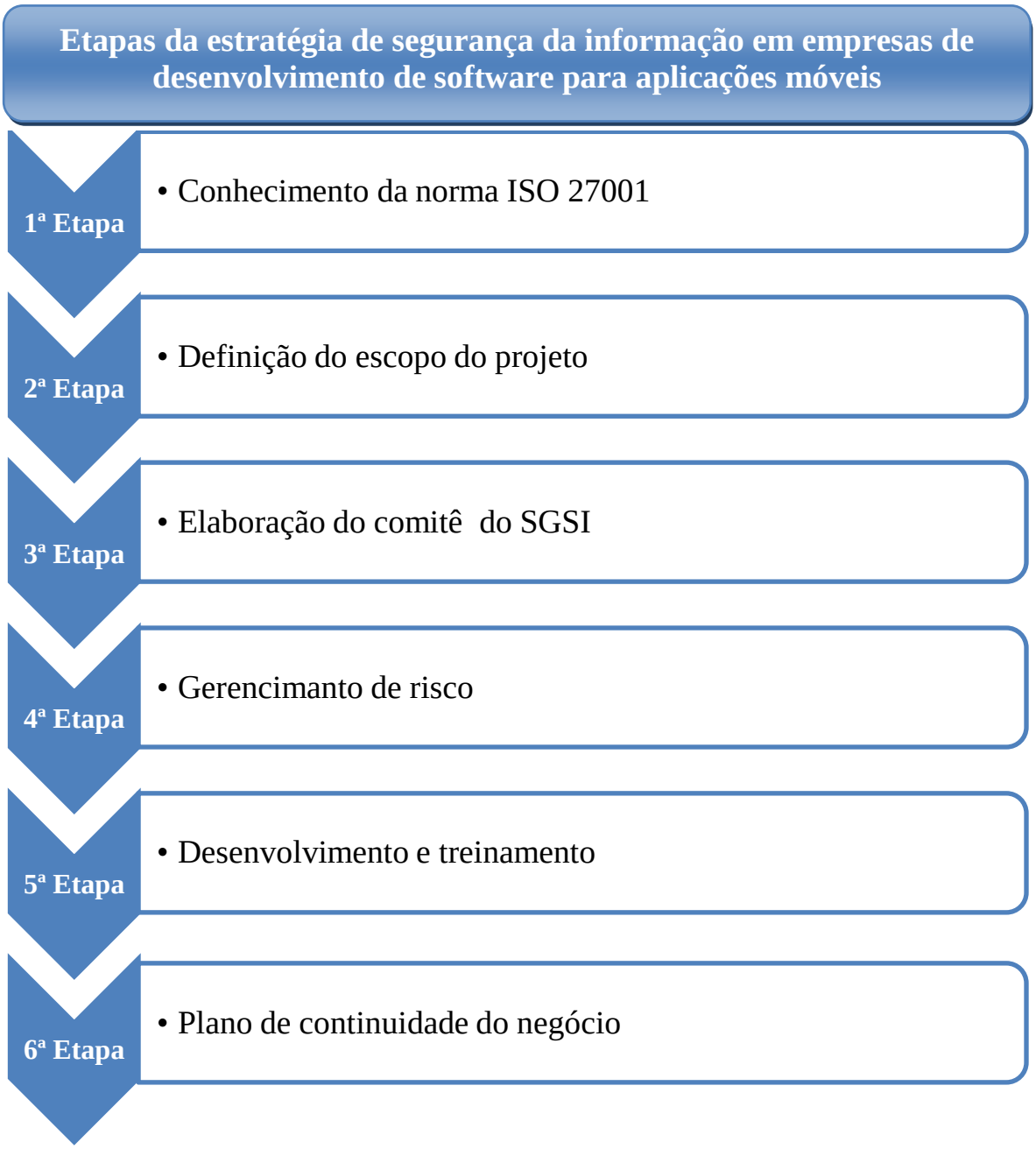

Figura 4.1: Estratégia de segurança da informação

Nas seções a seguir são descritas as etapas da estratégia apresentado na Figura 4.1 de forma detalhada.

4.2. Contribuição das normas ISO 27001 e ISO 27002 para a estratégia proposta

Para o desenvolvimento da estratégia de segurança da informação as normas ISO 27001 e ISO 27002 foram fundamentais. As mesmas apresentam requistos de segurança para todo tipo de empresa, no entanto, cada organização deve identificar quais as seções aplicáveis.

Os requisitos e controles utilizados para a proposta desta dissertação foram implementados com base nas características e desafios das empresas de aplicações móveis descritas no Capítulo 3.

4.3. Início do Projeto de Segurança

A estratégia de segurança da informação estará associada a todos colaboradores da empresa.

1ª Etapa: Conhecimento da norma ISO 27001

A fase de conhecimento da norma ISO 27001 deve ocorrer no início do projeto, para compreensão dos requisitos necessários de segurança do ambiente, na qual deverá ser realizados pelo gerente de segurança com a leitura dos requisitos 01, 02 e 03 detalhados no anexo A.

Primeiramente é realizada a análise do requisito 01 do escopo, no qual é definido o comitê gestor de segurança da informação (SGSI).

No requisito 02 é apresentada a norma ISO 27002 que contêm as melhores práticas adotadas para segurança da informação.

No requisito 03 têm os termos e definições relacionados à segurança da informação, por exemplo, a definição de ameaças, vulnerabilidades entre outros, como apresentado no Capítulo 2 desta dissertação. Após a leitura do Requisito 03 é possível realizar a leitura dos próximos requisitos e implantar a estratégia de segurança em empresa de desenvolvimento de software para dispositivos móveis.

2ª Etapa: Definição do escopo

De acordo com PMBOK (2008) o escopo do projeto é composto dos processos, conforme apresentado na Figura 4.2, para garantir que o projeto inclua todo o trabalho exigido, e somente o trabalho exigido, para completar o projeto com sucesso. A definição do escopo se segue ao entendimento dos objetivos do projeto, dos resultados esperados e à descrição sumária do trabalho a ser realizado.

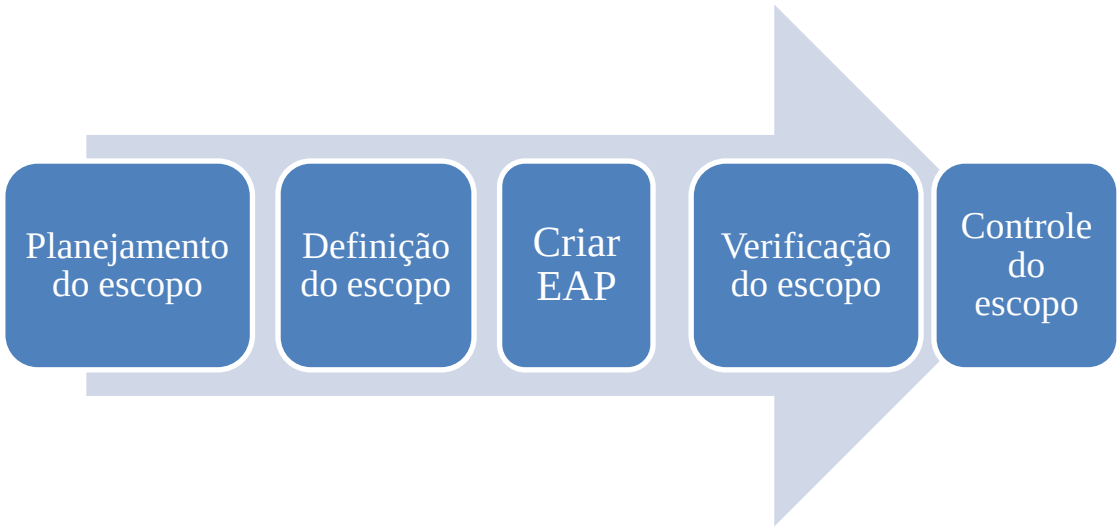

Figura 4.2: Processos para definição do escopo

A etapa do escopo da estratégia ocorre após a conhecimento da norma ISO 27001. É neste momento em que se determina a viabilidade do projeto, com base nos processos apresentados na Figura 4.2.

Planejamento do escopo: Criação de um plano de gerenciamento do escopo que documenta como o escopo do projeto será definido, verificado e controlado e como a estrutura analítica do projeto (EAP) será criada e definida.

Nesta fase são realizadas estimativas iniciais de custo, alocação de pessoal, cronograma, objetivos e metas abrangendo duas etapas:

- **Diagnóstico da situação atual:** verifica-se a existência de alguma política de Segurança da Informação, aproveitando-se de controles já implementados.
- **Planejamento do SGSI e preparação para a sua implantação:** nesta etapa, conforme as normas ISO/IEC 27001 e ISO/IEC 27002 recomenda-se a formação do comitê responsável pela implantação do SGSI na organização.

Definição do escopo: Desenvolvimento de uma declaração do escopo detalhada do projeto como a base para futuras decisões do projeto. Inclui também o levantamento dos ativos que

serão envolvidos, tais como: Equipamentos; Sistemas; Nome da organização; Estrutura de comunicação (Internet, correio eletrônico); Pessoas; Serviços; Infraestrutura de rede interna e externa e Classificação da informação.

Criar EAP: Criação da Estrutura Analítica do Projeto – decomposição hierárquica orientada à entrega do trabalho a ser executado pela equipe do projeto para atingir os seus objetivos e criar as entregas necessárias.

Verificação do escopo: A verificação do escopo é o processo de obter o aceite formal do escopo do projeto pelas partes envolvidas (patrocinador, cliente, etc). Isto exige uma revisão dos produtos e resultados do trabalho para garantir que tudo foi completado correta e satisfatoriamente.

Controle do escopo: O controle do escopo consiste em (a) influenciar os fatores que criam mudanças no escopo para garantir que as mudanças sejam discutidas e combinadas (b) determinar que uma mudança no escopo ocorreu, e (c) gerenciar as mudanças efetivas quando ocorrerem. O controle das mudanças do escopo deve se integrar aos demais processos de controle (controle de prazo, controle de custo, controle de qualidade).

Para definição do escopo da estratégia de segurança foram abordados e classificados requisitos analisados dos documentos de segurança da informação e das literaturas estudadas. Dentre os autores destaca-se: Fontes (2011) e Souza (2007).

Requisitos para definição do escopo

a) Custo: Implantação da norma ISO 27001;

b) Prazo para implantação da norma;

c) Descrição de atribuição a clientes, colaboradores, fornecedores incluindo termos de responsabilidade e acordos confidencialidades;

d) Elaboração da política de segurança da informação, caracterizada pelo conjunto de princípios e valores estruturais, nos quais a empresa explicita os seus propósitos, traduzidos em regras específicas para proteger as informações que são de sua propriedade ou que estão sob sua responsabilidade;

e) Classificação de ativos de software utilizados como programas fontes, ferramentas de apoio ao desenvolvimento;

f) Definição de equipamentos de Tecnologia da Informação que deverão dar suporte à Política que estão relacionados com os equipamentos computacionais (computadores de grande porte, microcomputadores, notebooks, etc.), equipamentos de comunicação

(roteadores, modens, switchs, etc.), dispositivos de entrada e saída (discos, impressoras, etc.);

g) Levantamento da estrutura de comunicação como ferramentas de conversação instantânea;

h) Classificação das pessoas envolvidas na empresa como direção, gerentes, colaboradores dos setores da empresa;

i) Definição de serviços realizados pela empresa que são as atividades desenvolvidas;

j) Levantamento da infraestrutura de equipamentos como no-breaks, geradores de eletricidade alternativa, quadros elétricos, equipamentos de refrigeração, etc.

3ª Etapa: Elaboração do comitê do SGSI

Nesta fase com a aprovação da direção é possível implementar o SGSI com os responsáveis de cada setor da empresa, ficando a cargo do Gerente de Segurança da Informação e do Analista de RH (Recursos Humanos) a responsabilidade de organizar o comitê gestor de segurança da informação. A figura 4.3 apresenta os principais critérios que farão parte da elaboração do SGSI.

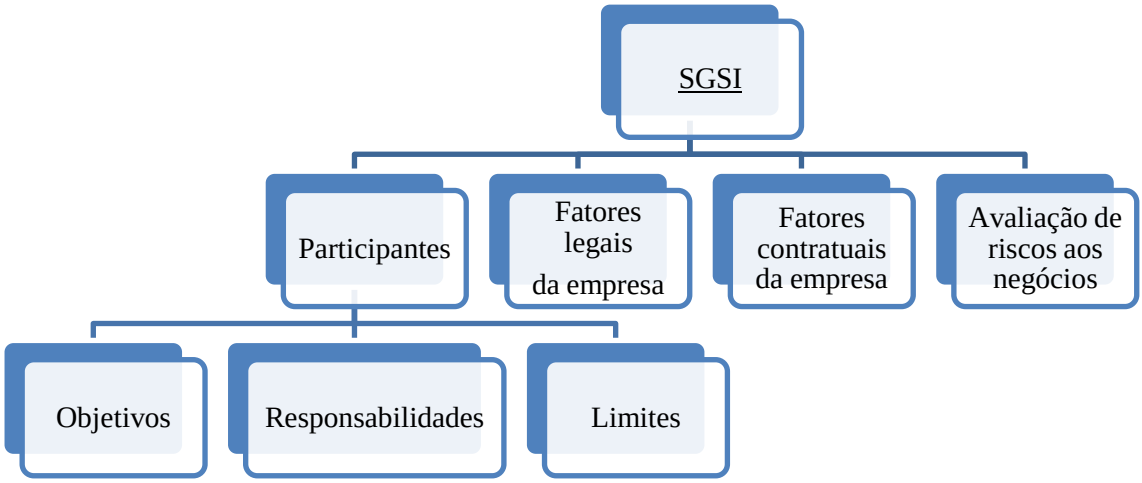

Figura 4.3: Critérios para elaboração do SGSI (adaptado da norma ISO 27001)

a) Participantes do SGSI: o SGSI será formado por representante de cada setor que são responsáveis pelos seus departamentos na empresa. A participação do departamento do RH é essencial, pois este detém os dados referentes aos colaboradores e, também, é responsável por gerenciar todos os treinamentos internos e externos. Fica a cargo do

gerente de segurança da informação o treinamento dos colaboradores, definições de *hardware* e *software*, além de implantar, configurar e monitorar toda atividade de troca e armazenamento de informações da empresa esclarecendo dúvidas quanto aos objetivos, responsabilidades e limites do SGSI.

1. Objetivos do SGSI: o objetivo do SGSI é ser um comitê aberto a discussões e voltado ao desenvolvimento contínuo do projeto de segurança da informação.
2. Responsabilidades do SGSI: o SGSI é responsável por divulgar a política da segurança da empresa e pelas auditorias internas.
3. Limites de atuação do SGSI: o SGSI é subordinado à direção da empresa.

b) Observar fatores legais e contratuais envolvidos nos negócios da empresa: o SGSI deve respeitar as leis federais, estaduais e municipais, bem como todos os contratos existentes com seus parceiros.
c) Critérios para avaliação de riscos aos negócios: devem ser desenvolvidos em conjunto com seus parceiros de negócios, sendo associado às leis e contratos existentes.
d) Para o desenvolvimento do SGSI deve ser adotado o modelo PDCA, discutido na seção 2.5.2 deste trabalho.

Após os requisitos apresentados anteriormente é apresentado na Figura 4.4 à metodologia do comitê gestor de sistema de informação para adoção.

Figura 4.4: Metodologia do comitê gestor de sistema de informação
Fonte: adaptado de Campos, (2011)

Interações no SGSI

Para melhor entender a Figura 4.4 são apresentadas as interações no SGSI:

- **Gestão de Negócios (GN):** processo representado pelos diretores da empresa. São os patrocinadores do projeto e os membros responsáveis por auditar todos os trabalhos do SGSI aplicando o conceito PDCA.
- **Gestão de Recursos (GR):** este processo é composto por dois departamentos:
  - **Recursos Humanos (RH):** responsáveis pelos treinamentos, construção das regras, mediação de conflitos entre setores da empresa;
  - **Suporte e Manutenção (SM):** responsável pelos treinamentos dos recursos informatizados *(hardware e software)* e também por manter a infraestrutura.
- **Responsáveis dos Setores:** são todos os gerentes, supervisores e encarregados de todos os setores da empresa que participam do desenvolvimento, aplicação e multiplicação da política de segurança da informação.
- **Sistema de Gestão de Segurança da Informação:** formado por todos os

componentes do SGSI. Responsável por criar, manter e desenvolver a política de segurança da informação.

4ª Etapa: Gerenciamento de Risco

Nesta etapa é realizado o diagnóstico da segurança para o escopo definido, através da identificação dos ativos de informação envolvidos e do mapeamento de todas as ameaças relacionadas a estes. Para cada ameaça deve ser determinado o nível de risco envolvido.

No desenvolvimento da análise de riscos, a ISO 27005 ocupa um papel importante. Conforme apresentado na seção 2.7.6, esta norma trata detalhadamente a questão de análise de riscos, apresentando diversas opções e estratégias de condução da análise de riscos que podem ser escolhidas em função do tempo e orçamento existente e dos objetivos.

Após o diagnóstico dos riscos, deve-se definir junto à alta administração da empresa, quais os níveis de risco aceitáveis e não aceitáveis. Entre os não aceitáveis, pode-se escolher uma entre as seguintes opções:

• **Reduzir o nível de risco:** através da aplicação de controles de segurança.

• **Aceitar o risco:** considerar que ele existe, mas não aplicar qualquer controle.

• **Transferir o risco:** repassar a responsabilidade de segurança a um terceiro, como, por exemplo, um *data center*.

• **Negar o risco**: esta é a opção menos recomendada.

Três pontos devem ser levados em consideração quanto ao gerenciamento do risco:

a) O que deve ser protegido;
b) Análise de risco (contra quem ou contra o que deve ser protegido);
c) Avaliação de riscos (análise da relação custo/benefício)

O relatório de análise de risco deve conter identificação e classificação de ativos e processos de negócio, análise de ameaças e vulnerabilidades, e análise e parametrização de riscos e definição de tratamento dos riscos.

O Gerenciamento de Riscos é um processo contínuo, que não termina com a implementação de uma medida de segurança. Através de uma monitoração constante, é possível identificar quais áreas foram bem sucedidas e quais precisam de revisões e ajustes.

Nessa etapa é estimado o impacto que um determinado risco pode causar ao negócio. Como é praticamente impossível oferecer proteção total contra todas as ameaças existentes, é preciso identificar os ativos e as vulnerabilidades mais críticas, possibilitando a priorização dos esforços e os gastos com segurança. Uma vez que os riscos tenham sido identificados e a

organização definiu quais serão tratados, as medidas de segurança devem ser de fato implementadas.

Nessa etapa ainda podem ser definidas medidas adicionais de segurança, como os Planos de Continuidade dos Negócios – que visam manter em funcionamento os serviços de missão-crítica, essenciais ao negócio da empresa, em situações emergenciais – e *Response Teams* – que possibilitam a detecção e avaliação dos riscos em tempo real, permitindo que as providências cabíveis sejam tomadas rapidamente.

Todo o processo do gerenciamento das áreas de risco de segurança da informação, praticamente desenvolve-se em sete etapas, conforme a Figura 4.5.

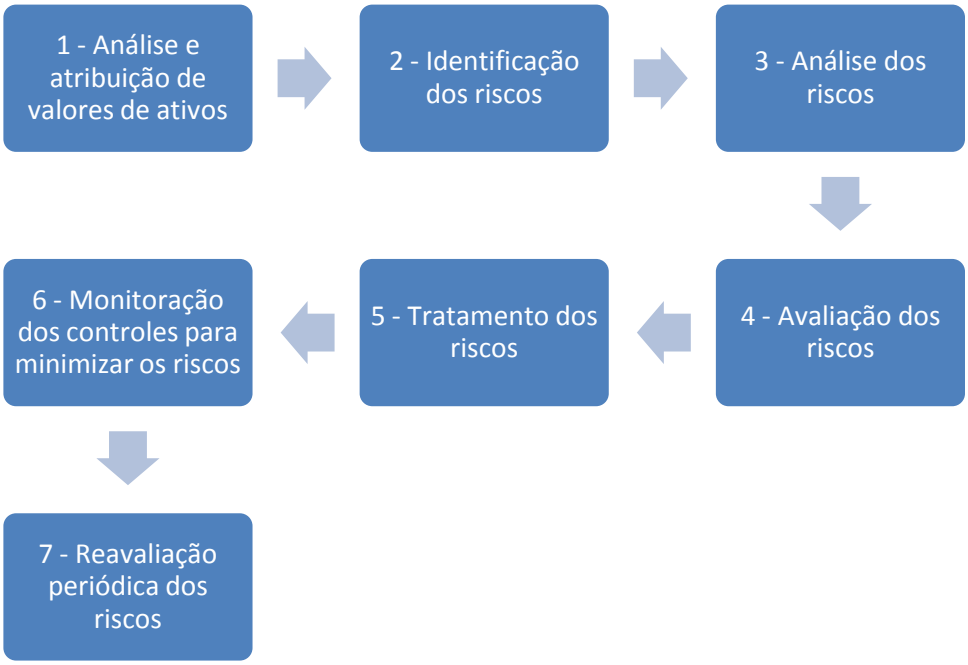

Figura 4.5: Gerenciamento das áreas de risco de segurança da informação

Descrição das etapas do gerenciamento de riscos:

1 - Identificação dos recursos a serem protegidos – *hardware*, rede, *software*, dados, informações pessoais, documentação, suprimentos;

2 - Identificação dos riscos (ameaças) - que podem ser naturais (tempestades, inundações), causadas por pessoas (ataques, furtos, vandalismos, erros ou negligências) ou de qualquer outro tipo (incêndios);

3 - Análise dos riscos (vulnerabilidades e impactos) - identificar as vulnerabilidades e os impactos associados;

4 - Avaliação dos riscos (probabilidade de ocorrência) - levantamento da probabilidade da ameaça vir a acontecer, estimando o valor do provável prejuízo. Esta avaliação pode ser feita com base em informações históricas ou em tabelas internacionais;

5 - Tratamento dos riscos (medidas a serem adotadas) - maneira como lidar com as ameaças. As principais alternativas são: eliminar o risco, prevenir, limitar ou transferir as perdas ou aceitar o risco;

6 - Monitoração da eficácia dos controles adotados para minimizar os riscos identificados;

7 - Reavaliação periódica dos riscos em intervalos de tempo não superiores a 6 (seis) meses;

Com a interpretação da norma ISO 27002 base nos riscos identificados pelas empresas em seus documentos de segurança da informação e em literaturas, foi possível realizar o levantamento dos riscos que impactam a segurança da informação em um ambiente de desenvolvimento de software para dispositivos móveis conforme apresentado na tabela 4.1.

Tabela 4.1: Riscos identificados com impacto a SI em empresas de desenvolvimento de software para dispositivos móveis

Risco	Descrição	Impacto à segurança da informação
[R-A]	Perda ou roubo do dispositivo móvel	Exposição de dados sigilosos ou aplicações estratégicas da empresa;
[R-B]	Acesso indevido à rede da empresa para uso de dispositivos móveis	Acesso a informações da empresa
[R-C]	Mau uso dos dispositivos móveis nas aplicações da empresa	Prejudicando testes e simulações das aplicações
[R-D]	Instalação de software não autorizado em dispositivos móveis da empresa	Expor informações dos resultados dos testes das aplicações
[R-E]	Interdições ou interrupções de serviços essenciais através do acesso à rede da empresa	Vulnerabilidade das informações através do mau uso de principalmente de equipamentos móveis e portáteis
[R-F]	Acesso à empresa de pessoas sem identificação	Acesso a informações indevidas
[R-G]	Omissão, erro, negligência, imprudência, imperícia, sabotagem e perda de conhecimento de pessoas devido à nova tecnologia.	Revelação de informações sensíveis.
[R-H]	Assédio dos recursos humanos pela concorrência devido a falta de mão de obra qualificada	Rotatividade de pessoal, com acesso a informações da empresa

5ª Etapa: Desenvolvimento e Treinamento do Documento de Segurança

Para o desenvolvimento do documento de segurança da informação dois requisitos são abordados:

- Requisitos de Segurança Lógica e;

- Requisitos de Segurança Física.

Para definição dos requisitos de segurança lógica são considerados os ativos de dados, informações, acesso, restrição. Já para a definição dos requisitos físicos os ativos como infraestrutura e pessoal são abordados.

Após o desenvolvimento do documento de segurança, o mesmo deve ser publicado para todos os colaboradores da empresa, bem como realizar treinamento identificando todos os itens abordados. Para definição dos requisitos físicos e lógicos de segurança da informação, foram consideradas as bases da estratégia de segurança apresentada no capítulo 3.

Requisitos de segurança do ambiente físico

a) Áreas de Segurança:

- Deverá ser estabelecido o perímetro físico do prédio da empresa, identificando todas as suas "fronteiras" e identificados todos os pontos de acesso.

b) Controle de entrada e saída de pessoas:

- Devem ser classificadas todas as áreas do prédio da empresa para acesso, quanto à criticidade – alta criticidade, média criticidade, baixa criticidade e sem criticidade – e quanto à restrição – alta restrição, média restrição, baixa restrição e sem restrição;
- Devem ser criados mecanismos para identificação e controle de acesso de pessoas que não sejam funcionários, às instalações da empresa, indicando quem teve acesso, data e hora e quem autorizou o acesso;
- Os funcionários terão seu controle de acesso através do registro de ponto eletrônico, que deverá ser disponibilizado nas portarias de acesso. Todos deverão registrar a entrada e saída, mesmo os liberados do controle de ponto.
- Devem ser criados mecanismos especiais que protejam o acesso aos locais considerados de alta restrição.

c) Autonomia do departamento de Suporte e Manutenção (SM):

- O departamento de SM possui total autonomia para atuar sobre os equipamentos da empresa, sem prévio aviso, no que se refere aos seguintes tópicos:
  - Realização de auditoria local ou remota em dispositivos móveis e desktop;
  - Definição de perfis de usuários cujos privilégios não permitam a realização de atividades tidas como prejudiciais ao hardware e software ou à rede com um todo;
  - A instalação e configuração de softwares de monitoramento em dispositivos móveis e desktop;

- A desinstalação de quaisquer softwares considerados prejudiciais à rede principalmente nos dispositivos móveis;
- Credenciamento e descredenciamento de usuários.

d) Proteção do prédio, equipamentos e infraestrutura:

- As instalações prediais devem ser seguradas, pelo menos contra incêndio;
- O cabeamento elétrico, que alimenta e interliga os vários equipamentos, deve ser protegido de forma adequada;
- Deverá ser instalado um sistema de no-break, que alimente pelo menos os equipamentos e os locais considerados críticos;
- Devem ser criados mecanismos de proteção e combate a incêndio, principalmente em locais considerados críticos;
- Os equipamentos, principalmente os considerados críticos, devem estar instalados em áreas protegidas de acesso;

Segurança Lógica

a) Documentação dos procedimentos de operação:

- Todos os sistemas, que estiverem em desenvolvimento deverão estar com a documentação atualizada.

b) Ambiente Operacional:

- Todos os equipamentos de infraestrutura, interligações das redes, interligações de hardware de grande porte, software básicos, de apoio e plataformas móveis deverão manter uma documentação necessária e suficiente, que possibilite a qualquer técnico habilitado entendê-la, visando a manutenções preventivas, corretivas e evolutivas, no ambiente operacional.

c) Gerenciamento e controle de mudanças:

- Qualquer mudança no ambiente de desenvolvimento móvel, seja ela de infraestrutura, hardware, comunicações, softwares básicos, softwares de apoio ao desenvolvimento das aplicações móveis, plataformas móveis, procedimentos etc., deverá ser planejada e documentada com no mínimo as seguintes informações: a descrição da mudança, os

responsáveis por ela, a data e hora da execução, o tempo previsto, o impacto potencial e um plano de recuperação em caso de insucesso e aprovada pela Direção da empresa.

- Para mudanças em regime de emergência devido às atualizações da tecnologia móvel, os procedimentos continuarão a serem os mesmos, porém, poderão ser executadas, com a aprovação da Direção, e documentadas logo após a solução do problema.

d) Gerenciamento e controle de problemas:

- Quaisquer problemas que ocorram no ambiente operacional sejam eles de infraestrutura, hardware, equipamentos móveis e de comunicação de dados, software e sistemas aplicativos móveis, devem ser registrados com, no mínimo, as seguintes informações: a descrição do problema, a data e hora da ocorrência do mesmo, a identificação de quem o registrou e de quem foi acionado para solucioná-lo, as consequências do problema, a data e a hora da solução, identificação de quem o solucionou e a descrição da solução adotada.

e) Diretrizes quanto à utilização da *internet*

- Implantação de um sistema de rede estruturado em Cliente / Servidor, um sistema de *Proxy* fazendo todo o bloqueio e monitoramento dos acessos a *sites*.
- A *internet* deve ser utilizada para fins corporativos, o enriquecimento intelectual de seus colaboradores ou como ferramenta para busca de informações de novos conceitos devido a atualização rápida da tecnologia móvel onde venham contribuir para o desenvolvimento de seus trabalhos.
- Fica vedada a utilização de *e-mail* pessoal na empresa, podendo somente ser utilizado o *e-mail* corporativo.
- Quanto à utilização das redes sociais será permitido apenas para o setor responsável pelo *marketing,* somente para fins de divulgação da empresa, ficando proibido para uso pessoal.
- O uso do dispositivo móvel só é permitido para fins de teste e simulações das aplicações da empresa.

f) *E-mail* corporativo:

- Desconfiar de todos os *e-mails* com assuntos estranhos ao ambiente de trabalho.
- Não reenviar *e-mails* do tipo corrente, aviso de vírus, propagandas de empresas, entre outros.
- Não utilizar o *e-mail* corporativo para fins pessoais.

g) A realização de *download*:

- A realização de *downloads* deve ser vista com muito cuidado e feita somente em casos de extrema necessidade para uso da empresa.
- A realização de *download* exige banda de navegação do servidor e, se realizado em demasia, congestiona o tráfego e torna a navegação para os demais usuários mais demorada principalmente para as simulações e testes das aplicações. Além disso, deverá ser limitada para arquivos grandes, pois podem congestionar o fluxo e comprometer os sistemas que funcionam *on-line.*

h) Execução de jogos e rádios *on-line*

- É proibida a execução de jogos, músicas ou rádios *on-line*, visto que esta prática congestiona a banda de *internet*, dificultando a execução de serviços que necessitam deste recurso, já que as aplicações são simuladas com uso da *internet.*

i) Senhas de acesso

- Cada setor deverá, através de comunicado oficial, indicar novos colaboradores e o perfil que devem possuir na rede e nos sistemas da empresa.
- A senha de acesso é pessoal, intransferível, cabendo ao seu titular total responsabilidade quanto ao seu sigilo.
- O compartilhamento de senhas de acesso é proibido e o titular que divulgar sua senha a outrem responderá pelas infrações por esse cometidas, estando passível de advertência.
- Caso o usuário desconfie que sua senha não seja mais segura, poderá solicitar ao departamento de SM a alteração desta.
- A senha para uso dos aplicativos móveis da empresa deverá ser autorizada pelo departamento de SM.

j) Controle de *Instant Messenger:*

- É proibido aos setores o uso de *software* de mensagem instantânea nos equipamentos de dispositivos móveis, portáteis ou desktop, que não forem autorizados pela empresa, ou que o uso não seja para fins da empresa.

k) A instalação de *software:*

- Qualquer *software* que, por necessidade do serviço, necessitar ser instalado, deverá ser comunicado ao departamento de SM, que procederá a instalação caso constate a necessidade do mesmo tanto nos dispositivos móveis com em desktop.
- Fica proibida a instalação de qualquer *software* sem licença de uso.
- O departamento de SM poderá utilizar de sua autonomia para desinstalar, sem aviso prévio, todo e qualquer *software* sem licença de uso, em atendimento à lei do *software* (Lei 9.609/98).

l) Acesso ao telefone:

- A utilização dos telefones da empresa será restrita ao desempenho das atividades laborais dos funcionários.
- Não será permitido o uso dos dispositivos móveis para realização de ligações tanto pessoal como para fins da empresa.
- Os dispositivos móveis serão para uso de teste e simulações das aplicações da empresa.

m) Penalidades:

- O usuário que infringir qualquer uma das diretrizes de segurança expostas neste instrumento estará passível das seguintes penalidades (sem prévio aviso):
    - Perda da senha de acesso aos sistemas de *internet;*
    - Cancelamento do *e-mail* corporativo*;*
    - Advertência formal por intermédio do departamento de RH podendo levar inclusive a demissão do colaborador.

n) Equipe de segurança da informação:

Os colaboradores relacionados a seguir são diretamente responsáveis pela implantação da política:

- Gerente de Segurança da Informação,
- Responsável de cada setor.

o) Divulgação e treinamento:

- O documento de segurança deve ser divulgado por intermédio de treinamento aos

colaboradores, clientes e fornecedores, podendo ainda ser divulgada por *e-mail* corporativo, mural ou jornal interno.

p) Vigência e validade:

- O documento passa a vigorar a partir da data de sua homologação e publicação, sendo válida por tempo indeterminado podendo ser alterada conforme necessidades previamente detectadas.

6ª Etapa: Plano de continuidade de negócio

Com o objetivo de manter em funcionamento os serviços e processos críticos da empresa, na eventualidade da ocorrência de desastres, atentados e falhas, devem ser preparados planos de continuidade.

Para cada situação, deve existir um plano de continuidade, contendo no mínimo as seguintes informações:

- Análise Qualitativa e Quantitativa de Riscos**:** consiste em avaliar a probabilidade (Baixo, Médio, e Alto) e o impacto (insignificante, tolerável, sério e catastrófico) dos riscos, de modo a priorizar seus efeitos sobre os objetivos do projeto.

Segundo (Crouhy, *et. al* 2004 *apud* Fernandes, *et. al* 2011) é possível considerar a existência de duas abordagens de mensuração de riscos, a qualitativa e a quantitativa. Em ambas, a mensuração é definida a partir do conhecimento das variáveis frequência (ou probabilidade de ocorrência) e severidade (ou impacto financeiro), associadas aos eventos de perdas identificados nos processos das empresas. Pela abordagem qualitativa, o nível de risco é avaliado a partir da atribuição de critérios de classificação à frequência e à severidade, enquanto que pela abordagem quantitativa o risco é avaliado por modelos probabilísticos (Jorion, 2003).

- Data de elaboração do plano;
- Data de atualização do plano;
- Data do último teste do plano;
- Fator desencadeador de ação;
- Equipe que elaborou o plano, quais as pessoas que o executarão e seus substitutos imediatos e os procedimentos para execução dos mesmos.

No entanto, o plano de continuidade deve ser elaborado pelo SGSI. O Apêndice A apresenta o modelo proposto para elaboração do plano de continuidade do negócio da empresa.

Levando em consideração os riscos e problemas identificados em empresas de desenvolvimento de software para dispositivos móveis apresentados nas tabelas 3.1, 3.3 e 3.7, sugerem-se planos para, no mínimo, as seguintes situações de contingenciamento conforme a Tabela 4.2.

Tabela 4.2: Situações de contingenciamento

Planos	Contingenciamento	Justificativa
[P-1]	Perda ou roubo de dispositivos móveis ou portáteis da empresa	Armazenamento de informações, testes e simulações são realizados diariamente.
[P-2]	Perda de equipamentos de grande porte – servidores de redes e arquivos.	Grande armazenamento de informações importantes da empresa.
[P-3]	Parada de softwares, plataformas de desenvolvimento, aplicativos, simulação e testes das aplicações móveis.	Alta demanda de aplicações devido ao número elevado de dispositivos móveis no mercado.
[P-4]	Rotatividade da equipe de desenvolvimento	Falta de mão de obra qualificada
[P-5]	Perda total do prédio	Recursos e ativos da empresa estão armazenados em único lugar.

Todo pessoal envolvido com o Plano de Continuidade do Negócio deve receber um treinamento específico para poder enfrentar os incidentes abordados na Tabela 4.1.

Nos documentos analisados das empresas de desenvolvimento de software para dispositivos móveis pouco se aborda sobre o plano de continuidade do negócio, no qual reforça ainda mais a implantação da estratégia proposta.

Os planos destacados na tabela 4.1 contribuem para o gerenciamento dos riscos que podem ser enfrentados pelas empresas, no entanto, cada empresa do contexto móvel deve analisar cuidadosamente suas particularidades. No entanto, com base nas empresas analisadas pode-se observar a necessidade mínima de implantação dos planos citados.

4.4. Considerações finais

A estratégia de segurança da informação proposta constitui-se de seis etapas que se resumem em: Conhecimento da norma ISO 27001, definição do escopo do projeto, elaboração

do comitê do SGSI, gerenciamento de risco, desenvolvimento e treinamento do documento de segurança da informação e gestão de continuidade do negócio.

Cada uma dessas etapas propõe solução para problemas de segurança da informação enfrentados por empresas de desenvolvimento de software para aplicações móveis com aplicações de algumas práticas relacionadas aos requisitos físicos e lógicos podendo auxiliar essas empresas em seus projetos e atividades diárias, minimizando os impactos negativos dos riscos.

Capítulo

5

Avaliação da estratégia proposta

5.1. Considerações iniciais

A avaliação da estratégia de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis, conforme apresentado na metodologia de desenvolvimento (Capítulo 1), utilizou-se da Engenharia de Software Experimental com base no trabalho de Mafra e Travassos (2006).

Com a identificação e o controle parcial das variáveis da pesquisa e a interação do grupo de avaliadores com a estratégia proposta, o estudo caracteriza-se como *quasi* experimental *in virtuo*.

Esta avaliação tem por objetivo justificar as estratégias de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis. Não é do mérito deste estudo provar a eficácia prática da estratégia, mas sim, verificar se a estratégia amplia o conhecimento da modalidade de segurança da informação em empresas desenvolvimento de software para dispositivos móveis e é passível de ser aplicada e produzir resultados positivos.

5.2. Organização da avaliação da estratégia de SI em empresas de desenvolvimento de software para dispositivos móveis

A organização da avaliação baseou-se no trabalho de Mafra e Travassos (2006), o qual apresenta a formatação apresentada na Figura 5.1.

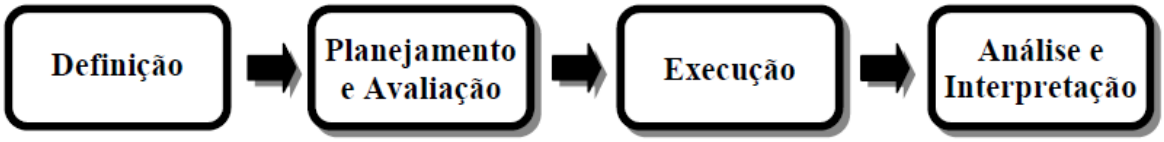

Figura 5.1: Etapas do processo da avaliação da estratégia proposta

Etapas da formatação da avaliação:

- Definição: trata do propósito do estudo experimental para avaliar a estratégia;
- Planejamento e avaliação: abordam a especificação e as técnicas aplicadas na avaliação;
- Execução: refere-se à condução do experimento;
- Análise e interpretação: envolvem à estatística descritiva e a interpretação dos dados para validar ou refutar as hipóteses definidas no planejamento.

5.3. Definição da avaliação

Analisar a estratégia de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis com o propósito de avaliar as bases e práticas definidas dentro das organizações que desenvolvem software para negócios móveis a partir do ponto de vista dos gestores da área de segurança da informação.

5.3.1. Objetivo geral da avaliação

Verificar a capacidade da estratégia de produzir efeitos positivos dentro das empresas que desenvolvem software para dispositivos móveis.

5.3.2. Objetivos específicos da avaliação

• Verificar se as regras, normas e procedimentos de segurança da informação tratadas na estratégia de SI em empresas de desenvolvimento de software para dispositivos móveis são consideradas críticas;

• Verificar se a estratégia de SI em empresas de desenvolvimento de software para dispositivos móveis é capaz de mitigar os riscos e desafios, apresentados no terceiro capítulo, relacionados à segurança da informação.

• Verificar o grau de aplicabilidade da estratégia sob o viés dos gestores de segurança da informação.

5.3.3. Questões da avaliação

• **Q1:** Os elementos apresentados são suficientes para elaborar uma estratégia de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis?
Métrica: As bases dos elementos da estratégia.

• **Q2:** A estratégia possui aplicabilidade nas atividades desenvolvidas pelas empresas de desenvolvimento de software para dispositivos móveis?
Métrica: As estratégias de riscos.

• **Q3:** A estratégia é capaz de produzir resultados eficientes em contextos de desenvolvimento de software para dispositivos móveis?
Métrica: A eficiência da estratégia.

5.4. Planejamento e avaliação

Esta etapa prepara a aplicação e condução do método da engenharia experimental por meio da seleção e justificativa do contexto e dos participantes, da definição das hipóteses e do projeto e instrumento do estudo.

5.4.1. Seleção do contexto e dos participantes

A estratégia de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis se propôs a resolver problemas reais produzidos pelos riscos e desafios existentes em contexto de desenvolvimento de software móvel. O contexto da avaliação é *off-line*, ou seja, não foi aplicado na indústria, e sim, sob á ótica de gestores de segurança da informação.

5.4.2. Hipóteses e variáveis

• **H0:** A estratégia de SI para empresa de desenvolvimento de software para dispositivos móveis é ineficiente para o contexto de desenvolvimento de software móvel.
Variáveis:

Tipo	Descrição	Escala
Independente	Eficiência da estratégia	Intervalar

• **H1:** Os elementos abordados na estratégia de SI para empresa de desenvolvimento de software para dispositivos móveis satisfazem com eficiência a segurança da informação de empresas do contexto móvel.

Variáveis:

Tipo	Descrição	Escala
Independente	Importância da estratégia	Intervalar
Dependente	Concordância com a estratégia	Intervalar

• **H2:** A estratégia de SI para empresa de desenvolvimento de software para dispositivos móveis minimiza os impactos negativos de riscos identificados.

Variáveis:

Tipo	Descrição	Escala
Independente	Importância da estratégia	Intervalar
Dependente	Concordância com a estratégia	Intervalar

5.4.3. Projeto do experimento e instrumentação

O experimento caracteriza-se como uma pesquisa de opinião e visa coletar dados a partir da análise de gestores da área de segurança da informação. Sendo assim, foram realizadas duas análises, uma de medida para identificar o perfil dos participantes e outra para apurar de forma descritiva a representatividade das medidas obtidas pela escala de *Likert*[2] para avaliar a estratégia.

Os resultados da escala de *Likert* serão sintetizados em valores representativos por meio do cálculo da moda, cujo resultado representa a opinião majoritária dos gestores. A Tabela 5.1 apresenta a escala de mensuração adotada para as variáveis dependentes e independentes.

[2] A escala *Likert* é um tipo de escala de resposta bipolar, medindo ou uma resposta positiva ou negativa a uma afirmação.

Tabela 5.1: Escala de mensuração das variáveis dependentes e independentes

Variável\Valor	[1]	[2]	[3]	[4]	[5]	[6]
Importância	Essenciais	Muito importante	Mais ou menos importante	Sem muita importância	Irrelevante	Sem resposta
Concordância	Concordo totalmente	Concordo parcialmente	Concordo/Discordo parcialmente	Discordo parcialmente	Discordo totalmente	Sem resposta

A Tabela 5.1 apresenta a escala das variáveis no qual varia de [1] a [5], a escala [6] foi incluída para eliminar as respostas não conformes (*outliers*[3]) geradas por dúvidas, desconhecimento ou interpretação que descarta o item a título de análise descritiva para obter o valor mais representativo, ou seja, a moda.

Como instrumento que prove meios para realizar a execução e análise do experimento selecionou-se o questionário de opinião. O Apêndice B ilustra este questionário cuja denominação é "Questionário de Avaliação de SI em Empresas de Desenvolvimento de Software para Dispositivos Móveis". O questionário cobriu 03 (três) grupos de informações, coletando dados sobre (a) o respondente, (b) as bases da estratégia proposta e (c) a estratégia proposta. O primeiro grupo (a) visa identificar o perfil dos respondentes, o grupo (b) avaliará os níveis de importância e concordância das bases utilizadas para elaboração da estratégia e, por conseguinte, o último grupo (c) avaliará a estratégia de segurança da informação para empresas de desenvolvimento de software para dispositivos móveis.

Para a validação buscou-se a técnica de validade conclusiva ou *constructo*. A partir da análise do perfil e conhecimento dos participantes sobre área de gestão de projetos de software (grupos (a) e (b) do questionário) será assumido como confiável ou não confiável os dados coletados. Esta técnica faz-se adequada para este estudo experimental, haja vista a restrição da aplicação prática em empresas.

5.5. Execução do experimento

Realizou-se uma apresentação a cada participante da avaliação abordando a fundamentação, as bases da estratégia e a estratégia de SI em empresas de desenvolvimento de software para dispositivos móveis. O "Questionário de Avaliação de SI em Empresas de Desenvolvimento de Software para Dispositivos Móveis." foi aplicado a 03 (três) participantes.

A duração média de resposta do questionário pelos respondentes foi de 02 horas. Após a devolução dos questionários os dados foram tabulados.

[3] *Outlier* é um resultado atípico que apresenta um grande afastamento dos demais valores. São ameaças em pesquisas e estudos experimentais.

5.5.1. Análise dos participantes

O questionário foi aplicado a três avaliadores, dos quais dois possuem conhecimento em desenvolvimento de software para aplicações móveis e um com experiência em desenvolvimento de software no contexto clássico. No entanto, dois deles com experiência em empresas de desenvolvimento de software para dispositivos móveis com certificação em SI. Os gestores estão na área de SI há mais de cinco anos.

5.6. Análise e interpretação do experimento

Esta etapa refere-se à estatística descritiva dos resultados tabulados dos grupos de informações sobre as bases da abordagem e a abordagem propriamente dita, bem como a verificação das hipóteses.

5.6.1. Análise das bases da estratégia

A mensuração das medidas de tendência central ressalta o comportamento da distribuição de valores em relação ao agrupamento em torno dos valores centrais. A moda é uma dessas medidas e representa o valor que ocorre com maior frequência em uma série de valores, ou seja, é calculada pela contagem do número de ocorrências de cada valor, selecionando o mais comum.

A escala de *Likert* possibilitou descrever as variáveis “importância” e “concordância” em uma escala intervalar de [1] à [5]. A partir da distribuição dessas variáveis é possível conhecer a tendência das respostas e a opinião majoritária dos respondentes, ou seja, a moda da distribuição estatística.

As Figuras de 5.1 a 5.9 que seguem este estudo mapeiam o domínio de frequência da variável independente e dependente sob cada análise estatística. Para exibir os resultados, a moda de cada variável é representada na forma de um gráfico de radar. O gráfico de radar foi selecionado por melhor apresentar o grau de importância e concordância das variáveis. Quanto mais **externo** os pontos maior o grau de importância e concordância, e quanto mais **interno** menor o grau de importância e concordância.

Para compreender a Figura 5.2 faz-se necessário a apresentação da Tabela 5.2, cujos elementos são associados a siglas.

Tabela 5.2: Tabela de siglas dos elementos

Elementos	**Sigla**
Conhecimento da norma ISO 27001	[E01]
Desenvolvimento do escopo do projeto	[E02]
Elaboração do SGSI	[E03]
Levantamento, análise e gerenciamento de risco.	[E04]
Desenvolvimento e treinamento dos requisitos de segurança da informação	[E05]
Gestão de continuidade do negócio	[E06]

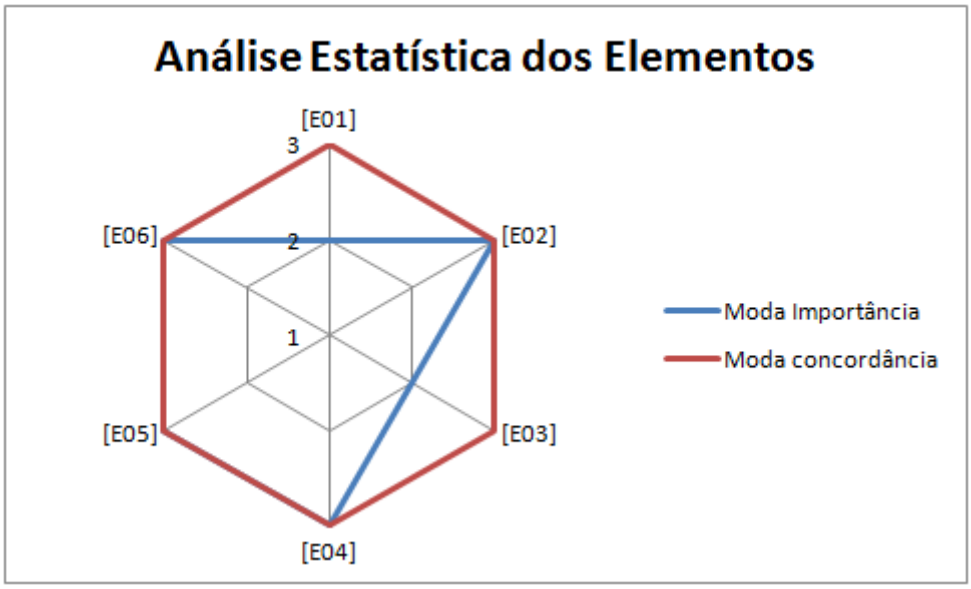

Figura 5.2: Análise dos elementos identificados para SI em empresas de desenvolvimento de software para dispositivos móveis

Pode-se observar na Figura 5.2 que os elementos [E01] "Conhecimento da norma ISO 27001" e [E03] "Elaboração do SGSI" são os únicos elementos cuja importância é razoável para SI em empresas de desenvolvimento de software para dispositivos móveis, mas que possui concordância total pelos gestores.

Similar à Tabela 5.2, a Tabela 5.3 apresenta as siglas associadas aos elementos do escopo.

Tabela 5.3: Tabela de siglas dos requisitos do escopo

Escopo	**Sigla**
Custo: Implantação da norma ISO 27001;	[S01]
Prazo para implantação da norma;	[S02]
Descrição de atribuição a clientes, colaboradores, fornecedores incluindo termos de responsabilidade e acordos confidencialidades;	[S03]
Elaboração da política de segurança da informação, caracterizada pelo conjunto de	[S04]

princípios e valores estruturais, nos quais a empresa explicita os seus propósitos, traduzidos em regras específicas para proteger as informações que são de sua propriedade ou que estão sob sua responsabilidade;	
Classificação de ativos de software utilizados como programas fontes, ferramentas de apoio ao desenvolvimento, softwares básicos e de apoio aos utilitários;	[S05]
Definição de equipamentos de Tecnologia da Informação que deverão dar suporte à Política que estão relacionados com os equipamentos computacionais (computadores de grande porte, microcomputadores, notebooks, etc.), equipamentos de comunicação (roteadores, modens, switchs, etc.), dispositivos de entrada e saída (discos, impressoras, etc.);	[S06]
Levantamento da estrutura de comunicação como ferramentas de conversação instantânea;	[S07]
Classificação das pessoas envolvidas na empresa como direção, gerentes, colaboradores dos setores da empresa;	[S08]
Definição de serviços realizados pela empresa que são as atividades desenvolvidas;	[S09]
Levantamento da infraestrutura de equipamentos como no-breaks, geradores de eletricidade alternativa, quadros elétricos, equipamentos de refrigeração, etc.	[S10]
Classificação dos ativos informação que são os dados contidos em SGBD – Sistemas Gerenciadores de Bancos de Dados, os dados contidos em arquivos convencionais, a documentação de sistema – análise, usuário e operação – a documentação de softwares básicos e de apoio e os planos de continuidade.	[S11]
Levantamento da infraestrutura do prédio como classificação de áreas críticas.	[S12]

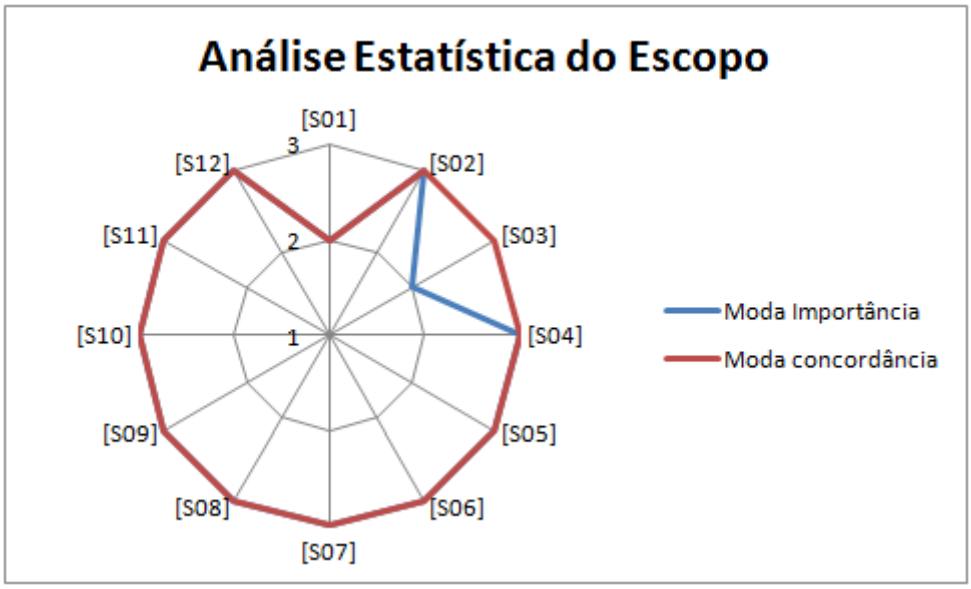

Figura 5.3: Análise dos elementos do escopo identificados para SI em empresas de desenvolvimento de software para dispositivos móveis

Na Figura 5.3 o elemento do escopo [S01], "Custo: Implantação da norma ISO 27001", não obteve concordância total dos gestores, no entanto, os gestores acreditam ser importante para o contexto SI em empresas de desenvolvimento de software para dispositivos móveis. O

elemento [S03], “Descrição de atribuição a clientes, colaboradores, fornecedores incluindo termos de responsabilidade e acordos confidencialidades”, todos concordam, porém, apresentam importância relevante.

A Tabela 5.4, apresenta as siglas associadas aos elementos identificados para o SGSI.

Tabela 5.4: Tabela de siglas dos requisitos do SGSI

SGSI	**Sigla**
Participantes dos SGSI: representante de cada setor. - Diretores, Recursos Humanos, Suporte e Manutenção.	[C01]
Responsabilidade: responsável por divulgar a política da informação da empresa e auditorias internas. - Observar fatores legais e contratuais envolvidos nos negócios da empresa - Desenvolver critérios para avaliação de riscos aos negócios.	[C02]

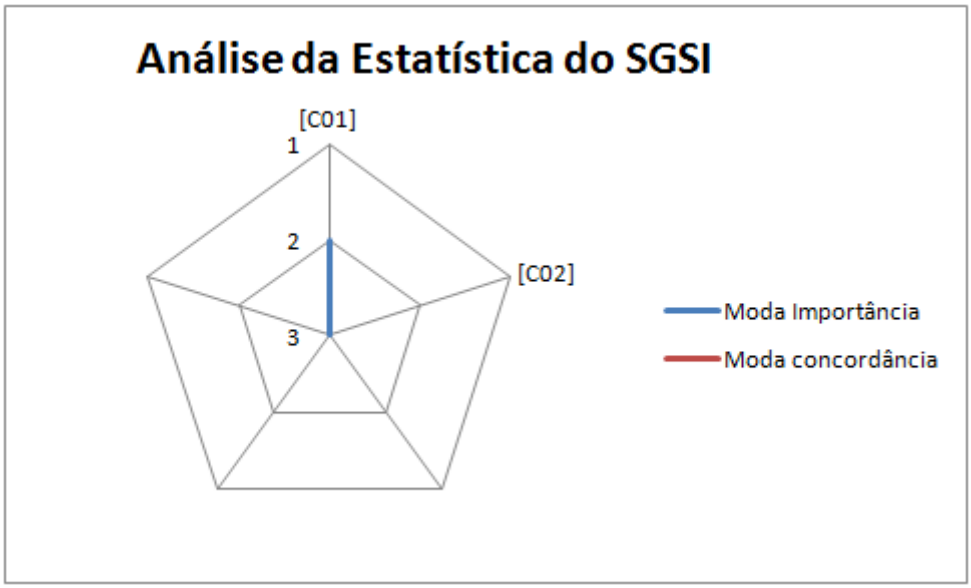

Figura 5.4: Análise dos elementos do SGSI identificados para SI em empresas de desenvolvimento de software para dispositivos móveis

Um fato interessante foi o resultado da Figura 5.4, no qual os dois elementos do SGSI [C01] e [C02], tiveram concordância e importância total na opinião dos entrevistados.

Para dar continuidade na análise dos requistos físicos abordados na estratégia, a Tabela 5.5 apresenta as siglas associadas aos requisitos.

Tabela 5.5: Tabela de siglas dos requisitos físicos

Requisitos físicos	**Sigla**
Áreas de segurança	[F01]
Controle de entrada e saída de pessoas	[F02]
Autonomia do departamento de SM	[F03]
Proteção do prédio	[F04]

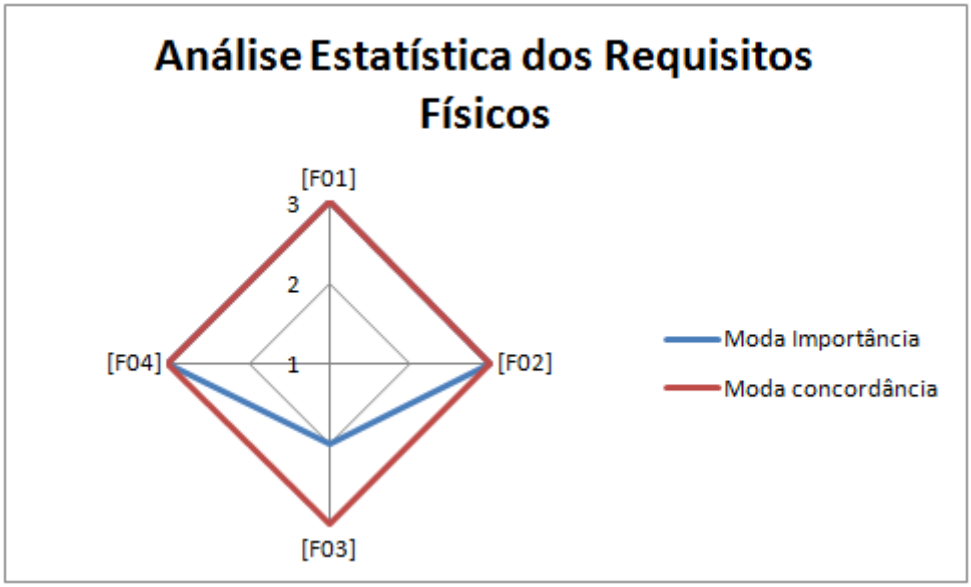

Figura 5.5: Análise dos requistos físicos identificados para SI em empresas de desenvolvimento de software para dispositivos móveis

Na Figura 5.5 os elementos [F01], "Áreas de segurança", [F02], "Controle de entrada e saída de pessoas", [F03] , "Autonomia do departamento de SM" e [F04], "Proteção do prédio", apresentaram concordância total no resultado da análise. Entretanto, ao avaliar a importância da "Autonomia do departamento de SM" da estratégia esta não foi unânime quanto ao nível de importância essencial.

A tabela de siglas associados aos requistos lógicos é apresentado na Tabela 5.6, assim podendo analisar a próxima figura.

Tabela 5.6: Tabela de siglas dos requisitos lógicos

Requisitos lógicos	**Sigla**
Documentação dos procedimentos de operação	[L01]
Ambiente operacional	[L02]
Gerenciamento e controle de mudança	[L03]

Gerenciamento e controle de problemas	[L04]
Diretrizes quanto à utilização da internet	[L05]
E-mail corporativo	[L06]
Realização de download	[L07]
Execução de jogos e rádios online	[L08]
Senhas de acesso	[L09]
Controle de instant messenger	[L10]
Instalação de software	[L11]
Acesso ao telefone	[L12]
Penalidades	[L13]
Equipe de segurança	[L14]
Divulgação e treinamento	[L15]
Vigência e validade	[L16]

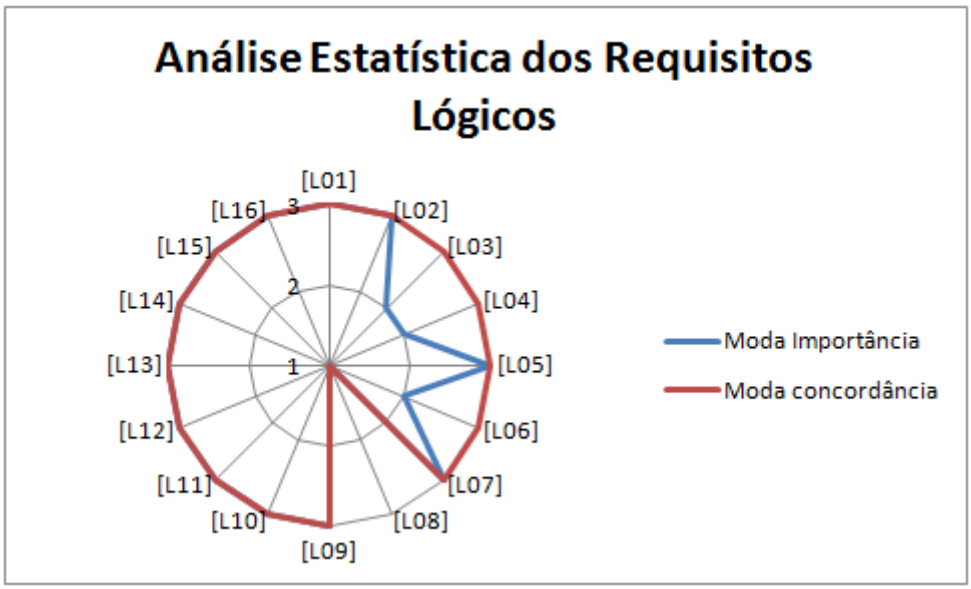

Figura 5.6: Análise dos requistos lógicos identificados para SI em empresas de desenvolvimento de software para dispositivos móveis

Percebe-se na Figura 5.6 que somente o requisito [L08] "Execução de jogos e rádios online" é o único risco cuja concordância total ou relevância para a SI na empresa de desenvolvimento de software para dispositivos móveis não é aceita pela maioria dos gestores, mas mesmo assim é considerado relevante. Nesta análise, destaca-se os requisitos lógicos

[L03] “Gerenciamento e controle de mudança”, [L04] “Gerenciamento e controle de problemas e [L06] “E-mail corporativo”, cujo grau de importância é razoável para a segurança da informação de empresa no contexto móvel.

As siglas para os planos de continuidade são apresentadas na Tabela 5.7.

Tabela 5.7: Tabela de siglas dos planos de continuidade

Plano de continuidade	**Sigla**
Perda ou roubo de dispositivos móveis ou portáteis da empresa	[P01]
Perda de equipamentos de grande porte – servidores de redes e arquivos.	[P02]
Parada de softwares, plataformas de desenvolvimento, aplicativos, simulação e testes das aplicações móveis.	[P03]
Rotatividade da equipe de desenvolvimento	[P04]
Perda total do prédio	[P05]

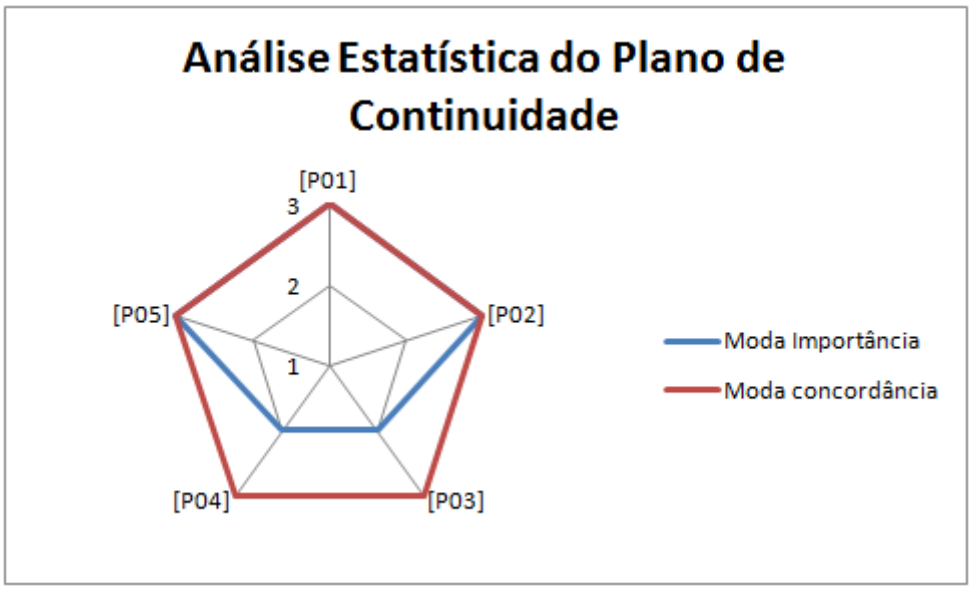

Figura 5.7: Análise dos planos de continuidade identificados para SI em empresas de desenvolvimento de software para dispositivos móveis

Na Figura 5.7 pode-se observar a concordância unânime dos planos de continuidade de negócio para os planos [P01] “Perda ou roubo de dispositivos móveis ou portáteis da empresa”, [P02] “Perda de equipamentos de grande porte – servidores de redes e arquivos”, [P03] “Parada de softwares, plataformas de desenvolvimento, aplicativos, simulação e testes das aplicações móveis”, [P04] “Rotatividade da equipe de desenvolvimento” e [P05] “Perda total do prédio”. Entretanto, para os planos [P03] e [P04] houve importância relevante.

5.6.1.1. Resultado das bases da estratégia

A partir da análise dos gráficos resultantes da análise das bases da estratégia de SI em empresas de desenvolvimento de software para dispositivos móveis pode-se concluir que um dos objetivos do estudo foi alcançado e a primeira questão (**Q1**) "Os elementos apresentados são suficientes para elaborar uma estratégia de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis?" possui resposta afirmativa.

Essa conclusão baseia-se nas premissas de importância e concordância dos gestores quanto às bases da estratégia.

5.6.2. Análise da estratégia

A mesma escala e medida utilizada na análise das bases da estratégia também foram aplicadas para analisar a estratégia proposta.

Uma análise geral sobre os quesitos de aplicabilidade de eficiência da estratégia também foi realizada. Em suma, os resultados foram satisfatórios e atenderam os objetivos do estudo. As Figuras 5.8 e 5.9 ilustram, respectivamente, o percentual de aceitação dos participantes da pesquisa quanto à aplicação da estratégia e sua eficiência se adotada pelas organizações.

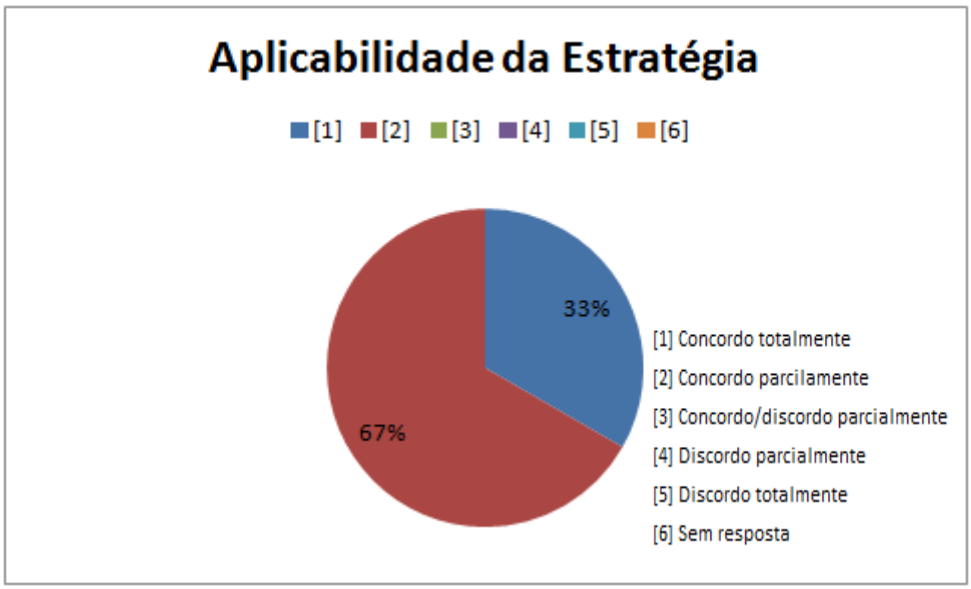

Figura 5.8: Análise quanto à aplicabilidade da estratégia de SI para empresas de desenvolvimento de software para dispositivos móveis

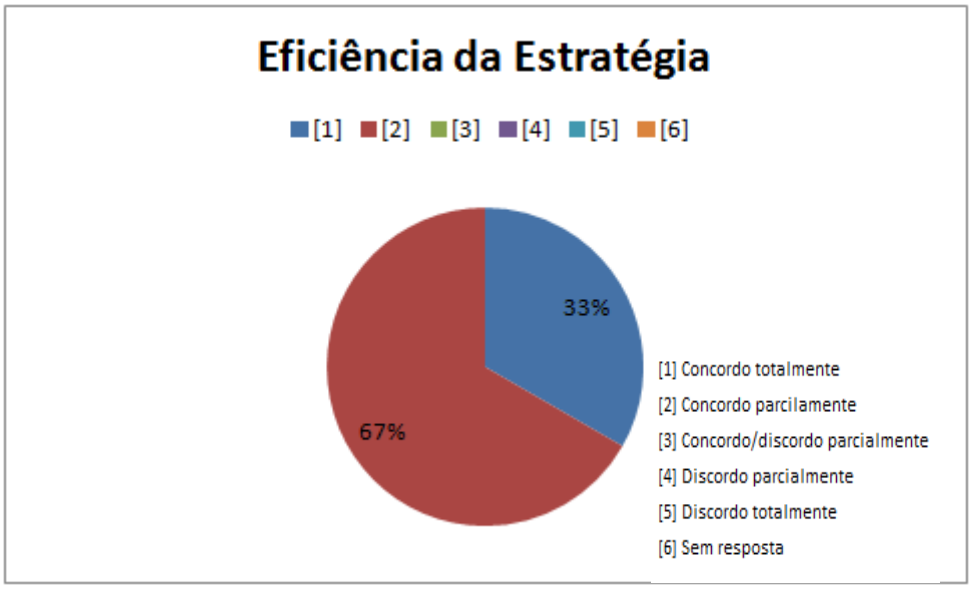

Figura 5.9: Análise quanto da eficiência da estratégia de SI para empresas de desenvolvimento de software para dispositivos móveis

Conforme observado nas figuras 5.8 e 5.9 tanto a aplicabilidade como a eficiência da estratégia foram satisfatórias no ponto de vista dos gestores de segurança da informação, apresentando um total de 67% de aceitação do nível de concordância dos requisitos abordados na estratégia.

5.6.2.1. Resultado da avaliação da estratégia

A partir da análise dos gráficos resultantes da análise da estratégia de SI em empresas de desenvolvimento de software para dispositivos móveis pode-se concluir que os objetivos do estudo foram alcançados e as questões (**Q2**) "A estratégia possui aplicabilidade nas atividades desenvolvidas pelas empresas de desenvolvimento de software para dispositivos móveis?" e (**Q3**) "A estratégia de SI é capaz de produzir resultados eficientes em contextos de desenvolvimento de software para dispositivos móveis?" possuem respostas afirmativas.

Essa conclusão baseia-se nas premissas no percentual de satisfação dos pesquisadores quanto à aplicabilidade e eficiência da estratégia nas empresas de desenvolvimento de software móvel.

5.6.3. Verificação das hipóteses

Com os resultados das Figuras 5.8 e 5.9 pode-se refutar a hipótese nula (**H_0**), ou seja, prova-se pelo percentual de concordância e eficiência que "A estratégia de SI para empresa de

desenvolvimento de software para dispositivos móveis é ineficiente para o contexto de desenvolvimento de software móvel". A partir da Figura 6.11 concluí-se também que as hipóteses alternativas (**H_1**) "Os elementos abordados na estratégia de SI para empresa de desenvolvimento de software para dispositivos móveis satisfaz com eficiência a segurança da informação de empresas do contexto móvel.", (**H_2**) "A estratégia de SI para empresa de desenvolvimento de software para dispositivos móveis minimiza os impactos negativos de riscos identificados", são afirmativas e expressam a opinião do grupo de gestores.

5.7. Considerações finais

Este capítulo buscou avaliar a estratégia de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis por meio da medida de tendência central denominada moda estatística. As conclusões sobre a avaliação e a estratégia são tratadas no próximo capítulo.

Capítulo

6

Conclusão

A segurança da informação caracteriza-se pela proteção de dados e informações da empresa. À medida que novas tecnologias surgem, novos riscos e desafios também surgem. No entanto, uma estratégia deve estar fundamentada em conceitos científicos acerca de componentes que envolvam o arcabouço dessa estratégia. Os temas sobre tecnologias móveis, dispositivos móveis, aplicações móveis, desafios no desenvolvimento de aplicações móveis, segurança da informação e desafios da segurança da informação foram descritos como componentes que proporcionaram o desenvolvimento da estratégia de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis.

A estratégia proposta apresenta diretrizes específicas para o gerenciamento e controle da segurança da informação em empresas de desenvolvimento de software para aplicações móveis, minimizando os impactos negativos dos riscos, uma vez que essas empresas apresentam características específicas em suas aplicações estas precisam ser gerenciadas de forma que suas particularidades sejam protegidas. Assim, esta estratégia preocupa-se com a segurança dessas particularidades ressaltando requisitos que satisfaçam a necessidade dessas empresas.

Esta premissa é confirmada pelo estudo experimental cujo propósito foi avaliar a aplicabilidade e eficiência da estratégia em empresas de desenvolvimento de software para dispositivos móveis. Pode-se observar nos resultados que a estratégia possui significância para os gestores de segurança da informação.

6.1. Dificuldades e limitações

Dentre as dificuldades e limitações encontradas durante a pesquisa e o desenvolvimento da estratégia estão:

• Dificuldade de acesso às empresas no âmbito regional que desenvolvem software para dispositivos móveis.

• A falta de colaboração dos gestores de segurança da informação para a coleta dos dados.

• A falta de colaboração dos gestores de segurança da informação para a avaliação da estratégia de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis.

6.2. Contribuições

Este trabalho contribui com uma linha de pesquisa pouco explorada, além de propor uma solução particular à gestão da segurança da informação em empresas de desenvolvimento de software para dispositivos móveis. Também, disponibiliza um material acessível para subsidiar a empresa e gerentes na segurança de dados e informações nas atividades desenvolvidas na empresa. Desta forma as contribuições da pesquisa são:

• A definição de uma estratégia segurança da informação em empresas de desenvolvimento de software para dispositivos móveis; e

• A indicação de técnicas específicas de segurança da informação para empresas de desenvolvimento de software para dispositivos móveis.

6.3. Sobre a avaliação da estratégia proposta

O teste de engenharia experimental envolveu aspectos teóricos e da experiência profissional individual de cada participante da avaliação, possibilitando ratificar a importância dos elementos de segurança específicos para empresas de desenvolvimento de software do contexto móvel e identificar um nível aceitável quanto à aplicabilidade e eficiência da estratégia.

6.4. Trabalhos futuros

Nesta seção, apresentam-se algumas indicações sobre trabalhos que poderão ser desenvolvidos a partir desta estratégia. São eles:

- Aplicação desta estratégia em organizações que atuam com desenvolvimento de software no contexto móvel e efetuar um estudo de caso no impacto por ele causado, com as dificuldades, bem como, as possíveis vantagens e benefícios alcançados pela sua utilização;
- Elaborar uma ferramenta de apoio automatizada da estratégia proposta para organizar as informações geradas.

Referências

ABNT ISO 17799. Associação Brasileira de Normas Técnicas (ABNT). Norma ABNT NBR ISO/IEC 17799:2005 – Código de Prática para Gestão da Segurança da Informação, 2005.

ABNT ISO 27001. Associação Brasileira de Normas Técnicas (ABNT). Norma ABNT NBR ISO/IEC 27001:2006 – Código de Prática para Gestão da Segurança da Informação, 2006.

ALI-HASSAN, H.; NEVO, D.; NEVO, S. *Mobile Collaboration: Exploring the Role of Social Capital*. ACM SIGMIS Database table of contents archive. ACM, New York, NY, v. 41, 2 ed., p. 9-24, may. 2010.

ANDRADE, S. C. Uma abordagem de Gerenciamento de Projetos de Software para Dispositivos Móveis. 2012. Dissertação (Mestrado em Ciência da Computação) – Departamento de Informática. Universidade Estadual de Maringá, Maringá. 2012.

ATAÍDES, A. C. Um Método para Acompanhamento e Controle da Implantação do CMMI**.** Dissertação de mestrado em Engenharia Elétrica. UnB – Universidade de Brasília, 2006.

BECKERS, K.; SCHMIDT, H.; KÜSTER, J. C. & FAßBENDER. **S.** Pattern-Based Support for Context Establishment and Asset Identification of the ISO 27000 in the Field of Cloud Computing. Sixth International Conference on Availability, Reliability and Security, 2011, p.327-333.

BLUE PHOENIX. "Boas práticas de segurança". Disponível em: www.bluephoenix.pt. Acessado em: 15/10/2011.

BOULHOSA.R.; Arquitetura de Pré-Autenticação Segura com Suporte a QoE para Aplicações Móveis Multimídia em Redes WiMAX. Disponível em: http://www.lrc.ic.unicamp.br/wra/2011/dmdocuments/85487_1.pdf. Acesado em: 10/11/2011.

CAMPOS, A. Sistema de segurança da informação: controlando os riscos. Florianopolis: Visual Books, 2ª ed, 2007.

CARVALHO, N. L. J. O problema da proteção e controle de acesso à informação – Proteção digital e vigilância do ambiente operacional de um módulo criptográfico. Rio de Janeiro: Universidade ferderal do Rio de Janeiro – UFRJ, Tese de Doutorado, Programa de Pós Graduação em Engenharia Civil, 2007.

CERT. br. Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil. Estatísticas do CERT. BR. Disponível em: HTTP://www.cert.br/incidentes/ Acesso em: 10 de março de 2013.

COUNTS, S.; HOFTE, H.; SMITH, I. Mobile Social Software: Realizing Potential, Managing Risks. In: CHI 2006 – Workshop. Montréal, Québec, Canada. pp.1703 - 1706

CUKIERMAN, H. L.; TEXEIRA, C.; PRIKLADINICKI, R. Um Olhar Sociotécnico sobre a Engenharia de Software. In: Revista de Informática Teórica e Aplicada - RITA. n 2, 2007.

Disponível em <http://www.seer.ufrgs.br/index.php/rita/article/view/rita_v14_n2_p199-219/3547>. Acesso em: 03 ago. 2010.

DIAS, K. L; SADOK, D. F.H. Internet Móvel: Tecnologias, Aplicações e QoS. XIX Simpósio Brasileiro de Redes de Computadores, 2001.

ENAMI, L. N. M. Um Modelo de Gerenciamento de Projeto para um Ambiente de Desenvolvimento Distribuído de Software. 2006. 217 f. Dissertação (Mestrado em Ciência da Computação). Universidade Estadual de Maringá, Maringá, 2006.

ENAMI, L.; TAIT, T. F. C.; HUZITA, E. H. M. *A Project Management Model to a Distributed Software Engineering Environment*. In: ICEIS 2006 - International Conference on Enterprise Information Systems, 2006, Papus. Anais do ICEIS'06, 2006.

FERNANDES, A. A.; ABREU, V. F. *Implantando a Governança de TI: da estratégia à gestão dos processos e serviços*. 2ª ed. Rio de Janeiro: Brasport, 2008. 444 p.

FONTES, E. L. G. Política de Segurança da Informação: uma contribuição para o estabelecimento de um padrão mínimo. Dissertação (mestrado). Faculdade de Tecnologia - FATEC. Centro Estadual de Educação Paula Souza, 2011.

FOUSKAS, K. G.; GIAGLIS, G. M.; KOUROUTHANASSIS, P. E.; KARNOUKOS, S.; PITSILLIDES, A.; STYLIANOU, M. A roadmap for research in mobile business. In: International Journal of Mobile Communications (IJMC), v.3, n.4. 2005.

GIBB, F.; BUCHANAN, S. A framework for business continuity management. International Journal of Information Management, Vol 26, Abril 2006, Pag 128-141

HELDMAN, K. Gerência de projetos: guia para o exame oficial do PMI. Tradução de Luciana do Amaral Teixeira. Rio de Janeiro: Elsevier, 2006 - 5ª Reimpressão.

HUZITA, E. H. M.; TAIT, T. F. C. Gerência de Projetos de Software. Escola Regional de Informática. Bandeirantes - Paraná, 2006.

KITCHENHAM, Barbara. Procedures for Performing Systematic Reviews. Keele, 2004.

ISSAC, H. e LECLERCQ, A. Give me a mobile phone, and I will work harder! - Assessing the value of mobile technologies in organizations : an exploratory research. Proceedings of the International Conference on Mobile Business (ICMB'06). 2006.

JOSANG, A. e SANDERUD, G. Security in mobile communications: challenges and opportunities. Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003 - Volume 21. Adelaide, Australia: Australian Computer Society, Inc.2003.

JORIOM, P. Value at Risk - A Nova Fonte de Referência para o Controle de Risco de mercado. 2º edição. Editora BM&F, 2003.

KROTOV, V. e JUNGLAS, I. Mobile Technology as an Enabler of Organizational Agility. Mobile Business, 2006. ICMB '06. International Conference on, 2006.

LEE, T. e JUN, J. Contextual perceived usefulness? Toward an understanding of mobile commerce acceptance. Mobile Business, 2005. ICMB 2005. International Conference on, 2005.

LUGANO, G. Digital Community Design: Exploring the Role of Mobile Social Software in the Processo f Digital Convergence. 2010. Tese (Doutorado) – University of Jyvaskyla, Jyvaskyla, 2010. Disponível em <http://digitalcommunity.cosix.it/>. Acesso em: 08 nov. 2011.

LUND, M. S.; SOLHAUG, B. & STØLEN, K. Evolution in relation to risk and trust management. IEEE Computer Society, 2010, p. 49-55.

MACHADO, C. B.; FREITAS, H. *Planejamento de Iniciativas de Adoção de Tecnologias Móvies*. Revista GEPROS, ano 4, n. 1, p. 101-115, jan/mar., 2008. Disponível em <http://www.ea.ufrgs.br/professores/hfreitas/files/artigos/2009/2009_gepros_cbm_hf_planejam_tecn_moveis.pdf >. Acesso em: 30 abr. 2011.

MACHADO, C., Modelo para Planejamento de Iniciativas de Adoção de tecnologias móveis na Interação entre Organização e Indivíduo. 2007. Dissertação de Mestrado em Administração. Universidade Federal do Rio Grande do Sul, 2007.

MAFRA, S. N.; TRAVASSOS, G. H. *Estudos Primários e Secundários apoiando a busca por Evidência na Engenharia de Software*. Rio de Janeiro: Programa de Engenharia de Sistemas e Computação. Mar. 2006. RT-ES 687/06.
METHA, Nivav. Mobile Web Development. Birmingham: Packt, 2008.

MODULO Security Soluction. 2011. Disponível em: http://modulo.com.br. Acesso em: 10 de setembro de 2012.

MOHELSKA, H.; Mobile Technologies and Their Use in a Company. In: World Multiconference on APPLIED ECONOMICS, BUSINESS AND DEVELOPMENT (AEBD '10), 2nd, 2010, Kantaoui, Sousse, Tunisia. APPLIED ECONOMICS, BUSINESS and DEVELOPMENT. WSEAS Press, may. 253 p., 141-146.

NAKAMURA, E.T.; GEUS, P. L. Segurança de Redes: Em ambientes Cooporativos. São Paulo: Novatec, 2007.

PMI.a Project Management Institute. Um Guia do Conhecimento em Gerenciamento de Projetos – Guia Pmbok. 4ª Edição, Newton Square, Pennsylvania, Editora Project Management Inst-id, 2008.

POTTER, B. Wireless security policies. Network Security, v. 2003, n. 10, p. 10–12, 2003.

SANTAELLA, L. Linguagens Líquidas na era da mobilidade. São Paulo: Editora Paulus, 2007 - Comunicação.

SANTANDER. “Principais itens em segurança da informação”. Disponível em: http://www.santander.com.br/document/gsb/seguranca_parceiros_principais_itens.pdf. Acessado em: 25/09/2011.

SANTOS, A. S. A methodology to implement an information security management system. Journal of Information Systems and Technology Management, Vol. 2, No. 2, 2005, pp. 121-136.

SEMOLA, M. Gestão da Segurança da Informação. São Paulo. Editora Campus, 2003.

SOUZA, R. M. Implantação de Ferramentas e Técnicas de Segurança da Informação em Conformidade com as Normas ISO 27001 e ISO 17799. 2007. Dissertação (Mestrado) – Pontifica Universidade Católica de Campinas.

SIMA. A.F.; Autenticação forte: aplicações e desafios para a computação móvel. Conferência IADIS Ibero-Americana. Disponível em: http://www.iadis.net/dl/final_uploads/200607P080.pdf. Acessado em: 15/11/2011.

TEIXEIRA, C. A. N.; CUKIERMAN, H. L. Por que Falham os Projetos de Implantação de Processos de Software?. In: III WORKSHOP Um Olhar Sociotécnico sobre a Engenharia de Software - WOSES, 2007, Porto de Galinhas. Pernambuco, 2007.

TRAVASSOS, G. H. *Introdução à engenharia de software experimental*. Relatório Técnico ES-590/02, Programa de Engenharia de Sistemas e Computação, COPPE/UFRJ, 2002.

TSOUMAS, V.; TRYFONAS, T. From risk analysis effective security management: towards an automated approach. In: International Journal of Information Management & Computer Security. Vol 12, fevereiro, 2004, Pag 91-101.

Thomas R. P. Information Security Risk Analysis**.** Editora**:** Auerbach Publications, 2001.

TURBAN, E. Administração de Tecnologia da Informação: teoria e prática. Rio de Janeiro. Editora Elsevier, 2005.

UNHELKAR, B. Mobile Enterprise Transition and Management. Auerbach Publications Boston, MA, USA. 2009. (Advanced and emerging communications technologies series).

RODRIGUES, E. A importância da segurança da informação em projetos. Techoje – uma revista de opinião, Belo Horizonte, abr. 2009.

VOS e KLEIN. *The Essential Guide to Mobile Business*. Prentice Hall: 2002.

WANGHAM M. S.; Mecanismos de Segurança para Plataformas de Agentes Móveis, baseados em Redes de Confiança SPKI/SDSI. XXI Simpósio Brasileiro de Redes de Computadores, v.3, n.5. 2007.

Apêndice A

Código: **Status:**									
Responsável:								**Data: _____/_____/_____**	
Descrição do Risco:									
Análise do Risco									
Impacto		**Baixo**		**Médio**		**Alto**			
Probabilidade		**Insignificante**		**Tolerável**		**Sério**		**Catastrófico**	
Consequência:									
Fator desencadeador de ação:									
Plano de Ação									
Objetivo do plano		**Evitar**		**Minimizar**		**Transferir**		**Contingência**	
Detalhamento do Plano:									

Apêndice B

Questionário de Avaliação da Estratégia de SI em empresas de desenvolvimento de software para dispositivos móveis

Hora Início:_____ Hora Término:_____

Sobre o respondente

1 – Formação

Informe o curso referente ao maior grau de escolaridade (ex: Ciência da Computação, Administração com ênfase em TI)
[_____]

2 – Possui experiência em desenvolvimento de software?

○ Sim ○ Não

Tempo [_____] [ ] meses [ ] anos

3 - Possui experiência em desenvolvimento de software para dispositivos móveis?

○ Sim ○ Não

Tempo [_____] [ ] meses [ ] anos

4 – Possui experiência em gestão de segurança da informação há quanto tempo?

Tempo [_____] [ ] meses [ ] anos

5 – Já implantou políticas de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis?

○ Sim ○ Não

6 – Possui certificação em segurança da informação?

○ Sim ○ Não

Qual?

Sobre as bases da estratégia proposta

Legenda para as questões de 7 a 14						
Variável\Valor	**[1]**	**[2]**	**[3]**	**[4]**	**[5]**	**[6]**
Importância	Essenciais	Muito	Mais ou menos	Sem muita	Irrelevante	Sem

		importante	importante	importância		resposta
Concordância	Concordo totalmente	Concordo parcialmente	Concordo/Discordo parcialmente	Discordo parcialmente	Discordo totalmente	Sem resposta

7 – Avalie a "importância" e "concordância" dos elementos de segurança abordados e classificados na estratégia de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis.
Para cada elemento listado marque o grau de importância e concordância.

Importância						**Elementos**	**Concordância**					
SR	[5]	[4]	[3]	[2]	[1]		[1]	[2]	[3]	[4]	[5]	SR
○	○	○	○	○	○	Conhecimento da norma ISO 27001	○	○	○	○	○	○
○	○	○	○	○	○	Desenvolvimento do escopo do projeto	○	○	○	○	○	○
○	○	○	○	○	○	Elaboração do SGSI	○	○	○	○	○	○
○	○	○	○	○	○	Levantamento, análise e gerenciamento de risco.	○	○	○	○	○	○
○	○	○	○	○	○	Desenvolvimento e treinamento dos requisitos de segurança da informação	○	○	○	○	○	○
○	○	○	○	○	○	Plano de continuidade do negócio	○	○	○	○	○	○

8 – Avalie a "importância" e "concordância" dos requisitos classificados no escopo do documento de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis.
Para cada requisito listado marque o grau de importância e concordância.

Importância						**Escopo**	**Concordância**					
SR	[5]	[4]	[3]	[2]	[1]		[1]	[2]	[3]	[4]	[5]	SR
○	○	○	○	○	○	Custo: Implantação da norma ISO 27001;	○	○	○	○	○	○
○	○	○	○	○	○	Prazo para implantação da norma;	○	○	○	○	○	○
○	○	○	○	○	○	Descrição de atribuição a clientes, colaboradores, fornecedores incluindo termos de responsabilidade e acordos confidencialidades;	○	○	○	○	○	○
○	○	○	○	○	○	Elaboração da política de segurança da informação, caracterizada pelo conjunto de princípios e valores estruturais, nos quais a empresa explicita os	○	○	○	○	○	○

						seus propósitos, traduzidos em regras específicas para proteger as informações que são de sua propriedade ou que estão sob sua responsabilidade;						
○	○	○	○	○	○	Classificação de ativos de software utilizados como programas fontes, ferramentas de apoio ao desenvolvimento, softwares básicos e de apoio aos utilitários;	○	○	○	○	○	○
○	○	○	○	○	○	Definição de equipamentos de Tecnologia da Informação que deverão dar suporte à Política que estão relacionados com os equipamentos computacionais (computadores de grande porte, microcomputadores, notebooks, etc.), equipamentos de comunicação (roteadores, modens, switchs, etc.), dispositivos de entrada e saída (discos, impressoras, etc.);	○	○	○	○	○	○
○	○	○	○	○	○	Levantamento da estrutura de comunicação como ferramentas de conversação instantânea;	○	○	○	○	○	○
○	○	○	○	○	○	Classificação das pessoas envolvidas na empresa como direção, gerentes, colaboradores dos setores da empresa;	○	○	○	○	○	○
○	○	○	○	○	○	Definição de serviços realizados pela empresa que são as atividades desenvolvidas;	○	○	○	○	○	○
○	○	○	○	○	○	Levantamento da infraestrutura de equipamentos como no-breaks, geradores de eletricidade alternativa, quadros elétricos, equipamentos de refrigeração, etc.	○	○	○	○	○	○
○	○	○	○	○	○	Classificação dos ativos informação que são os dados contidos em SGBD – Sistemas Gerenciadores de Bancos de Dados, os dados contidos em arquivos convencionais, a documentação de sistema – análise, usuário e operação – a documentação de softwares básicos e de apoio e os planos de continuidade.	○	○	○	○	○	○

○	○	○	○	○	○	Levantamento da infraestrutura do prédio como classificação de áreas críticas.	○	○	○	○	○	○

9 – Avalie a "importância" e "concordância" da equipe do SGSI (membros e função) classificados no documento de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis.
Para cada elemento listado marque o grau de importância e concordância.

Importância						**SGSI**	**Concordância**					
SR	[5]	[4]	[3]	[2]	[1]		[1]	[2]	[3]	[4]	[5]	SR
○	○	○	○	○	○	Participantes dos SGSI: representante de cada setor. - Diretores, Recursos Humanos, Suporte e Manutenção.	○	○	○	○	○	○
○	○	○	○	○	○	Responsabilidade: responsável por divulgar a política da informação da empresa e auditorias internas. - Observar fatores legais e contratuais envolvidos nos negócios da empresa - Desenvolver critérios para avaliação de riscos aos negócios.	○	○	○	○	○	○

10 – Avalie a "importância" e "concordância" dos requisitos físicos classificados no documento de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis.
Para cada elemento listado marque o grau de importância e concordância.

Importância						**Requisitos Físicos**	**Concordância**					
SR	[5]	[4]	[3]	[2]	[1]		[1]	[2]	[3]	[4]	[5]	SR
○	○	○	○	○	○	Áreas de segurança	○	○	○	○	○	○
○	○	○	○	○	○	Controle de entrada e saída de pessoas	○	○	○	○	○	○
○	○	○	○	○	○	Autonomia do departamento de SM	○	○	○	○	○	○
○	○	○	○	○	○	Proteção do prédio	○	○	○	○	○	○

11 – Avalie a "importância" e "concordância" dos requisitos lógicos classificados no documento de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis.
Para cada elemento listado marque o grau de importância e concordância.

Importância						Requisitos Lógicos	Concordância					
SR	[5]	[4]	[3]	[2]	[1]		[1]	[2]	[3]	[4]	[5]	SR
○	○	○	○	○	○	Documentação dos procedimentos de operação	○	○	○	○	○	○
○	○	○	○	○	○	Ambiente operacional	○	○	○	○	○	○
○	○	○	○	○	○	Gerenciamento e controle de mudança	○	○	○	○	○	○
○	○	○	○	○	○	Gerenciamento e controle de problemas	○	○	○	○	○	○
○	○	○	○	○	○	Diretrizes quanto à utilização da internet	○	○	○	○	○	○
○	○	○	○	○	○	E-mail corporativo	○	○	○	○	○	○
○	○	○	○	○	○	Realização de download	○	○	○	○	○	○
○	○	○	○	○	○	Execução de jogos e rádios online	○	○	○	○	○	○
○	○	○	○	○	○	Senhas de acesso	○	○	○	○	○	○
○	○	○	○	○	○	Controle de instant messenger	○	○	○	○	○	○
○	○	○	○	○	○	Instalação de software	○	○	○	○	○	○
○	○	○	○	○	○	Acesso ao telefone	○	○	○	○	○	○
○	○	○	○	○	○	Penalidades	○	○	○	○	○	○
○	○	○	○	○	○	Equipe de segurança	○	○	○	○	○	○
○	○	○	○	○	○	Divulgação e treinamento	○	○	○	○	○	○
○	○	○	○	○	○	Vigência e validade	○	○	○	○	○	○

12 – Avalie a “importância” e “concordância” dos requisitos do gestão de continuidade classificados no documento de segurança da informação em empresas de desenvolvimento de software para dispositivos móveis.
Para cada elemento listado marque o grau de importância e concordância.

Importância						Gestão de Continuidade do Negócio	Concordância					
SR	[5]	[4]	[3]	[2]	[1]		[1]	[2]	[3]	[4]	[5]	SR
○	○	○	○	○	○	Perda ou roubo de dispositivos móveis ou portáteis da empresa	○	○	○	○	○	○
○	○	○	○	○	○	Perda de equipamentos de grande porte – servidores de redes e arquivos.	○	○	○	○	○	○
○	○	○	○	○	○	Parada de softwares, plataformas de desenvolvimento, aplicativos,	○	○	○	○	○	○

						simulação e testes das aplicações móveis.						
○	○	○	○	○	○	Rotatividade da equipe de desenvolvimento	○	○	○	○	○	○
○	○	○	○	○	○	Perda total do prédio	○	○	○	○	○	○

Sobre a estratégia

13 – Em sua opinião, a estratégia proposta atende o quesito de aplicabilidade?
A estratégia é funcional e passível de ser aplicada dentro das organizações.

Concordância					
SR	**[5]**	**[4]**	**[3]**	**[2]**	**[1]**
○	○	○	○	○	○

14 - Em sua opinião, a estratégia proposta atende o quesito de eficácia?
A estratégia é funcional e capaz de mitigar os riscos e auxiliar a empresa e gerentes na condução de segurança no desenvolvimento de software para dispositivos móveis.

Concordância					
SR	**[5]**	**[4]**	**[3]**	**[2]**	**[1]**
○	○	○	○	○	○

Considerações do questionário

Maringá, _____ de _____ de 2013

ANEXO A

Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos

2 Referência normativa

O documento a seguir referenciado é indispensável para a aplicação desta Norma. Para referência datada, aplica-se apenas a edição citada. Para referência não datada, aplica-se a última edição do documento referenciado (incluindo as emendas).

ABNT NBR ISO/IEC 17799:2005, Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.

3 Termos e definições

Para os efeitos desta Norma, aplicam-se os seguintes termos e definições.

3.1 Ativo

Qualquer coisa que tenha valor para a organização [ISO/IEC 13335-1:2004]

3.2 Disponibilidade

Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada [ISO/IEC 13335-1:2004]

3.3 Confidencialidade

Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados [ISO/IEC 13335-1:2004]

3.4 Segurança da informação

Preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas [ABNT NBR ISO/IEC 17799:2005]

3.5 Evento de segurança da informação

Uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação [ISO/IEC TR 18044:2004]

3.6 Incidente de segurança da informação

Um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação [ISO/IEC TR 18044:2004]

3.7 Sistema de gestão da segurança da informação (SGSI)

A parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação.

NOTA: O sistema de gestão inclui estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos.

3.8 Integridade

Propriedade de salvaguarda da exatidão e completeza de ativos [ISO/IEC 13335-1:2004]

3.9 Risco residual

Risco remanescente após o tratamento de riscos [ABNT ISO/IEC Guia 73:2005]

3.10 Aceitação do risco

Decisão de aceitar um risco [ABNT ISO/IEC Guia 73:2005]

3.11 Análise de riscos

Uso sistemático de informações para identificar fontes e estimar o risco [ABNT ISO/IEC Guia 73:2005]

3.12 Análise/avaliação de riscos

Processo completo de análise e avaliação de riscos [ABNT ISO/IEC Guia 73:2005]

3.13

avaliação de riscos

processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco [ABNT ISO/IEC Guia 73:2005]

3.14 Gestão de riscos

Atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos

NOTA: A gestão de riscos geralmente inclui a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos. [ABNT ISO/IEC Guia 73:2005]

3.15 Tratamento do risco

Processo de seleção e implementação de medidas para modificar um risco [ABNT ISO/IEC Guia 73:2005]

NOTA: Nesta Norma o termo “controle” é usado como um sinônimo para “medida”.

3.16 Declaração de aplicabilidade

Declaração documentada que descreve os objetivos de controle e controles que são pertinentes e aplicáveis ao SGSI da organização.

NOTA: Os objetivos de controle e controles estão baseados nos resultados e conclusões dos processos de análise/avaliação de riscos e tratamento de risco, dos requisitos legais ou

regulamentares, obrigações contratuais e os requisitos de negócio da organização para a segurança da informação.