Universidade Estadual de Londrina

ROGER WILLIAM COÊLHO

GAIA-MLIS: UMA ABORDAGEM APLICADA A UM DIAGNÓSTICO DE NÍVEL DE MATURIDADE EM SEGURANÇA DA INFORMAÇÃO

Londrina
2016

ROGER WILLIAM COÊLHO

GAIA-MLIS: UMA ABORDAGEM APLICADA A UM DIAGNÓSTICO DE NÍVEL DE MATURIDADE EM SEGURANÇA DA INFORMAÇÃO

Dissertação apresentada ao Programa de Mestrado em Ciência da Computação do Departamento de Computação da Universidade Estadual de Londrina, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação.

Orientador: Prof. Dr. Mario Lemes Proença Jr.

Londrina
2016

Ficha de identificação da obra elaborada pelo autor, através do Programa de Geração Automática do Sistema de Bibliotecas da UEL

Coêlho, Roger William.

GAIA-MLIS: Uma Abordagem Aplicada a um Diagnóstico de Nível de Maturidade em Segurança da Informação / Roger William Coêlho. - Londrina, 2016.

107 f. : il.

Orientador: Mario Lemes Proença Junior.

Dissertação (Mestrado em Ciência da Computação) - Universidade Estadual de Londrina, Centro de Ciências Exatas, Programa de Pós-Graduação em Ciência da Computação , 2016.

Inclui bibliografia.

1. Segurança da Informação - Tese. 2. Governança de TI - Tese. 3. GAIA-MLIS - Tese. I. Proença Junior, Mario Lemes. II. Universidade Estadual de Londrina. Centro de Ciências Exatas. Programa de Pós-Graduação em Ciência da Computação . III. Título.

ROGER WILLIAM COÊLHO

GAIA-MLIS: UMA ABORDAGEM APLICADA A UM DIAGNÓSTICO DE NÍVEL DE MATURIDADE EM SEGURANÇA DA INFORMAÇÃO

Dissertação apresentada ao Programa de Mestrado em Ciência da Computação do Departamento de Computação da Universidade Estadual de Londrina, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação.

BANCA EXAMINADORA

_____

Orientador: Prof. Dr. Mario Lemes Proença Jr.
Universidade Estadual de Londrina - UEL

_____

Prof. Dr. Alexandre de Aguiar Amaral
Instituto Federal de Santa Catarina - IFSC

_____

Prof. Dr. Elieser Botelho Manhas Jr.
Universidade Estadual de Londrina - UEL

_____

Prof. Dr. Wesley Attrot
Universidade Estadual de Londrina - UEL

Londrina, 27 de junho de 2016.

Este trabalho é dedicado a Deus, a minha família e amigos que me apoiaram nessa nova etapa da minha vida e aos meus professores por terem a paciência de ensinar não só o conteúdo das matérias, mas também passando a experiência necessária para que eu me tornasse um ótimo profissional.

AGRADECIMENTOS

A Deus, pelo poder do Espírito Santo, conceder a sabedoria, paciência e a inteligência necessária para o cumprimento dessa etapa na minha carreira profissional e na minha vida pessoal.

Agradeço a minha família pelo apoio durante o programa do mestrado desde o início até a conclusão. Aos meus amigos pela compreensão e força diante a elaboração desse trabalho.

Meus sinceros agradecimentos ao professor e orientador Dr. Mario Lemes Proença Junior, pela paciência de me ensinar e contribuir para o meu sucesso nesse mestrado. Aos demais professores que proporcionaram o conhecimento técnico e científico necessário para a realização desse trabalho. Também quero deixar aqui os meus mais sinceros agradecimentos a toda ajuda do meu amigo Luiz Fernando Carvalho, que durante o programa de mestrado pôde me ajudar no laboratório para a realização e o sucesso deste trabalho.

COÊLHO, Roger William. **GAIA-MLIS:** Uma Abordagem Aplicada a um Diagnóstico de Nível de Maturidade em Segurança da Informação. 2016. 107 f. Dissertação (Mestrado) – Universidade Estadual de Londrina, Londrina, 2016.

RESUMO

A proteção da informação com gestão estratégica, bem como bens físicos e pessoas, são observados como ativos importantes para a elaboração, execução e continuação do negócio. Gerenciar risco de segurança é uma tarefa difícil, mas para encontrar o sucesso, investimentos em suporte e gestão de tecnologia devem ser feitos, além de verificar o nível de maturidade do sistema de segurança da informação, cujo objetivo é identificar pontos fortes e pontos fracos nos processos avaliados. Assim, a abordagem GAIA-MLIS é proposta para analisar qual é o nível de maturidade em segurança da informação e como as organizações podem melhorar seus processos e métricas. Esta abordagem tem o objetivo de fazer uma avaliação diagnóstica em cinco áreas relacionadas a serviços de Tecnologia da Informação e Comunicação, identificando pontos fortes e fracos nos processos, normas e políticas de segurança implementados. Esta avaliação será utilizada para identificar e sugerir pontos de melhorias com base na abordagem de maturidade em segurança proposta.

Palavras-chave: Segurança da Informação. Governança de TI. GAIA-MLIS.

COÊLHO, Roger William. **GAIA-MLIS:** Uma Abordagem Aplicada a um Diagnóstico de Nível de Maturidade em Segurança da Informação. 2016. 107 p. Dissertação (Mestrado) – Universidade Estadual de Londrina, Londrina, 2016.

ABSTRACT

The protection of information with strategic management as well as of physical assets and people, is considered as important assets for the development, implementation and continuation of the business. Managing security risk is a difficult task, but to find success, investment in support and technology management should be done, besides the verification of the maturity level of information security system, which aims to identify the strengths and weaknesses in the evaluation processes. Thus, the GAIA-MLIS model is proposed to analyze what is the maturity level in information security and how organizations can improve their processes and metrics. This approach aims to make a diagnostic evaluation in five areas related to Information and Communication Technology services, identifying strengths and weaknesses in the processes, implemented security standards and policies. This assessment will be used to identify and suggest points of improvement based on the proposed security maturity approach.

Keywords: Information Security. IT Governance. GAIA-MLIS.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

CIS	*Center for Internet Security*
COBIT	*Control Objectives for Information and Related Technology*
CSC	*Critical Security Control*
FM	Fator Multiplicativo
GED	Gerenciamento Eletrônico de Documentos
IDS	*Intrusion Detection System*
IP	*Internet Protocol*
IPS	*Intrusion Prevention System*
ISO	*International Organization for Standardization*
MLIS	*Maturity Level Information Security*
NSA	*National Security Agency*
SOA	*Service Oriented Architecture*
SRI	*Stanford Research Institute*
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
TLS	*Transport Layer Security*
UCLA	*University of California, Los Angeles*
UCSB	University of California, *Santa Barbara*
UEL	Universidade Estadual de Londrina
VoIP	*Voice over* IP

SUMÁRIO

1 INTRODUÇÃO

Como um resultado rápido do progresso tecnológico, a rede de dados tornou-se uma ferramenta que promove mecanismos importantes de comunicação. Este progresso proporcionou a popularização de serviços como *e-commerce* (comércio eletrônico), acesso remoto, compartilhamento de arquivos, *Voice over* IP (VoIP), *Cloud Computing*, entre outros. Além disso, devido ao aumento da disponibilidade de rede em vários locais é possível acessar os serviços por meio de dispositivos móveis, trazendo praticidade na obtenção da informação [1].

Embora a evolução das redes tenha trazido benefícios, alguns problemas surgiram em paralelo, como exposição dos dados dos usuários e a complexidade empregada no controle de acesso a informações sigilosas [1]. Nesse cenário, uma nova preocupação começou a difundir-se perante a comunidade científica, a segurança da informação. Desde o ataque com o *worm* desenvolvido por Morris em 1988, novas técnicas de ataques tornaram-se mais complexas e sofisticadas [2]. Dessa maneira, o aprimoramento das técnicas de invasão influencia para a criação de medidas de segurança da informação, como políticas, questões de privacidade, treinamento e ética [3].

A informação no âmbito organizacional é um recurso importante para possibilitar as atividades operacionais da empresa. Este fato independe do porte, segmento ou se a empresa pertence à iniciativa privada ou pública. Com a utilização da informação, os funcionários podem desenvolver as suas atividades profissionais, a fim de gerar e compartilhar conhecimento, tendo como foco o seu crescimento corporativo. Assim, os objetivos da empresa são atingidos, produzindo maior chance de sua evolução no nicho no qual atua.

A disponibilidade, integridade e a confidencialidade com que a informação precisa ser mantida e transmitida são necessidades encontradas no âmbito organizacional. Com o avanço tecnológico, as empresas conseguem manter maiores quantidades de informações de modo mais seguro, permitindo a disponibilidade para mais pessoas a qualquer momento. Isso gera grandes possibilidades de negócios, novos serviços e produtos.

Falhas no sistema ou ações criminosas podem tornar públicas as informações sigilosas, ou efetuar bloqueio ao acesso às informações críticas usadas para a realização dos objetivos organizacionais. A informação pode posicionar a organização em um determinado patamar, elevando-a perante ao mercado, ou comprometendo-a e colocando-a em uma situação

desfavorável. Essa condição negativa ocorre em caso de eventos de segurança, erros ou fraudes, ocasionando impacto financeiro, na imagem e na parte operacional da organização [4].

Apesar da grande quantidade de trabalhos desenvolvidos na área de segurança, o surgimento de novos problemas impulsiona a investigação de uma abordagem de avaliação do nível de maturidade neste contexto. Alguns autores realizam trabalhos com o intuito de introduzir a análise da segurança no âmbito da governança de TI (Tecnologia da Informação) [5] [6]. O trabalho de Rigon *et al.* [5] preconiza um modelo baseado nas normas ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 e no COBIT (*Control Objectives for Information and Related Technology*). Seu modelo utiliza-se de um método quantitativo para as análises de riscos e, por meio de escalas, mensura e descreve o potencial dos impactos que um evento de segurança pode ocasionar.

Por sua vez, Karokola *et al.* [6] descreve uma proposta de um Modelo de Maturidade em Segurança da Informação (MMSI) para os serviços de governo eletrônico. Basicamente, esse modelo é baseado nos resultados da análise crítica de abordagens de maturidade de segurança da literatura. Esse trabalho é de cunho teórico e não apresenta um estudo de caso de aplicação do modelo proposto.

Com base no COBIT 5 e nas normas ISO/IEC 27001 e ISO/IEC 27002, o objetivo do presente trabalho é apresentar uma abordagem de avaliação de segurança da informação no contexto organizacional. Esta abordagem, GAIA-MLIS (*Maturity Level Information Security*), possui o propósito de identificar, nas áreas analisadas, os pontos de melhoria nos processos, normas e políticas de segurança implementados pelas empresas, posicionando-os de acordo com uma abordagem de nível de maturidade em segurança da informação.

A GAIA-MLIS é composto por um conjunto de métricas descritivas responsáveis por mapear os aspectos de avaliação com o nível de maturidade, e indica quais são as características de cada área em análise. Essas áreas são: (i) *hardware*, (ii) *software*, (iii) instalações/espaços físicos, (iv) pessoas e (v) informação. O mecanismo de avaliação do nível de segurança da informação utilizado é baseado em um questionário que visa investigar os principais elementos deste contexto. Os trabalhos de Rigon *et al.* [5] e Karokola *et al.* [6] contribuem com o GAIA-MLIS por auxiliarem na elaboração das medidas e ações, além de subsidiarem as escolhas das normas ISO 27000 e do *framework* COBIT. Porém, esses trabalhos diferem da abordagem proposta por não verificarem as cinco áreas de forma conjunta.

Com os dados e as métricas de segurança da informação, os Gestores de TI podem efetuar planos e metas, a fim de atingirem níveis mais consistentes em segurança da

informação, além de terem uma abordagem capaz de auxiliar no alcance dessas metas. Desse modo, a abordagem GAIA-MLIS surge para auxiliar no melhoramento contínuo do nível de maturidade em segurança da informação. As respostas obtidas por meio de um questionário de avaliação diagnóstica tem o objetivo de indicar o nível de maturidade em segurança da informação. Através dos resultados, as necessidades e melhorias para os processos e políticas já existente são expostas. Por meio do GAIA-MLIS, é possível determinar uma série de ações capazes de indicar quais práticas de segurança devem ser aprimoradas, com base nas respostas obtidas.

O trabalho está organizado do seguinte modo: O capítulo 2 apresenta a contextualização da segurança da informação. O capítulo 3 aborda a governança de TI apresentando o *framework* COBIT, normas e padrões utilizados em conjunto da segurança da informação. O capítulo 4 detalha a abordagem da GAIA-MLIS. O capítulo 5 demonstra e avalia os resultados da aplicação do questionário diagnóstico da GAIA-MLIS, além de ações que podem ser tomadas para elevar o nível de maturidade das áreas verificadas. Por fim, o capítulo 6 apresenta as conclusões e os trabalhos futuros.

2 SEGURANÇA DA INFORMAÇÃO

Durante as últimas décadas, perdas, indisponibilidades e vazamento de dados proporcionaram o comprometimento dos processos de negócios, causando danos às instituições, desde prejuízos financeiros a acordos de nível de serviço não cumpridos [11]. Recentemente, jornais e revistas publicaram o comprometimento de informações sigilosas de países e organizações, como as divulgações efetuadas pela página de Internet *Wikileaks* e o caso Edward Snowden, em que a Agência Nacional de Segurança dos Estados Unidos da América, sigla em inglês NSA (*National Security Agency*) adquiria dados sem um mandado judicial. Esse crescente vazamento de dados proporciona o desenvolvimento de métodos e medidas para minimizar ou evitar possíveis ataques.

Com uma grande variedade de vulnerabilidades e ameaças que podem ser exploradas por pessoas ou organizações mal-intencionadas, existe a necessidade da implementação de conjuntos de controles, incluindo políticas, processos, procedimentos, entre outros. Esses controles devem ser estabelecidos, implementados, monitorados, analisados e revisados, com o objetivo de garantir a segurança da gestão dos processos de negócios da organização [5].

O cenário torna-se ainda mais crítico com o crescente número de vulnerabilidades associadas aos diversos ativos, como pessoas, *softwares*, instalações/espaços físicos, entre outros, os quais oferecem suporte aos processos de negócio das empresas. As organizações devem desenvolver meios capazes de proteger os ativos considerados críticos, como pessoas e a informação. Dessa forma, a gestão de risco é importante para que as empresas possam identificar vulnerabilidades e ameaças, além dos impactos de um incidente de segurança da informação [12].

Contudo a informação deve ser protegida para que a sua operabilidade e continuidade sejam mantidas. Para isso, o planejamento estratégico da organização tem a necessidade de voltar-se para a segurança da informação.

Segundo Hua [13], a disciplina dedicada à proteção da informação define a forma de garantir a continuidade dos negócios, tendo como objetivo minimizar os danos causados por algum incidente de segurança e maximizar o retorno dos investimentos.

Riscos e ameaças à segurança, como vírus, *worms*, *spyware* e *phishing*, entre outros, tornaram-se um problema para os usuários e profissionais de TI, uma vez que com o comprometimento do sistema computacional e da rede de dados, como também a submissão da

informação pode ser realizada. O comprometimento da segurança resulta na exposição de informações sensíveis aos processos de negócios das organizações, bem como informações pessoais de clientes podem ser usadas para fins escusos [14].

A fim de prover um melhor gerenciamento na segurança da informação, alguns métodos estão sendo desenvolvidos, como o trabalho realizado por Mayer e Fagundes [12] um método para análise, medindo o nível de maturidade em segurança da informação. Dessa forma, há um auxílio no gerenciamento e na documentação dos padrões de segurança.

Métodos e formas de como gerenciar, planejar e monitorar os ativos presentes dentro de uma organização acarreta em investimentos pesados em segurança da informação, seja ela em ambiente virtual, como em ambiente físico. A necessidade de gerir a informação, também passa por um processo que envolve as pessoas que trabalham nas empresas, visto que estas são as mais propícias a causarem um evento de segurança.

Um conceito novo na área de segurança que está ganhando força refere-se à forense corporativa. Este conceito é definido como a busca de uma coleção de evidências nos sistemas computacionais, como forma de padronizar e documentar, além de manter a aceitabilidade em um processo judicial. Esse novo método é necessário nas organizações, a fim de investigar como um tipo de evento de segurança da informação foi ocasionado [15].

2.1 Trabalhos Relacionados

Esta seção apresenta uma breve descrição de diversos trabalhos relacionados que são destinados à obtenção do nível de maturidade em segurança da informação. Esses trabalhos foram escolhidos devido a sua relevância dentro do campo de segurança da informação.

O modelo proposto por Woodhouse [48] visa indicar controles, não somente na parte técnica da segurança da informação, mas também na parte gerencial e operacional. Esse modelo possui nove níveis, de menos três até cinco, e cada um deles descreve a cultura corporativa que garante os riscos aceitos pela organização e seus parceiros. Dessa forma, o trabalho indica questões culturais e comportamentais do ambiente de trabalho para que as empresas possam identificar o nível de maturidade em segurança da informação.

Mayer e Fagundes [49] descrevem um modelo para avaliar o nível de maturidade do processo de gerenciamento de riscos em segurança da informação. Esse trabalho é baseado no gerenciamento de riscos aceitáveis e não aceitáveis pelas empresas e, a partir

desse, estudo o nível de maturidade em segurança da informação é determinado para a empresa. O modelo é subdividido em cinco níveis do inicial ao otimizado, esses subníveis estão dentro de outros três níveis maiores, os quais são classificados como imaturo, maduro e excelente. O trabalho tem como base a utilização da norma ISO 27005.

Regulwar et al. [50] apresentam um *framework* de processos em engenharia de segurança da informação capaz de verificar o nível de maturidade das organizações. O objetivo desse modelo é desenvolver uma cultura organizacional de melhoria contínua nos processos de engenharia de segurança através de medição e produção de novas ações. Esse trabalho consiste em uma sequência de cinco níveis de maturidade que orientam a empresa a verificarem os processos através de pequenos ajustes, visando processos de melhoria na engenharia de segurança.

No trabalho desenvolvido por Stambul e Razali [51] é discutido um modelo com três níveis de maturidade em segurança da informação que consiste em medir e avaliar o grau da segurança dentro da empresa. Esse estudo utiliza parâmetros de modelos gerais e normas e padrões em segurança da informação usados na literatura. As áreas analisadas no desenvolvimento dos níveis de segurança da informação do modelo proposto são processos, tecnologia e pessoas.

No estudo realizado por Kassou et al. [52] um modelo de nível de maturidade é definido por meio de abordagens de melhores práticas em segurança da informação, como a norma ISO 27002. O paradigma aplicado é arquitetura orientada a serviços. Cinco níveis de segurança da informação são usados para a análise da empresa. O nível inicial é o *Trial SOA (Service Oriented Architecture)* que denota a segurança básica. O nível de maior expressão é o *On Demand SOA* que indica uma segurança dinâmica para a proteção da informação da corporação.

No trabalho realizado por Zhao e White [53] é proposto níveis de alerta de ameaças compartilhada com a comunidade cibernética. O modelo apresentado possui quatro níveis de segurança da informação, sendo o nível inicial apresenta maior deficiência e o nível quatro denota maior eficiência na segurança. Por meio desses níveis a comunidade cibernética consegue identificar os riscos aceitos em seus processos e compartilhar a informação de gerenciamento de riscos com base na análise proposta.

Esses trabalhos diferem do GAIA-MLIS por não analisarem as áreas de *hardware*, *software*, instalações, pessoas e informação de forma conjunta. Também, tem como finalidade avaliar o nível de maturidade em segurança da informação nessas áreas. Quatro

níveis de segurança da informação são propostos. A abordagem tem o mapeamento de parâmetros diagnosticados e os respectivos pontos de melhoria para as cinco áreas.

2.2 Definições sobre Segurança da Informação

Nesta seção serão apresentados alguns conceitos de segurança da informação. Esses conceitos são caracterizados como a base da segurança em um ambiente computacional.

Ataque cibernético é caracterizado pela utilização de dispositivos eletrônicos conectados à rede de dados, com o objetivo de obter informação de uma organização ou pessoa de forma não autorizada. Um ataque pode causar danos nos serviços prestados por uma entidade[1], por meio de ataques de negação de serviço, falsificação de *e-mail*, *scan* não autorizados na rede de dados, interceptação de tráfego, entre outros [1].

Um evento de segurança da informação é a eventualidade identificada em uma rede de dados, sistema de informação ou serviço, que indica uma possível violação de segurança da informação ou falhas nos processos e controles, ou uma situação previamente desconhecida, que passa ser relevante para a segurança da informação [45].

A característica de um incidente de segurança da informação é expressa por um simples ou por séries de eventos de segurança da informação indesejados ou inesperados, que possuem grande probabilidade de acontecer e comprometer as operações do negócio e ameaçar às informações da empresa [42].

Ameaça a segurança da informação é caracterizada pela causa potencial de um incidente não desejado, e o mesmo pode resultar em dano para o sistema ou organização [42].

Vulnerabilidade é a fragilidade que um ativo de informação apresenta, que pode ser explorada por uma ou mais ameaças, sejam elas, *crackers*, falhas de códigos, entre outros [45].

O princípio da disponibilidade é a propriedade caracterizada pela informação estar acessível e utilizável sob demanda por uma pessoa ou organização autorizada [42]. A confidencialidade é o princípio que a informação esteja relacionada ao fato de manter as informações longe de usuários não autorizados [1]. A integridade é a propriedade de salvaguarda da completeza e exatidão dos ativos da informação [45].

[1] A entidade pode ser um programa de computador, pessoa ou organização.

Não repúdio ou irretratabilidade é a propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente realizada. Autenticação identifica se a entidade é realmente quem ela diz ser [1].

2.3 Necessidade da Segurança da Informação

Nos últimos anos, as organizações tem sido expostas a diversos tipos de ameaças à segurança da informação, como vírus, DoS, entre outros, nos sistemas de informação e redes de computadores. Estas ameaças incluem fraudes eletrônicas, sabotagem, espionagem etc. Os *crackers* usam códigos maliciosos e ataques como o de negação de serviço para adquirir informações sigilosas de uma organização. Definir, alcançar, manter e melhorar a segurança da informação asseguram uma maior confiabilidade e competitividade das organizações [5]. As questões de segurança da informação refletem, também, no âmbito da segurança nacional, já que nos últimos anos há uma crescente guerra cibernética em curso. Dessa maneira, proteger a informação passou de uma mera formalidade para uma real necessidade das organizações [16].

Grandes exigências e obrigações internas e externas, como critérios de confidencialidade aos clientes, parceiros e prestadores de serviço, além dos riscos e do alto custo para a efetivação de uma política de segurança da informação são as razões para o interesse de uma segurança com um alto nível de proteção para as empresas [17].

A confiabilidade, disponibilidade e a integridade das infraestruturas de redes corporativas são essenciais para as organizações, para que sejam utilizadas em conformidade com o planejamento estratégico. Para tanto, proteger a informação tem como o objetivo manter o acesso disponível aos usuários, ou seja significa que toda a informação deve chegar de forma íntegra e confiável. Uma informação mantida de maneira sigilosa em conjunto com a integridade e a disponibilidade são propriedades importantes para a segurança [18].

A Figura 2.1 apresenta os ataques realizados em várias regiões do mundo, monitorados por meio do monitor *Akamai*. Com esses dados, é possível identificar as regiões onde ocorre o maior número de ataques nesse período de tempo. Esses levantamentos são referentes ao dia 27 de maio de 2016.

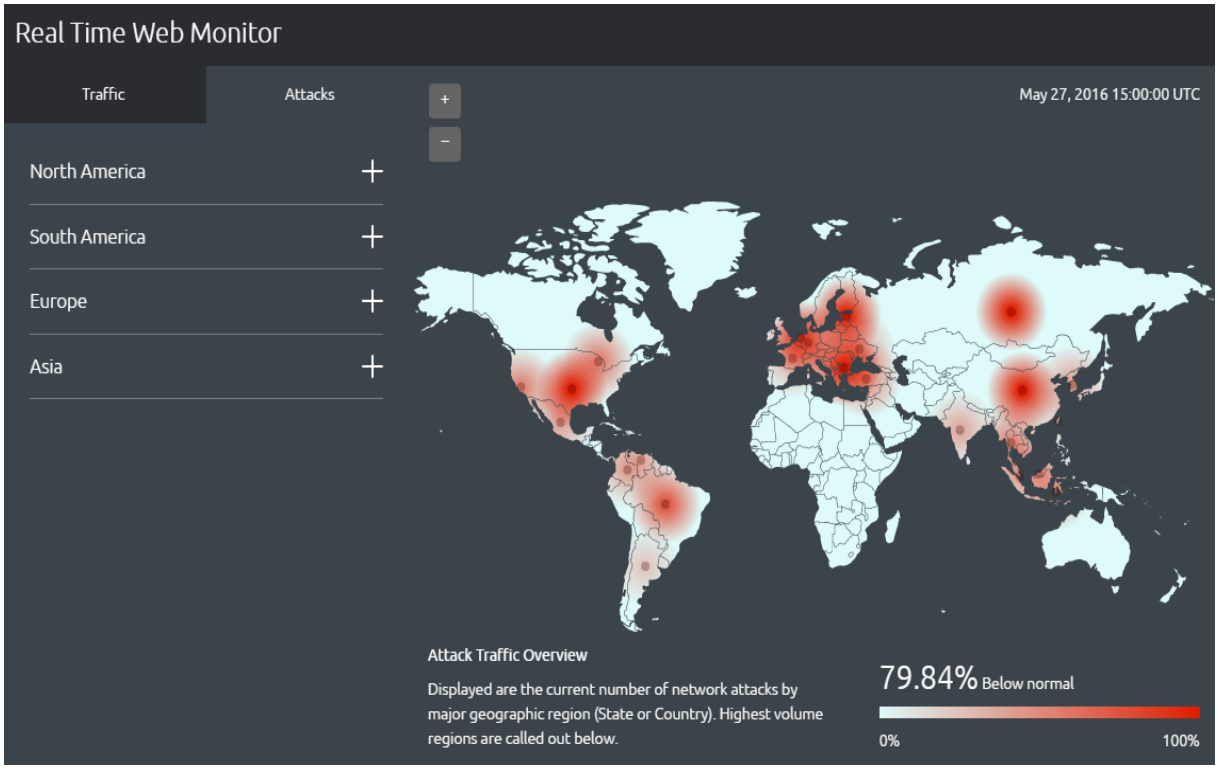

Figura 2.1 – Monitoramento de ataques. Fonte akamai [19].

Visto que há uma demanda de ataques virtuais crescentes, os processos de segurança devem estar alinhados a um planejamento eficaz e supervisionado, para que os riscos previstos e as responsabilidades e os papéis de cada funcionário ou setor sejam determinados e delegados. Consequentemente, é necessário que a organização mantenha um processo de governança de riscos de segurança que é estrategicamente dirigido e sistematicamente capaz de utilizar os recursos disponíveis de forma eficiente [17].

A Figura 2.2 refere-se às propriedades que são importantes para a informação.

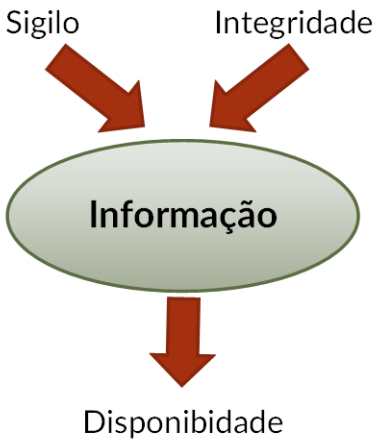

Figura 2.2 – Propriedades importantes da segurança. Fonte [18].

Como apresentado na Figura 2.2 o sigilo e a integridade estão relacionados à informação, o que acarreta em disponibilidade de acesso aos usuários. Dessa forma, a segurança da rede é essencial para que a disponibilidade da informação seja mantida e transmitida sem ser alterada por agentes[1] internos ou externos da rede que não possuem acesso autorizado [18].

A Figura 2.3 é demonstram o total de incidentes reportados ao CERT por ano.

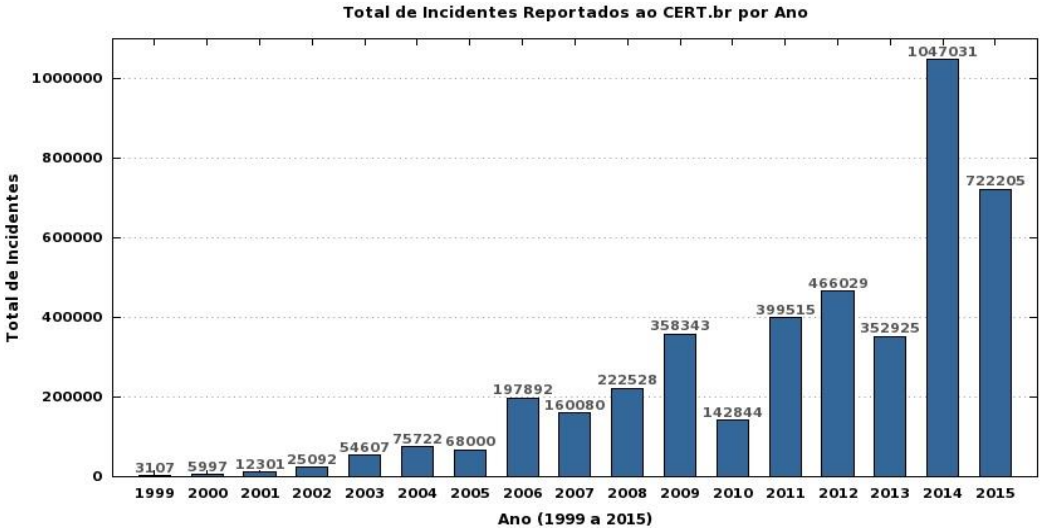

Figura 2.3 – Total de incidentes reportados ao CERT.br. Fonte cert.br [20].

Como pode ser verificado na Figura 2.3, o número de incidentes totais reportados ao CERT é crescente a cada ano, mesmo que em alguns anos esse número seja um pouco inferior ao anterior. O ano com menor taxa de incidentes reportados é o de 1999 com um total de 3107 incidentes, enquanto o ano que teve mais incidentes foi o de 2014 com um total de 1047031. Isso indica que quanto mais as empresas estão informatizando e utilizando a rede de dados para os seus planos de negócios, os ataques direcionados para roubo de dados estão acontecendo com maior frequência. Isso acarreta às organizações prejuízos financeiros em acordos de serviços não cumpridos e na credibilidade das mesmas junto ao mercado.

Alguns tipos de ataques reportados mais comuns são fraudes, *scan*, web, invasão, ataque de negação de serviços (DoS) dentre outros, que não fazem parte das categorias anteriores. Ataques do tipo fraude, são caracterizados pela tentativa de obter vantagem. Ataques tipo *scan*, são caracterizados por varreduras nas redes de computadores para a identificação de quais computadores estão ativos e os tipos de serviços disponibilizados por eles. Ataque tipo web visa o comprometimento de servidores Web ou alterar páginas na Internet. Ataque tipo invasão é aquele que resulta no acesso não autorizado a um computador ou rede. Ataque *Denial*

[1] Pessoa ou organização que possui acesso a informação.

of Service (DoS) é resultante de negação de serviço, em que o atacante utiliza um conjunto de computadores para tirar de operação alguma rede ou serviço [20].

A Figura 2.4 evidencia os dados referentes aos tipos de ataques acumulados reportados ao CERT.

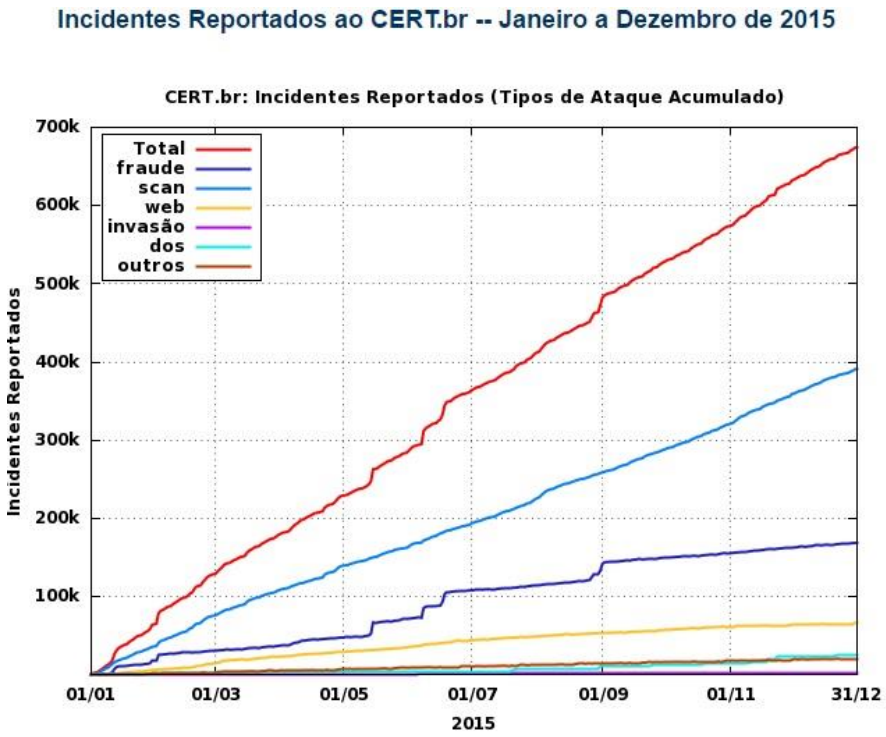

Figura 2.4 – Ataques acumulados. Fonte cert.br [20].

Estes incidentes aconteceram com maior frequência via *scan* explorando quais os computadores ativos e os serviços que os mesmos estavam operando. Fato este que totalizou, no fim do ano de 2015, aproximadamente 400 mil incidentes reportados.

Um tipo de envio de informações não solicitadas via e-mail, também conhecido como *spam*, gera um grande número de notificações por ano. Os *spams* são caracterizados pelo grande envio de e-mails para um grande número de pessoas. Esses e-mails não são solicitados pela pessoa, ou até mesmo não são enviados pelas pessoas que tem o seu endereço eletrônico usado para esse fim. Isso se deve pela popularização do correio eletrônico como forma de comunicação pessoal, como na utilização para os negócios. Uma média de 120 bilhões *spams* por dia são enviados. Estes tipos de e-mails não desejados interferem desde prestadores de serviços de e-mails como a usuários finais. São utilizados filtros AntiSpam para o bloqueio do envio e do recebimento de e-mails não desejados, mesmo assim a atuação do usuário final na proteção do computador é determinante para a diminuição na ocorrência de envio de *spams* [21].

Vários métodos de segurança que vão desde em equipamentos e até mesmo a do ambiente de trabalho são utilizados pelas organizações, a fim de evitarem ou minimizarem as perdas e os danos ocasionados por um evento de segurança. Porém, devido aos grandes avanços tecnológicos, novas funcionalidades estão surgindo e como consequência novos riscos à segurança da informação devem ser considerados. Assim, faz-se necessário a utilização de novas técnicas e tecnologias para a defesa contra os ataques.

2.3.1 Riscos em Segurança da Informação

Os riscos que as organizações sofrem de um possível ataque de segurança da informação, vão além da parte técnica e virtual. Muitas vezes, os pontos que antes não eram muito explorados, como a engenharia social e a estrutura física são comumente averiguados por organismos criminosos ou governamentais.

Especificamente, na parte técnica, algo que pode ser explorado são as falhas de equipamentos ou configurações inadequadas. Isto acarreta em alguma oportunidade para a realização de uma invasão na rede. Estes tipos de falhas acontecem corriqueiramente, à medida que os fabricantes visam o lançamento dos produtos como forma de venda e novas soluções, diminuindo o tempo de desenvolvimento. Assim os produtos chegam até ao mercado sem um controle de qualidade adequado, e muitas vezes com falhas graves em segurança [18].

Porém, o elo mais fraco na cadeia de segurança de informação são os usuários, pelo simples fato de que eles podem ser manipulados por *crackers* por meio de algum método ilícito, como forma de obter alguma informação de dentro da empresa [22]. Por conseguinte, a engenharia social utilizada neste contexto, refere-se a várias técnicas que são construídas para obter informação, a fim de explorar os sistemas de segurança pela sua vulnerabilidade humana [23]. Isso ocorre porque muitas pessoas não têm ciência de que essas técnicas são utilizadas em um ataque. Na maioria dos incidentes, as pessoas não percebem que são vítimas ou acreditam que nunca serão vítimas de um ataque. Os indivíduos não percebem o valor de algumas informações e o impacto das consequências geradas pela divulgação de algum dado que pode ser usada de forma maliciosa [24].

Visto que existem várias maneiras de obter-se informações sigilosas de uma organização, seja pelo meio tecnológico (por exemplo, invasão de servidores ou exploração de falhas dos sistemas), como pela engenharia social, as empresas devem estar capacitadas para

responder às ocorrências de algum tipo de evento de segurança da informação. Dessa maneira, faz-se necessário gerenciar os potenciais riscos de segurança da informação que a empresa possa ter.

2.4 Gerenciamento de Risco

Os sistemas de informação e as redes de dados são utilizados por mais pessoas a cada dia, muito disto deve-se à crescente interconexão de vários dispositivos, sejam eles computadores, *smart* TVs, smartphones, entre outros. Novos serviços são disponibilizados pelas empresas com a finalidade de atrair mais usuários conectados a essas redes. Porém, garantir a proteção dos dados de um usuário, parceiro de negócios, e até mesmo as informações da empresa prestadora do serviço, consiste em uma tarefa árdua e difícil de ser gerida. Como mencionado anteriormente, vários métodos, como os de caráter técnicos e a engenharia social, são utilizados pelos atacantes como forma de obtenção de dados restritos das organizações.

Dessa maneira, a prevenção e a capacidade de analisar os riscos, assim como, a de neutralizar as ameaças que ocorrem ou podem ocorrer, tem se tornado um fator para o sucesso e a credibilidade da organização. A gestão dos processos de negócios fornece conceitos para a otimização econômica de processos, enquanto a gestão de riscos concentra-se na concepção de processos de negócios, para atingir uma compreensão diferente da esperada, no que se refere à melhoria dos processos de negócios da empresa alinhada a uma segurança da informação eficiente [25].

Desse modo, a gestão de risco possui como desafio proteger um dos principais ativos de uma organização, a informação. Os processos para gerenciar um risco compreendem atividades coordenadas que visam controlar e orientar uma organização. A abrangência dessas atividades tem como contexto a análise, avaliação, tratamento, aceitação e a comunicação e o acompanhamento dos riscos de segurança da informação. Convém salientar que os riscos podem ser vistos como a probabilidade de vulnerabilidades aproveitadas por ameaças geradas por atacantes, o que pode resultar na perda da confidencialidade, integridade e a disponibilidade da informação, além de um possível impacto na imagem da empresa junto ao mercado [12].

As abordagens da gestão de risco diferem na sua aplicação específica, porém a maioria dos métodos existentes consistem em pelo menos uma das seguintes fases. A primeira fase baseia-se na identificação dos potenciais riscos, tendo por objetivo desenvolver uma estratégia capaz de lidar com diferentes riscos de segurança. Para tanto, é de suma importância

avaliar e priorizar quais os tipos de riscos são mais propícios à ocorrência. A segunda fase os riscos precisam ser verificados, e portanto, devem ser monitorados, para que caso ocorra uma possível mudança nos tipos analisados, a prioridade ou até mesmo a forma de tratamento seja alterada. E por fim, a terceira fase avalia os riscos como um mecanismo de garantia de uma melhoria na gestão dos processos e da gestão de segurança da informação [25].

A identificação dos riscos é o processo de encontrar incidentes que podem danificar os sistemas de informação e os processos de negócios. A avaliação dos riscos possui aplicações tanto na ordem quantitativas ou qualitativas como forma de prever os impactos dos potenciais incidentes identificados [25]. O tratamento dos riscos é o processo que ocorre após a avaliação, nessa etapa, podemos identificar quatro práticas. A primeira não fazer nada e aceitar o risco. A segunda, evitar potenciais acidentes, alterações ou extinção das ações associadas ou processos de negócios. A terceira é baseada na transferência segura dos riscos para outros parceiros e a quarta e última, é a aplicação de medidas de segurança adequadas para reduzir os riscos a níveis aceitáveis. Por fim, o monitoramento e a reavaliação dos riscos visam identificá-los de forma residual, bem como aqueles que se tornaram aceitáveis, com a finalidade de garantir a precisão e a eficácia da avaliação e do tratamento da informação. Além disso, uma organização necessita reavaliar as suas falhas, a fim de refletir sobre as grandes mudanças no modo de como um evento de segurança da informação pode ser tratado [26].

A Figura 2.5 é uma adaptação do trabalho desenvolvido por Goluch *et al*. [25] que demonstra uma breve descrição do conceito criado pelos autores sobre a segurança da informação e as suas ameaças. Esta contribuição refere-se ao gerenciamento de risco de uma organização.

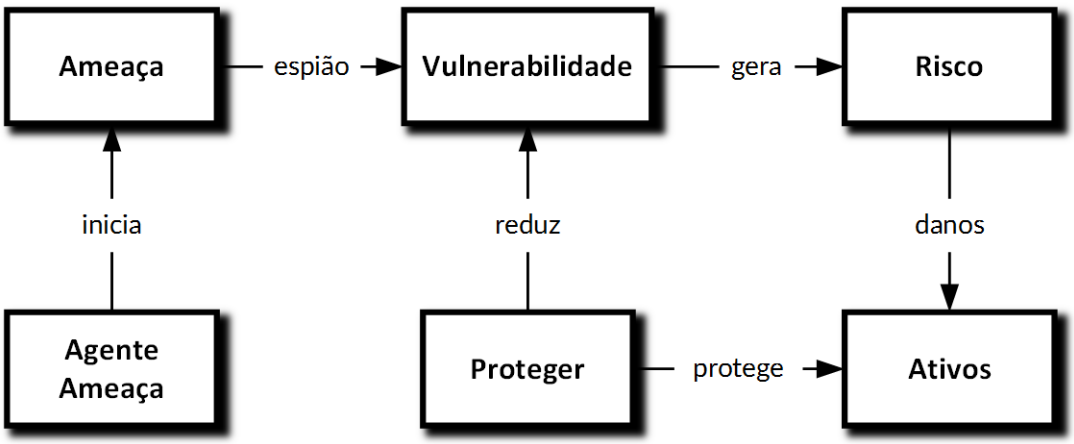

Figura 2.5 – Relacionamento de segurança. Adaptado de [25].

Como é possível observar, o agente da ameaça inicia uma ação com a intenção de realizar um ataque. O espião é o responsável por encontrar as vulnerabilidades presentes nos

processos de segurança da organização, com a finalidade de explorar potenciais falhas de segurança e por meio delas furtar qualquer tipo de informação. Para tanto, um processo documentado visa verificar quais são as vulnerabilidades presentes nos processos de segurança, para que com isso haja a redução de potenciais riscos e que os ativos da organização sejam protegidos.

A avaliação de riscos de uma organização auxilia na obtenção da segurança da informação conjunta com o planejamento estratégico.

Portanto, o método da avaliação de risco de segurança fornece duas vantagens principais. A primeira é a de monitorar as políticas de segurança e proteger efetivamente os ativos críticos corporativos. A segunda vantagem é a de fornecer dados para a análise de futuras estimativas, dos potenciais riscos e pela obtenção destas informações possa desenvolver uma gestão de segurança [27]. Muitas vezes, os processos de um gerenciamento de risco podem sofrer algum tipo de modificação, ainda mais, quando os serviços realizados dentro da organização passam por algum tipo de terceirização. É importante salientar áreas como gestão de instalações, processos de negócios, finanças, e até mesmo, a tecnologia da informação estão sofrendo esse processo como forma de baratear os custos da empresa, e de certa forma, tomar como o foco a área de negócios, investindo mais no produto da empresa propriamente dito do que em funcionários efetivos da organização. Esses riscos podem ser mais significativos pela má intenção de um funcionário terceirizado ou pelo uso da engenharia social sofrida por estes tipos de profissionais [28].

A Figura 2.6 demonstra a complexidade do gerenciamento de risco dentro de uma organização.

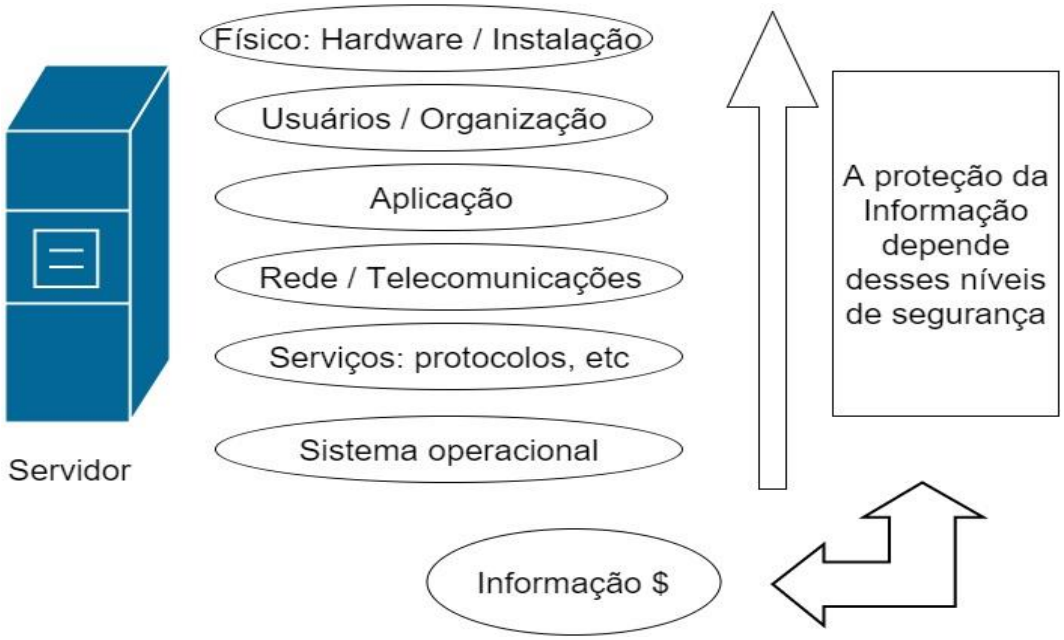

Figura 2.6 – Complexidade da segurança da informação. Fonte [18].

Partindo do sistema operacional, até a parte da segurança física do ambiente, todos esses níveis devem ser verificados e classificados quanto à segurança da informação. O ambiente monitorado e protegido precisa atender de forma conjunta todos os processos dentro da organização. A complexidade é alta quando há funcionários que não são somente efetivos, mas também, aqueles que são terceirizados e prestam serviço para a organização, visto que os dados da empresa devem ser mantidos protegidos contra agentes internos ou externos não autorizados.

O gerenciamento de risco ajuda na concepção de métodos e métricas capazes de auxiliarem na construção de um planejamento de tratamento de eventos de segurança da informação. Para um melhor gerenciamento dos riscos, os diretores das empresas devem atentar que a governança corporativa voltada para a área de segurança da informação precisa ser vista como um mecanismo de elaboração de responsabilidades entre os setores e funcionários. A governança corporativa auxilia na criação de padrões que a corporação poderá adotar para definir medidas e planos de contingência como forma de solucionar ou evitar eventos em segurança da informação.

2.4.1 Política de Segurança

A política de segurança é uma das bases do gerenciamento de riscos. A necessidade de que seja estabelecido uma política de segurança é algo recorrente dentro das

corporações, uma vez que o fracasso ou o sucesso em ser estabelecidos procedimentos e normas depende da adesão dos funcionários [29]. Assim, a política de segurança visa conceber e implementar normas e procedimentos que definam a autorização de funcionários conforme o seu setor e o cargo [30].

A política de segurança tem como importância evitar eventos que possam comprometer a estrutura organizacional, com relação a toda informação dos ativos presentes dentro da sua base de dados. Dessa maneira, a política de segurança da informação não tende, somente, tratar dos aspectos tecnológicos da organização, mas também abrange os aspectos humanos e culturais, fato este que permite considerar os processos e os negócios, como também a legislação local vigente. Além da preocupação com as questões relacionadas com a segurança as políticas, já integrando a parte cultural da organização, têm como função gerenciar todos os ativos e recursos corporativos [18].

Efetivar a segurança da informação não pode ser somente através de políticas e procedimentos técnicos realizados no ambiente virtual, mas torna-se primordial estabelecer uma governança de TI capaz de gerir e suprir deficiências que geram algum risco à informação da empresa. Portanto, o ambiente corporativo precisa garantir uma governança que indica normas e procedimentos a serem realizados junto à segurança da informação. Assim, o capítulo 3 apresenta normas e padrões utilizados pelo GAIA-MLIS para guiar a análise das respostas do questionário de avaliação desenvolvido, almejando a efetivação da Governança de TI, voltada à segurança da informação.

3 GOVERNANÇA DE TI

Com as empresas mais dependendes de sistemas computacionais, e a necessidade de contribuir para uma nova etapa de desenvolvimento financeiro, o ambiente corporativo tem a necessidade de apresentar medidas e procedimentos capazes de administrar os seus investimentos. Com muitos ativos para controlar, como pessoas, clientes, dinheiro e as instalações, os diretores possuem a preocupação de como a informação é transmitida, coletada e armazenada. As soluções em tecnologia da informação envolvem investimentos imediatos e contínuos, que buscam resultados, os quais, ninguém pode prever com certeza se alcançará o que foi inicialmente planejado [4]. Assim, o uso difuso da tecnologia tem provocado a necessidade da gestão que consiste em liderança, estruturas e processos organizacionais que permitirão garantir a sustentabilidade das estratégias e objetivos da empresa [31].

Um componente crítico das operações de uma corporação, a tecnologia da informação, e suas capacidades estratégicas junto à organização, têm concentrado esforços aos diretores em estabelecerem e implementarem uma Governança de TI madura. Os investimentos realizados, tanto na governaça corporativa, quanto na de tecnologia da informação resultam em efeitos superiores, como o retorno de lucratividade nas gestões de negócio. Em conformidade com a governança corporativa e a de TI, as seguintes áreas, entrega de valor, gestão de recursos, gestão de riscos e medição de desempenho são concentradas dentro de um alinhamento estratégico, o qual estabelece e indica quais seriam as áreas a serem alinhadas. No caso da TI, as áreas são: a realidade do ambiente de negócio, o portifólio dos projetos e os objetivos de negócios [32].

A governança de TI visa indicar normas e procedimentos, os quais destinam-se a desenvolver práticas para as transmissões de informações estruturadas e inteligíveis sobre o estado de TI e o seu papel dentro do desenvolvimento no sistema empresarial. As responsabilidades na gestão e na elaboração de normas e procedimentos são delegadas aos diretores executivos e do conselho de administração [3].

Para as empresas, a questão de governança de tecnologia da infomação pode ser vista como paradigma na implementação, e também, é um tema polêmico dentro do ambiente corporativo. Alguns modelos que contribuem para a elaboração e desenvolvimento da governança, como o COBIT, são os primeiros passos para a elaboração formal documentada de normas e procedimentos a serem seguidos pela empresa, e como próximo estágio a implementação da abordagem selecionada como uma solução para conduzir a um alinhamento

estratégico de TI [31].

Para o estímulo dos comportamentos desejáveis no uso de TI, a governança representa um quadro de decisão e responsabilidades. Da mesma forma, a governança corporativa é definida como as responsabilidades e práticas exercidas pela diretoria e gerência executiva com o objetivo de desenvolver estratégias e assegurar a obtenção de objetivos de negócios. Em suma, a governança de TI pertence à governança corporativa, que ajuda a controlar informações e ativos de TI dentro da empresa [33].

A Figura 3.1 faz uma associação entre a governança corporativa com a governança de TI.

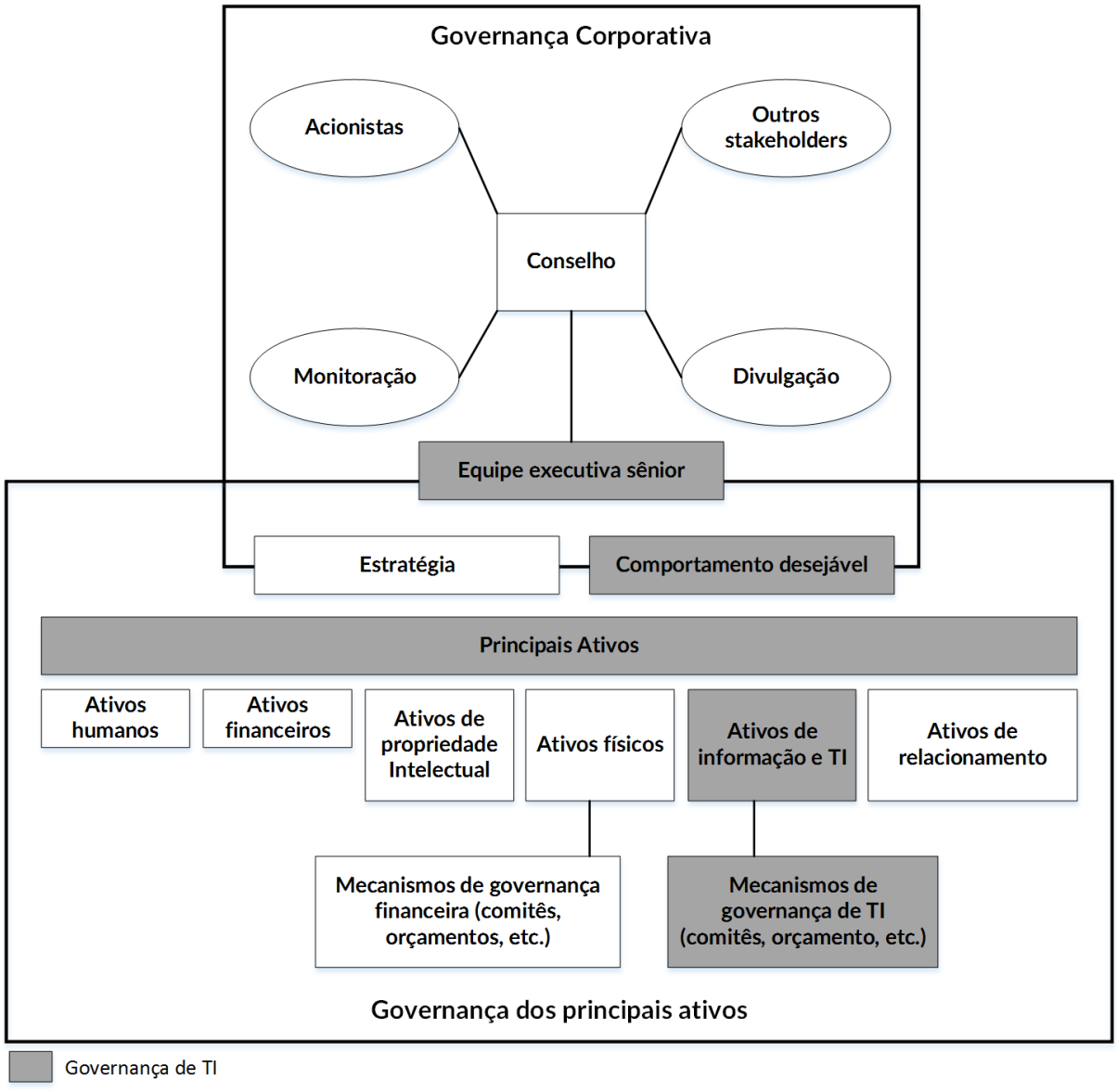

Figura 3.1 – Associação entre governança corporativa e de TI. Fonte [4].

A parte superior da figura representa o relacionamento no conselho administrativo, que são representados pelos acionistas, outros *stakeholders*, ou seja o público estratégico, a monitoração, a divulgação e a equipe executiva sênior. A parte que corresponde à área pintada refere-se diretamente a Governança de TI. Na parte inferior da figura, pode ser visualizado os principais ativos que são: ativos humanos (as pessoas, treinamentos, planos de carreiras, competências, entre outros), ativos financeiros (dinheiro, investimentos, passivo, fluxo de caixa, entre outros), ativos físicos (instalações dos equipamentos de informática, prédios, fábricas, segurança, utilização, entre outros), ativos de propriedade intelectual (serviços e processos devidamente patenteados, produtos, entre outros), ativos de informação e TI (dados informatizados, desempenho de processos, sistema de informação, entre outros; ativos de relacionamentos e de reputação junto a clientes e ao mercado, unidade de negócios, órgãos reguladores etc) [4].

Com base na Figura 3.1, a importância da TI e o valor gerado dentro do ambiente corporativo e de governança propiciam em retorno de lucratividade, além de conceber maior integração. A cinergia que envolve os ativos promove um maior enlace para a cooperação entre diferentes setores, convergindo para a elaboração do planejamento estratégico empresarial.

Dessa forma, identificar mecanismos para a implantação da Governança de TI que contribuem para que haja um maior auxílio para os diretores verificarem quais são os seus objetivos e metas que devem conceber para que se obtenha uma implementação efetiva da governança de tecnologia da informação.

3.1 COMO EFETIVAR A GOVERNANÇA DE TI

A efetivação da Governança de TI só é capaz com a contribuição de mecanismos aptos para gerarem valor, com o objetivo de promoverem comportamentos que sejam desejáveis para a tecnologia da informação, como decisões administrativas, que podem ser transformadas em investimentos na área de tecnologia. Como consequência deste empreendimento, o arranjo de conjunto de mecanismos como, estruturas, processos e comunicação auxiliam na elaboração efetiva da governança, porém a implementação realizada de forma errada não produzirá os resultados desejados. A dependência de TI, também por causa da necessidade de transparência dos riscos organizacionais e dos *stakeholders*, e as práticas tradicionais de gestão, já não podem ser suficientes para uma gestão eficiente. Para que seja estabelecida uma gestão eficaz torna-se primordial a utilização de processos de governança

como forma de gerar valor a um custo acessível com um nível aceitável de risco [32].

As empresas de sucesso reconhecem que a tecnologia da informação é um apoio importante no sucesso econômico e um cooperador estratégico. É essencial para gerenciar as transações, informações e conhecimentos necessários para iniciar, manter, apoiar e desenvolver atividades econômicas e de negócios. A necessidade de transparência dos riscos corporativos e a proteção das partes interessadas são evidenciadas pela implementação do incentivo, para que a gestão possa recorrer a processos de governança de TI.

Efetivar a governança de TI garante tomadas de decisões dentro do departamento de TI, as quais segundo Weill e Ross [4], são divididas em cinco inter-relacionamentos sobre a tecnologia da informação: princípios de TI, a arquitetura de TI, a infra-estrutura de TI, as necessidades de aplicações do negócio e, os investimentos e a priorização de TI.

A Figura 3.2 refere-se aos tipos de decisões que são destinadas aos princípios de TI.

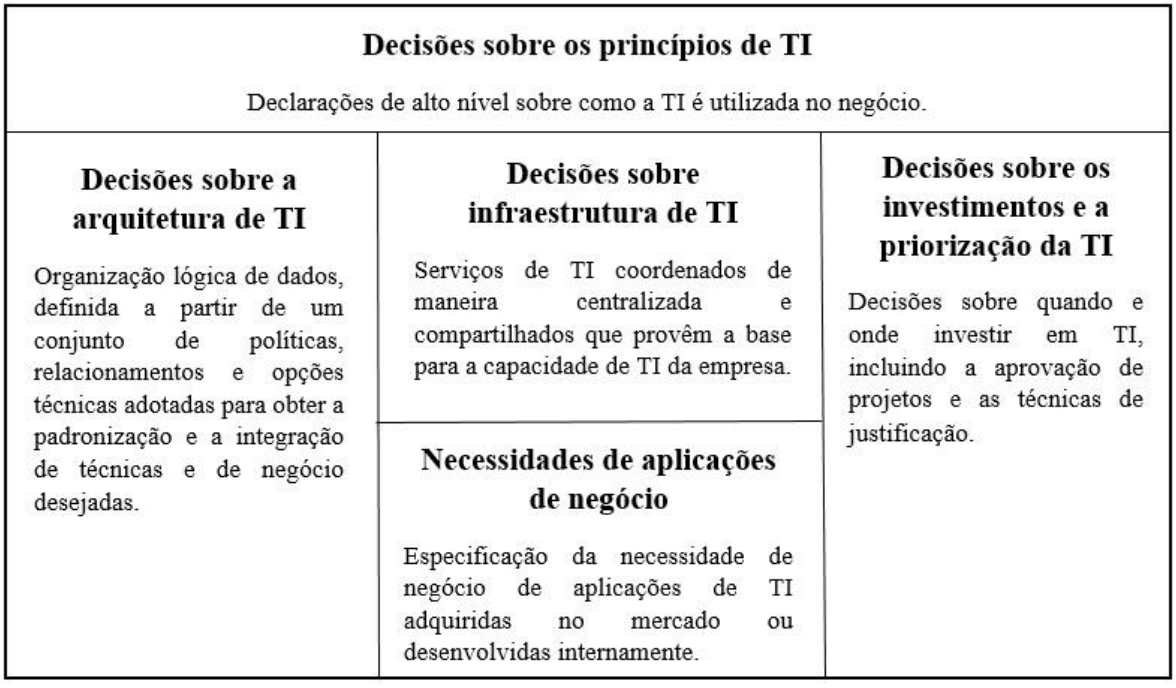

Figura 3.2 – Decisões sobre os princípios de TI. Fonte [4].

Como verificado, na parte superior da figura encontram-se as decisões sobre os princípios de TI, que são conjuntos de resoluções e comportamentos desejáveis para que a orgnização, por meio do setor de tecnologia da infomação, planejem e atijam metas de negócios que inicialmente foram apresentadas. As decisões sobre a arquitetura de TI visam a padronização por meio de políticas, relacionamento e técnicas, a organização lógica de dados e

aplicações e infra-estruturas. Decisões sobre infra-estrutura de TI caracterizam-se pela centralização e compartilhamento dos serviços de TI que são responsáveis pela base para a capacidade tecnológica da organização. Necessidades de aplicações de negócio são os alicerces da TI desenvolvida dentro da própria empresa ou utilizada junto ao mercado através de parceiros. Decisões sobre os investimentos e a priorização da TI correspondem às decisões de quanto deve ser investido em TI, incluindo a justificativa de técnicas utilizadas, o quanto deve ser gasto no projeto a ser desenvolvido, como deve ser realizada a execução do projeto e o que o mesmo propiciará de benefícios à empresa na forma de lucratividade no negócio.

Para tanto, efetivar a governança de TI, com todos esses conjuntos de tomadas de decisões, pode facilitar o ambiente corporativo, visando a uma melhor qualificação empresarial perante o mercado. Assim, o departamento de tecnologia da informação é altamente estratégico junto ao planejamento empresarial, já que a TI é um setor que se bem utilizado, gera valor e competitividade dentro da empresa.

3.2 TI: VALOR E COMPETIVIDADE

O setor de tecnologia da informação nem sempre é contemplado como um departamento que gera lucratividade e retorno de investimento. Há muita descrença junto à TI, por ser mencionada como um setor que gera alto custo e que não há a necessidade de capital massivos. Isso ocorre, pelo fato, das aplicações serem destinadas a outros setores, como o de vendas, produção, etc. Porém, há muitos diretores de TI que acreditam que o valor gerado pelo departamento de tecnologia da informação deva vir da área administrativa, enquanto esse valor deve ser almejado pela própria TI [34].

Pode ser afirmado que crenças e hábitos aparentemente bons são capazes de propiciar armadilhas de valor, ocasionando problemas dentro da organização. Essas armadilhas obrigam que haja o direcionamento de conversas que não são convenientes para o departamento de tecnologia da informação ou que reduzem ainda mais o seu valor, concebendo barreiras entre o setor de TI e os demais departamentos da empresa. Muitas desses percalços são ocasionados, porque as empresas adotam as mesmas decisões de forma repetitiva esperando resultados diferentes, porém esse comportamento não garante soluções diferentes a não ser um desgaste na já ferida imagem da TI [35].

3.3 COBIT *framework* para Governança de TI

Vivemos em um mundo cada vez mais conectado às redes de informação, sejam elas, a Internet, as emissoras de TVs, ou as redes de dados móveis. Mais do que nunca, a tecnologia ajuda a diminuir distâncias geográficas e o acesso aos acontecimentos tornam-se mais rápidos e difusos. A tecnologia, na sociedade atual, realiza um papel significativo em relação a criação e a destruição da informação. Para as organizações, tal recurso contribui para a realização de novos serviços, processos de negócios e conquistas de novos mercados, bem como a submissão ou alteração de dados podem proporcionar às organizações percas de acordos comerciais e credibilidade. Como consequência, as empresas devem obter esforços para que a informação seja, mantida, agregue valor ao negócio a partir dos investimentos de TI, alcance excelência operacional, mantenha o nível de risco em TI em um nível aceitável, otimize custos dos serviços utilizados e da tecnologia empregada e cumpra a legislação, como, leis, acordos comerciais, políticas, dentre outros [36].

Empresas bem-conceituadas visam a comunicação entre os demais setores e o departamento de TI como forma estratégica dentro da organização, para a realização do planejamento estratégico, viabilizam trabalhos em conjunto entre os vários diretores da organização com a finalidade de garantir que a TI esteja incluída na governança e gestão empresarial. Isto decorre pelo fato de novas normas e leis serem aprovadas para atenderem a essa necessidade [37].

Destaca-se que para a organização aprovar uma gestão eficiente e capaz de lidar com vários desafios, uma ferramenta de Governança de TI deve ser utilizada para realizar a elaboração de normas e padrões, além de definir responsabilidades. Esta ferramenta é o COBIT[1].

O COBIT 5 proporciona auxílio às empresas para a criação de valor através da TI, conservando o equilíbrio entre os benefícios realizados e o aprimoramento dos níveis de riscos e da utilização de recursos. Este *framework* fornece uma abordagem ampla, que proporciona as organizações atingirem seus objetivos de gestão e governança de TI. O COBIT 5 estabelece que a TI seja governada e gerida para toda a organização, abrangendo o planejamento estratégico como um todo, levando em consideração os interesses externos e internos relacionados à TI. Assim, o COBIT 5 é universal e útil em organizações públicas ou privadas e de qualquer porte ou seguimento de negócio [38].

[1] Modelo corporativo para a Governança e Gestão de TI. Adaptado [38].

O *framework* do COBIT estabelece controles básicos, cumpre os seus objetivos, alinhando-os aos objetos de negócios, porém não define os processos que serão executados. O COBIT consiste em objetivos de negócios ligados a objetivos de TI, o qual identifica as responsabilidades e aos processos de negócios e de TI, indicando abordagens de maturidade e métricas para medir a eficiência desses processos [4].

A Figura 3.3, demonstra os princípios do COBIT 5.

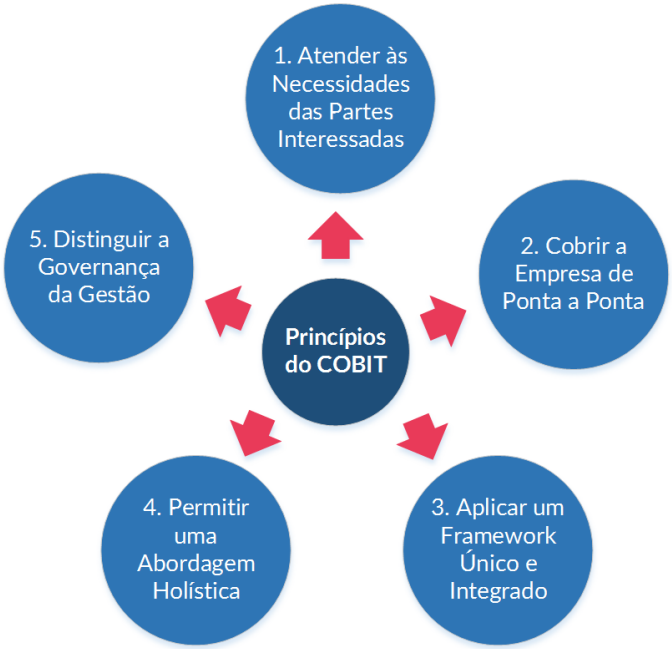

Figura 3.3 - Princípios do COBIT 5. Fonte [38].

Como mencionado o COBIT 5 possui cinco princípios que regem a documentação para que a governança de TI seja efetivada. Esses princípios são: atender às necessidades das partes interessadas; cobrir a empresa de ponta a ponta; aplicar um *framework* único e integrado; permitir uma abordagem holística e distinguir a governança da gestão. Através do inter-relacionamento entre esses princípios os diretores das empresas podem reunir em uma documentação todas as regras que regem a governança de TI, disponibilizando normas de conduta, distribuindo responsabilidades, bem como, verificar a governança com a conformidade do planejamento estratégico da organização.

O COBIT é um *framework* capaz de auxiliar, também, na formalização de uma governança de TI voltada para a segurança da informação, porém esta ferramenta sozinha não é capaz de gerar uma documentação formalizada nesse sentido. Destacamos que outros

documentos são capazes de auxiliarem na elaboração formal de uma regulação capaz de gerir a segurança da informação.

Para a abordagem GAIA-MLIS, o COBIT apoia a criação de ações junto ao planejamento estratégico da empresa, as quais são usadas nas cinco áreas analisadas com a finalidade de melhorar a segurança da informação.

3.4 Documento de Segurança Center for Internet Security (CIS)

Podemos dizer que estamos em um ponto crucial para a evolução da defesa cibernética. Mas, a grande preocupação com perdas de dados, violação de cartão de crédito, propriedade intelectual submetida por *crackers*, roubo de identidades, as ameaças a nossa privacidade, ataques de negação de serviço tornaram-se um modo de problema na nossa vida na Internet. Alguns documentos são desenvolvidos para auxiliarem na segurança da informação, como as normas ISO 27000 e o *Center for Internet Security* (CIS).

O CIS, uma organização sem fins lucrativos, desenvolve uma documentação capaz de cooperar com os diretores das organizações, visando uma melhor contribuição para a segurança cibernética para o setor público e privado [39].

Os controles de segurança do CIS são informados em tempo real, sobre os ataques que estão acontecendo em todo o mundo e os conhecimentos adquiridos referentes a estes ataques são analisados e estudados como forma de material de apoio para as organizações. Todo o aparato técnico é utilizado para reconhecer e reportar as ameaças de segurança é fornecido por empresas, governos e indivíduos que atuam diretamente para garantir uma melhor eficiência na segurança da informação. Dessa maneira, os controles são garantidos como um conjunto eficaz e específico de medidas técnicas disponíveis para detectar, prevenir, responder e mitigar os danos dos ataques mais comum, bem como dos mais avançados.

Para o CIS, os cinco princípios críticos de um sistema de defesa cibernética são: proteção contra crimes de violação, priorização, métricas, diagnósticos, mitigação contínuas e automação. Estes controles não estão limitados a bloquear um possível ataque, mas eles também são capazes de detectar qualquer ato criminoso, com o objetivo de impedir ou interromper qualquer ato de criminosos cibernéticos durante a ação [39].

Estes controles do CIS ajudam na confecção de uma documentação formal capaz de contribuir no contínuo controle da segurança da informação das empresas, além de

proporcionar métricas para mensurar se o planejamento de risco está atendendo o planejamento estratégico, e disponibiliza como forma de contribuição os ensinamentos nele proporcionados, para uma governança eficaz da TI. Por consequência, elaborar uma governança de TI voltada para a segurança da informação torna-se mais eficaz com a junção desse documento.

3.5 Normas ISO 27001 e 27002

As informações, os sistemas, processos que apoiam a organização e até mesmo as redes de computadores são importantes ativos para o negócio da organização. Com o objetivo de alcançar uma maior competitividade e visibilidade junto ao mercado, as empresas proporcionam atividades tais como, definir, alcançar, manter e melhorar a segurança da informação, e elas devem ser revistas a cada período de tempo no âmbito de averiguar se o planejamento inicial está de acordo com a execução estabelecida primariamente e se atende a realidade da organização [40].

É fato que as organizações passam frequentemente por diversos tipos de ameaças aos seus sistemas e redes de computadores, as quais podem-se incluir, espionagem, pessoas mal-intencionadas dentro da empresa, fraudes eletrônicas, entre outros. A segurança da informação é importante para qualquer organização, seja ela, órgão público, com o modelo de governo eletrônico (e-gov), ou privado, como no caso do e-commerce prevenir ataques a sua integridade física e cibernética. É fato que, com a computação distribuída, um controle centralizado torna-se mais difícil de implementar, na medida que as interconexões de redes públicas com redes privadas compartilham recursos de informação [5].

Muitos sistemas não foram projetados visando a segurança. Algumas organizações não têm processos e procedimentos apropriados. É essencial que os requisitos de segurança da informação sejam identificados. As normas ISO/IEC 27001:2006 e 27002:2005 têm como objetivo ajudar os gerentes de TI e aos demais gerentes, a estabelecerem quais são os requisitos de segurança da informação que devem ser adotados, conforme a necessidade da organização. As normas servem como guia prático para desenvolverem as práticas e procedimentos de segurança da informação e auxiliarem na criação de confiança focando atividades inter organizacionais.

As normas ISO são utilizadas para a elaboração de ações que devem ser tomadas com base no nível de maturidade do GAIA-MLIS.

3.5.1 Norma ISO 27001:2006

A norma ISO/IEC 27001 tem como objetivo, designar a tecnologia, processos e pessoas para ajudarem as organizações a resguardar os seus dados e ativos físicos, utilizando um Sistema de Gestão de Segurança da Informação (SGSI), com o objetivo de monitorar, analisar, implementar, operar, estabelecendo, mantendo e melhorando seus serviços. Tais procedimentos são adotados visando uma melhor tomada das estratégias relacionadas às decisões da organização, sendo que alguns procedimentos devem ser levados em consideração como o tamanho das empresas, a segurança, os processos empregados e a estrutura, bem como a seleção de controles de segurança adequados para protegerem os ativos de informação e proporcionarem confiança as partes interessadas [41].

O Modelo adotado pela norma é conhecido por PDCA (*Plan-Do-Check-Act*), ou seja, planejar, fazer, checar e agir. Na fase do planejamento devem ser adotados os processos, as políticas, os objetivos e os procedimentos. Na fase "fazer", operar a política, o controle, os processos e os procedimentos. Na fase checar, monitorar e analisar o SGSI. Na fase agir, melhorar e manter o SGSI [42].

A norma discute e analisa exemplos de riscos que podem prejudicar o gerenciamento da organização. Esses riscos devem ser identificados e após uma análise é avaliado quais são os impactos que a organização pode sofrer com relação a segurança da informação no âmbito da confidencialidade, disponibilidade e integridade.

Todos os documentos requeridos pelo SGSI devem ser protegidos e controlados. Qualquer procedimento documentado deve aprovar documentos, analisar e atualizar, muitas vezes, reprovar, assegurar que todas as alterações sejam identificadas e qual é a situação atual do documento, entre outros. Segundo a norma, os registros devem ser estabelecidos e mantidos para fornecer evidências de conformidade aos requisitos e da operação eficaz do SGSI [42].

A organização deve sempre realizar auditorias em intervalos de tempo pré-determinados a fim de, verificar se os objetivos de controles, processos e procedimentos do SGSI atendam as recomendações da norma, os requisitos de segurança da informação identificados, se todos os objetivos estão mantidos e implementados eficazmente e se estão sendo executados conforme o esperado. A organização deve sempre melhorar o SGSI, aplicar ações corretivas e preventivas [43].

Portanto, a norma visa ajudar os Gerentes de TI a elaborarem um Modelo de Gestão de Segurança da Informação, a qual sugere uma melhoria contínua no processo. Com o planejamento estratégico e a utilização do PDCA, os Gerentes de TI irão analisar e verificar os dados estatísticos para a determinar a eficiência do processo empregado na organização [40].

3.5.2 Norma ISO 27002:2005

A norma ISO/IEC 27002:2005 tem como objetivo estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação dentro da organização. Os objetivos previstos na norma referem-se a diretrizes gerais correspondentes às metas que, em sua grande maioria, são aceitas para gestão da segurança da informação [44].

A norma está estruturada em onze seções, as quais tratam sobre a segurança da informação, trinta e nove categorias principais e uma seção introdutória que aborda o tratamento de riscos com base na análise e avaliação. As ordens das seções não indicam prioridade, ou seja, cada organização determina o que é mais importante conforme a sua realidade [45].

As seções da norma são divididas em: 1) Política de segurança da informação; 2) Organizando a segurança da informação; 3) Gestão de ativos; 4) Segurança em recursos humanos; 5) Segurança física e do ambiente; 6) Gestão das operações e comunicações; 7) Controle de acesso; 8) Aquisição, desenvolvimento e manutenção dos sistemas de informação; 9) Gestão de incidentes de segurança da informação; 10) Gestão da continuidade do negócio; 11) Conformidade [46].

Como a norma ISO/IEC 27001:2006, a norma ISSO/IEC 27002:2005 discute e analisa situações de riscos de segurança da informação. Com base em resultados extraídos das análises, os diretores de TI e os demais diretores da organização podem determinar as ações e quais riscos serão aceitos com base na estratégia de negócio da empresa. Vale salientar que os riscos podem ser analisados como em toda organização, parte da mesma, sistemas utilizados, clientes, entre outros [5] [47].

Com relação as normas ISO 27000 foram obtidos os modelos de ações para as políticas, como por exemplo, aquisição de *hardware*, atualização de *software*, treinamento de pessoas, entre outros. Do COBIT foram usados os conceitos da Figura 4.3, que correspondem aos princípios desse *framework* para a análise das cinco áreas por meio do questionário de

avaliação. Também, esses princípios são utilizados para a realização de medidas e ações para obter uma visão holística da situação da segurança da empresa, aplicando uma abordagem única e integrada. A Tabela 3.1 detalha os princípios de segurança das normas ISO 27000 e do COBIT 5 usados para a criação do GAIA-MLIS.

Tabela 3.1 – Princípios do GAIA-MLIS retirados das boas práticas de segurança.

COBIT 5	Norma ISO 27001	Norma ISO 27002
Atender às Necessidades das Partes Interessadas	Estabelecer um Sistema de Gestão de Segurança da Informação	Política de Segurança da Informação
Cobrir a Empresa de Ponta a Ponta	Implementar e Operar o Sistema de Gestão de Segurança da Informação	Organização da Segurança da Informação
Aplicar uma Abordagem Único e Integrado	Monitorar o Sistema de Gestão de Segurança da Informação	Gestão de Ativos
Permitir uma Abordagem Holística	Manter e Melhorar o Sistema de Gestão de Segurança da Informação	Segurança em Recursos Humanos
		Segurança Física e do Ambiente
		Gestão das Operações e Comunicações
		Controle de Acesso
		Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação
		Gestão de Incidentes de Segurança da Informação
		Gestão da Continuidade do Negócio
		Conformidade

Os detalhes sobre o desenvolvimento da GAIA-MLIS, bem como das áreas analisadas são abordados no capítulo 4. Além disso, são discutidas as características que permitem a classificação dos níveis de maturidade de cada uma das áreas.

4 GAIA-MLIS

A abordagem GAIA-MLIS para a Segurança da Informação faz parte de um conjunto de *frameworks* desenvolvido no laboratório GAIA, do Departamento de Computação da Universidade Estadual de Londrina (UEL). O objetivo da GAIA é propor novas soluções para o apoio e a realização de projetos de TI. Diversos tipos de modelos, abordagens e soluções nas áreas de Engenharia de *Software*, Gerenciamento de Serviços de TI e Governança de TI são desenvolvidos em tal laboratório.

A GAIA-MLIS é uma abordagem de Governança de TI voltada para a Segurança da Informação, o que o difere dos demais *frameworks* criados pela equipe de pesquisa do laboratório GAIA. Dentre os vários trabalhos realizados pela equipe GAIA no âmbito de *frameworks*, as principais referências são:

- Um *framework* para desenvolvimento de governança de TIC: Proposto por Briganó [7] com o objetivo de oferecer diretrizes para o seu desenvolvimento;
- GAIA Catálogo de Serviços de TI: Um *framework* para Construção de Catálogos de Serviços de Tecnologia da Informação proposto por Taconi [8]. Compreende todo o processo de desenvolvimento de um Catálogo de Serviços;
- GAIA Lições Aprendidas: *framework* proposto por Góes [9]. Tem como objetivo aplicar práticas de lições aprendidas dentro do processo de desenvolvimento de *software*, gerando conhecimento dentro da empresa por meio da melhoria na qualidade do *software*;
- GAIA Riscos: Esse *framework* foi proposto por Gaffo [10] para o gerenciamento de riscos no processo de desenvolvimento de *software*. O objetivo é facilitar a tomada de decisões para aderir aos padrões de gerenciamento de riscos no processo de desenvolvimento de *software*, permitindo a implantação da gerência, afim de melhorar a qualidade do *software* gerado.

Na página www.gaia3.uel.br, encontram-se os demais *frameworks* da família GAIA que auxiliam na solução de diversos outros desafios, como recursos humanos, riscos, requisitos, etc.

4.1 Abordagem GAIA-MLIS

A abordagem GAIA-MLIS realiza análise diagnóstica em cinco áreas: *hardware*, *software*, instalações, pessoas e informação com o objetivo de verificar ações relacionadas à segurança. A escolha dessas áreas deve-se ao inter-relacionamento entre as mesmas e o fato de elas representarem a essência dos serviços de TIC atualmente. A partir dessas áreas é definido um conjunto de objetos de estudo capaz de verificar pontos fortes e fracos nos processos de segurança.

O inter-relacionamento entre as áreas utilizadas na abordagem GAIA-MLIS. A utilização de *hardware* está relacionada ao uso de *software* e aos colaboradores, da mesma forma que as instalações seguras contribuem para que o acesso aos equipamentos de informática fique restritos às pessoas autorizadas. *Software* está relacionado a processos e sistemas de informação, e estes são utilizados pelas pessoas/funcionários. As instalações estão associadas ao controle de acesso dos colaboradores e demais pessoas dentro do espaço físico da empresa, da mesma maneira, relaciona-se diretamente à toda informação. A área de pessoas está alusiva a utilização dos espaços físicos empresariais, bem como a utilização dos sistemas de informação e os equipamentos de informática, o que acarreta na acessibilidade da informação.

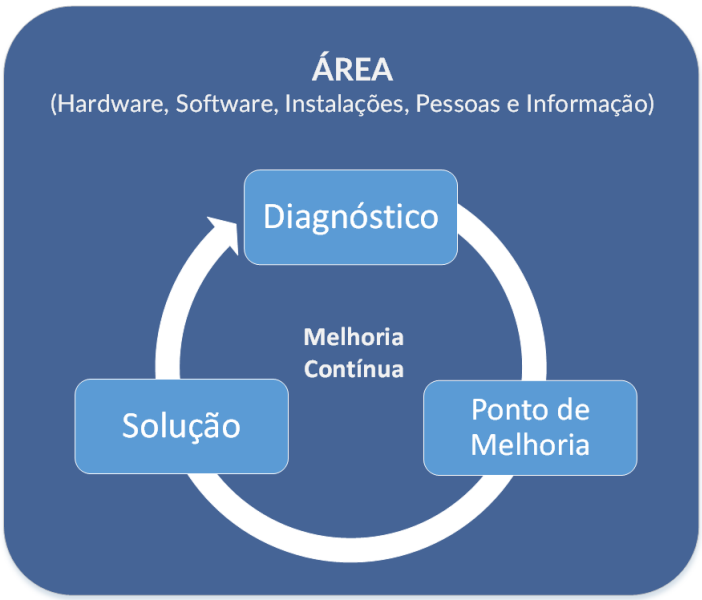

Figura 4.1 – Processo de análise do nível de maturidade em segurança da informação realizado pelo GAIA-MLIS.

Conforme apresentado na Figura 4.1, o nível de maturidade em segurança da informação é identificado por meio da análise diagnóstica das áreas verificadas. Os pontos de melhoria, sejam eles problemas ou processos a serem reexaminados, levam às soluções que serão aplicadas em conformidade com o planejamento estratégico. Desse modo, as ações e metas indicadas pelo GAIA-MLIS contribuem para uma gestão de segurança eficiente e delineada, almejando a melhoria contínua.

4.2 ÁREAS DO GAIA-MLIS

Foram escolhidas cinco áreas que melhor representam a realidade de serviços de TIC dentro de um ambiente corporativo a fim de verificar o nível de maturidade em segurança da informação da empresa. Através dessas áreas as empresas podem identificar os pontos fortes e os pontos fracos dentro do processo de segurança e governança de TI e, com esses resultados demonstrarem qual é o menor nível dentre as áreas, o que também caracteriza o nível de segurança da informação geral da empresa.

4.2.1 Área de *Software*

Esta área é a responsável pelos sistemas de informação utilizados nas empresas. Os *software*s são criados ou adquiridos com a finalidade de cooperar junto ao planejamento estratégico da organização. Inúmeros eventos de segurança da informação podem ocorrer devido a falhas (erros não intencionais no código fonte), falta de atualização, falta de treinamento dos funcionários, não formalização de processos e na má utilização dos *software*s por parte dos usuários. A Figura 4.2 exemplifica os parâmetros avaliados da área de *software*, que por meio do questionário, tem suas falhas e pontos de melhoria indicados.

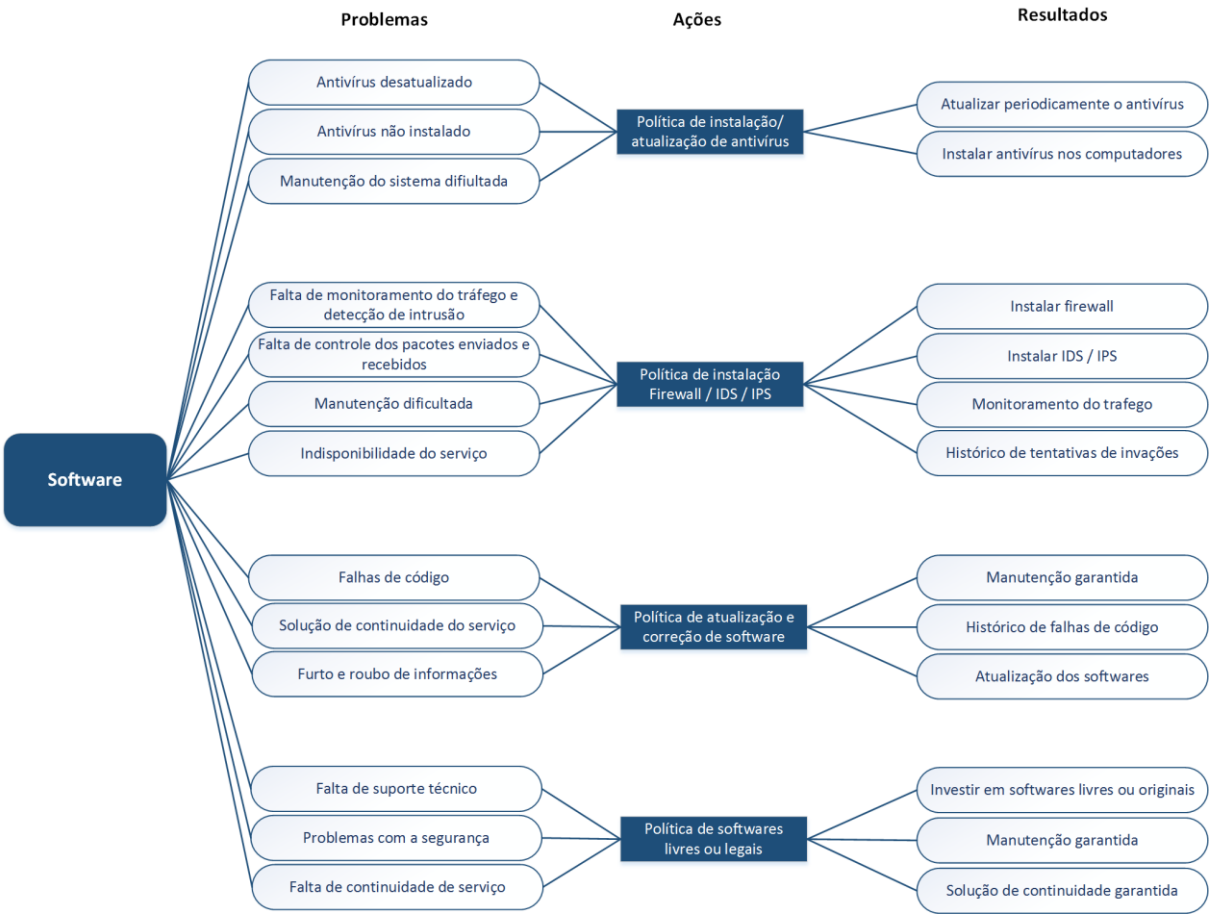

Figura 4.2– Processo de análise diagnóstica da área de *software*.

Um ambiente virtual seguro caracteriza-se pela utilização de processos capazes de evitar violação da segurança, como o uso de *firewall*, programas para detecção de intrusão (IDS), sistemas para prevenção de intrusão (IPS), e uma eficiência na gerência de redes. Os *software*s ajudam as corporações nos seus planos de negócio, proporcionando agilidade na comunicação de dados e em pesquisa e desenvolvimento de novos produtos. Vale salientar que, sem a devida manutenção técnica e atualizações periódicas dos *software*s, os dados e arquivos da empresa poderão ser comprometidos por falhas de segurança presentes nos códigos.

O uso de *software*, adquiridos com licenças pagas, legais ou livres possibilita suporte e atualizações capazes de corrigirem falhas de código, as quais podem ocasionar eventos de segurança da informação. Da mesma forma, a documentação de falhas ajuda na melhoria do suporte, e o *feedback* entre os usuários e a equipe técnica permite que pontos de melhoria nos processos de produção de *software*s sejam analisados e implementados.

4.2.2 Área de *Hardware*

A área de *hardware* é responsável pelos equipamentos de informática, como computadores, servidores e equipamentos presentes na rede de informação. As trocas de equipamentos de informática devem ser realizadas periodicamente. As tecnologias de *hardware* são comumente atualizadas conforme a necessidade operacional de instalação de um novo *software* e de novos processos informatizados. Equipamentos obsoletos podem impedir atualizações de sistemas operacionais e outros *software*s utilizados. A Figura 4.3 exemplifica a análise diagnóstica da área de *hardware* empregada pela abordagem GAIA-MLIS.

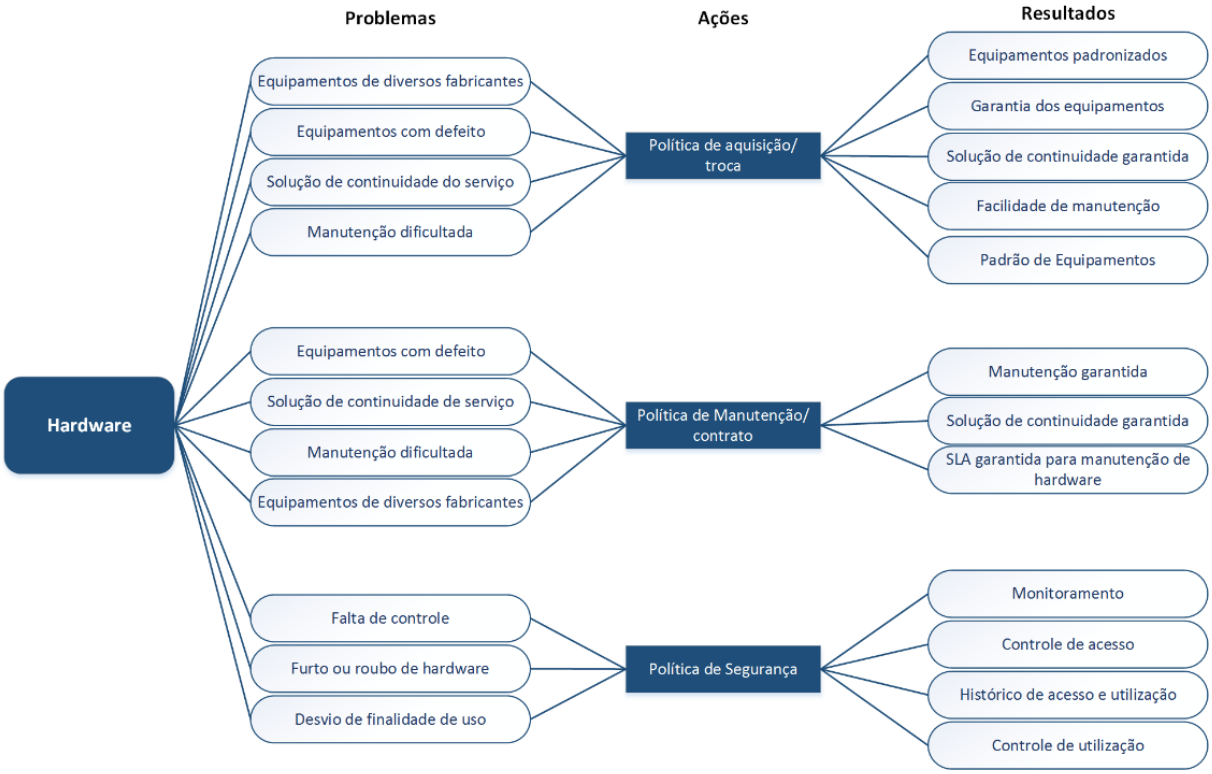

Figura 4.3 – Processo de análise diagnóstica área de *hardware*.

Vale salientar que contratos de manutenção de *hardware* diminuem custos relacionados à manutenção com os próprios funcionários e equipamentos. As vantagens do contrato de manutenção são: atendimento personalizado e seguro; orientação e suporte técnico; consultoria especializada. Outra vantagem é a padronização de *hardware*, permitindo à organização um gerenciamento de segurança eficaz, na qual configurações específicas são utilizadas para melhor desempenho do *hardware*.

As políticas de segurança para *hardware* permitem que os equipamentos de informática sejam mantidos, identificados e monitorados dentro do ambiente físico empresarial.

Por meio dessa documentação, é definida quais as responsabilidades dos funcionários e departamentos caso algum evento de segurança da informação contra *hardware* ocorra.

4.2.3 Área de Instalações

As instalações físicas seguras são importantes para a segurança da informação, visto que sem o monitoramento e o controle de acesso, pessoas não autorizadas podem invadir o ambiente e adquirir dados diretamente dos equipamentos de informática e dos sistemas de informação. Também, podemos indicar que com a falta de vigilância, equipamentos podem ser furtados e essa negligência compromete a credibilidade da empresa perante o mercado. A Figura 4.4 exemplifica a análise diagnóstica da área de instalações/espaços físicos.

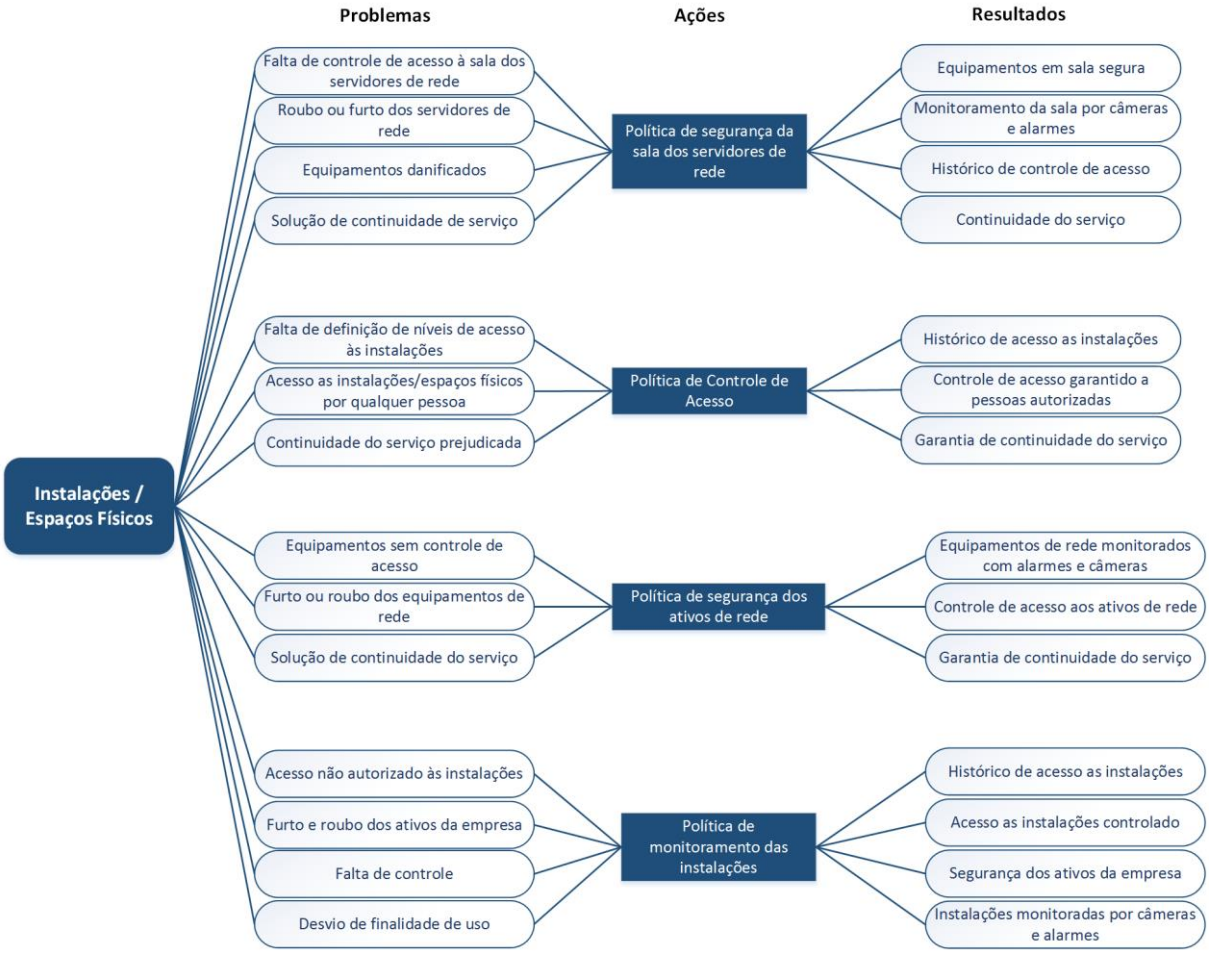

Figura 4.4 – Processo de análise diagnóstica área de instalações.

Um ambiente físico seguro caracteriza-se por processos capazes de evitar a violação da segurança, como o monitoramento por câmeras, instalação de alarmes, e um controle de acesso rígido de pessoas nos espaços físicos empresariais, bem como o

monitoramento dos ativos de rede da organização. Esse tipo de monitoramento proporciona maior segurança, podendo evitar furtos dos equipamentos de informática ou o acesso direto ao *hardware* por pessoas não autorizadas.

Política de acesso de pessoal deve ser documentada com o objetivo de garantir registros de presenças e atividades desempenhadas pelos usuários, assegurando um melhor controle da segurança dos ambientes e dos equipamentos.

4.2.4 Área de Pessoas

Esta área é a que transmite preocupação para os diretores das empreasas. Funcionários descontentes ou com a falta de comprometimento com a organização podem ocasionar vários tipos de eventos de segurança, desde os envolvidos em corrupção, ocasionando venda de informações sigilosas da organização, bem como, a destruição de dados de clientes, entre outros. A Figura 4.5 ilustra a análise diagnóstica da área de pessoas.

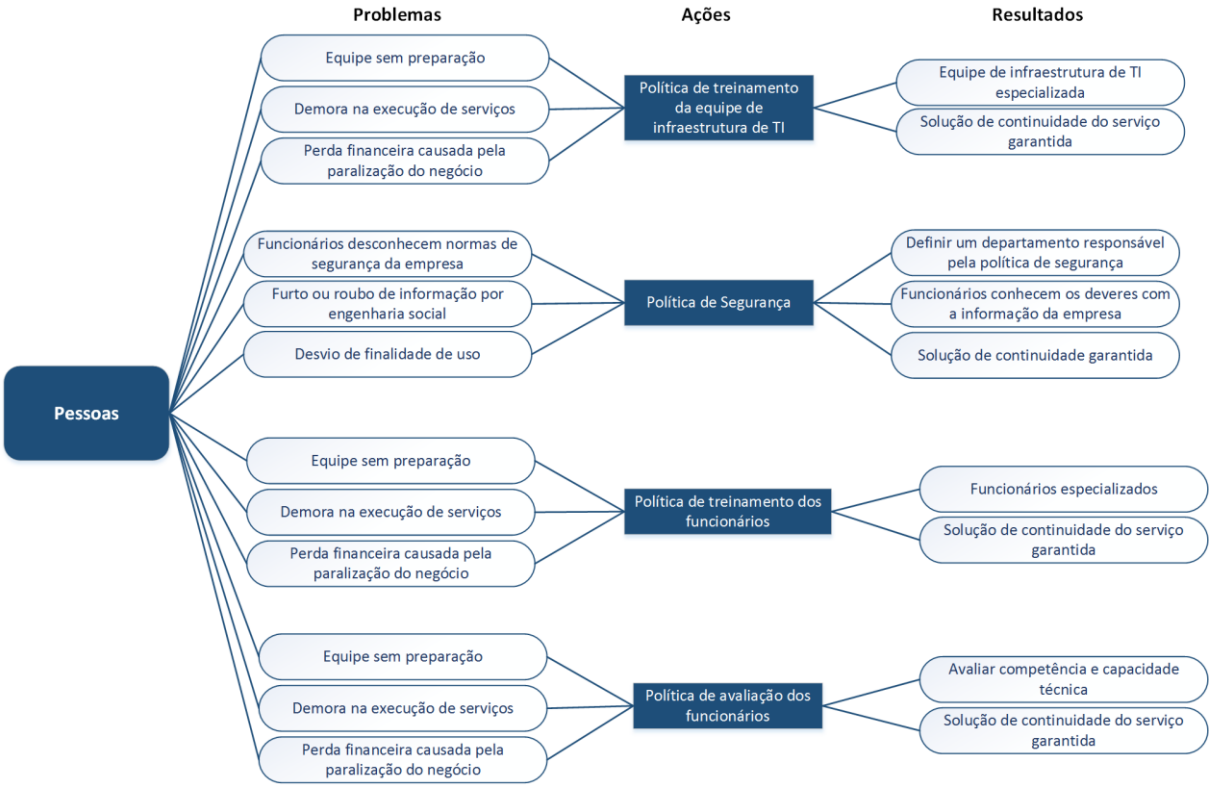

Figura 4.5 – Processo de análise diagnóstica área de pessoas.

Um detalhe importante é a utilização da engenharia social. As organizações criminosas utilizam de meios para persuadirem as pessoas com a finalidade de obterem acesso a dados da organização alvo. Muitas vezes, as pessoas que passam pelo processo de engenharia

social, somente se dão conta quando o evento de apropriação indevida das informações já foi realizado.

A falta de políticas voltadas para treinamentos contínuos podem causar problemas de segurança, visto que, novos métodos de ataques e novas tecnologias são usadas para o roubo da informação. Portanto, as empresas devem promover periodicamente a capacitação técnica dos funcionários, além de investir em incentivos, sejam eles, financeiros ou em projetos como forma de participação dos seus empregados em treinamentos.

4.2.5 Área da Informação

Um ou mais bancos de dados podem ser utilizados para armazenar as informações da organização, desde que as premissas de disponibilidade e integridade sejam satisfeitas. Porém, ainda existem empresas que não possuem um grau elevado em tecnologia e políticas de GED (Gerenciamento Eletrônico de Documentos) bem definidas, resultando no armazenamento dos arquivos em papéis.

A informação, muitas vezes, deve possuir algum mecanismo de proteção como a criptografia e rotinas de *backup*. A utilização desses padrões dificultam e evitam a violação de dados pelos *crackers*, e garante que a informação seja transmitida e recebida de forma confiável e íntegra. Porém, a utilização de técnicas de criptografia desatualizadas podem desencadear eventos de segurança da informação, os quais podem levar ao vazamento, roubo e alteração de dados.

Dessa maneira, proteger a informação é uma necessidade de qualquer empresa, independente do porte, bem como, a verificação de se as técnicas utilizadas estão atendendo ao planejamento de riscos e colaborando com a proteção para o planejamento estratégico empresarial. A Figura 4.6 apresenta a análise diagnóstica da área de informação, que por meio do questionário, tem suas falhas e pontos de melhoria indicados.

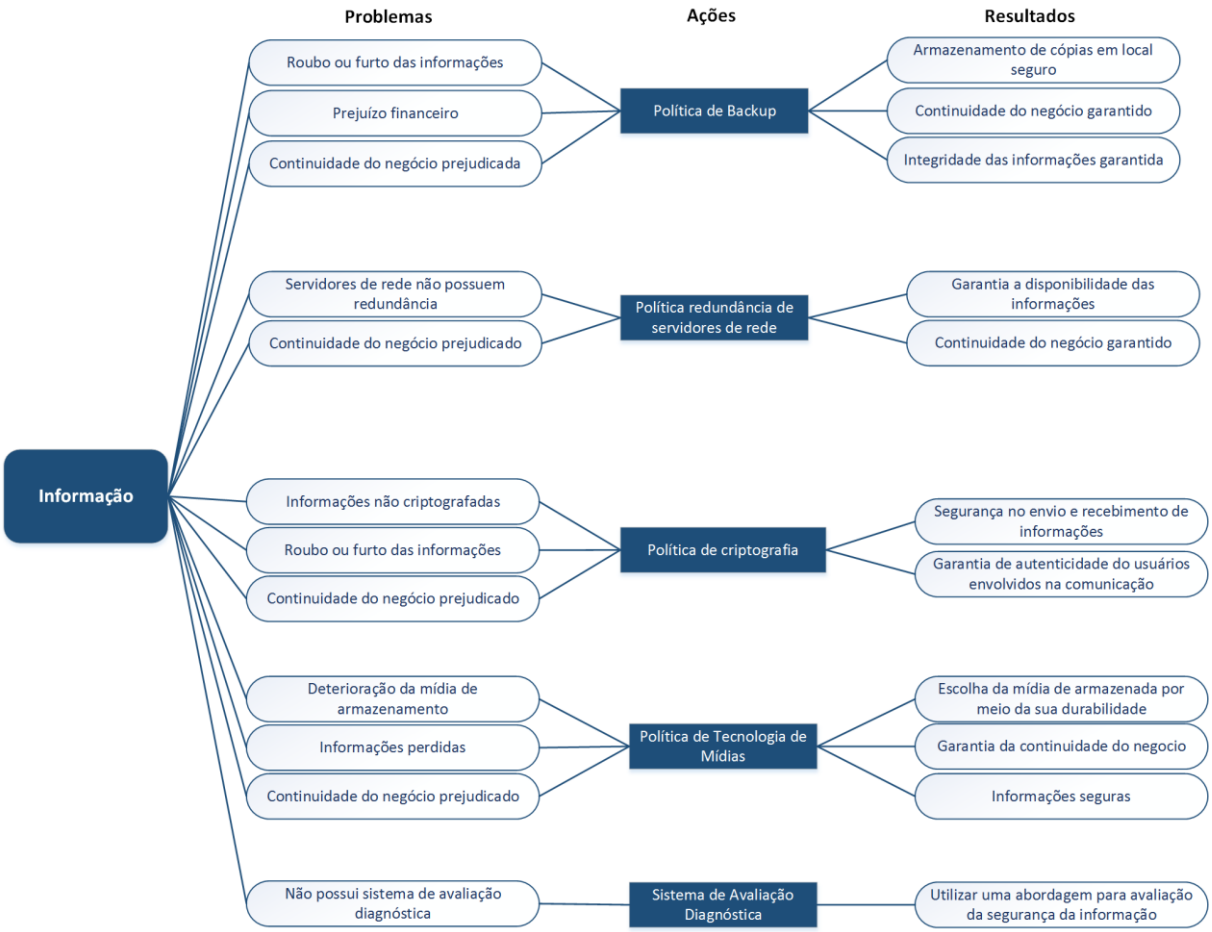

Figura 4.6 – Processo de análise diagnóstica área de informação.

Políticas de *backup* devem ser usadas para garantir a proteção da informação por meio de cópias disponibilizadas caso algum dado seja adulterado ou perdido. As cópias de segurança carecem de lugares protegidos, sendo que boas práticas indicam que elas não devem ser mantidas nos mesmos ambientes ao qual foram coletadas. Como forma de garantia ao acesso à informação por um período mínimo, o tempo que o *backup* precisa estar disponível deve ser definido por meio de políticas, e essa deve estar de acordo com a vida útil da mídia utilizada para o armazenamento [45].

Também, há a necessidade do controle de acesso às informações com a autenticação dos usuários, garantindo os níveis de acesso dos funcionários com base em perfis individuais. Isso resulta em um melhor gerenciamento dos dados acessados da empresa e, consequentemente, a segurança da informação.

4.3 Mecanismos de Análise GAIA-MLIS

O mecanismo de análise é baseado em trabalhos anteriores do grupo GAIA [7], no qual os pesos P são relacionados as questões com as áreas por meio da eficiência, que é obtida por uma matriz $Q \times 5$, na qual cada coluna corresponde ao peso da questão e a quantidade de linhas corresponde ao número de questões Q. Cada questão possui um vetor de fatores multiplicativos f associados com as alternativas. O elemento f_i é o fator multiplicativo selecionado da i-ésima questão. O valor do questionário é calculado na área e, dado por (1).

$$Resultado\ do\ Questionário\ (e) = \sum_{i=1}^{Q} f_i * p_{i,e} \quad (1)$$

A determinação dos valores $VMX(e)$ e $VMN(e)$ representam os valores máximo e mínimo, respectivamente, os quais delimitam a faixa em que os resultados do questionário irão ser interpretados. A utilização desses valores admite a obtenção de um resultado proporcional à faixa de pontuação, permitindo identificar como a organização se encontra dentro dos limites possíveis do questionário [7]. Este cálculo é realizado pela resolução do questionário. Dessa maneira, sempre que o questionário sofrer alterações deve-se verificar seus valores e máximos e mínimos para que o diagnóstico continue válido. A pontuação da empresa é determinada individualmente em cada área e. Assim, a faixa de pontuação é dada por (2).

$$Faixa\ de\ Pontuação\ (e) = VMX(e) - VMN(e) \quad (2)$$

A faixa de pontuação representa o intervalo em que o resultado do questionário pode variar. Para a interpretação dos resultados é necessário que as respostas sejam ajustadas. Dessa maneira, o fator de ajuste é dado por (3).

$$Fator\ de\ Ajuste\ (e) = 0 - VMN(e) \quad (3)$$

O cálculo do valor obtido pelo questionário nas áreas é realizado através da normalização dada por (4).

$$Taxa\ de\ Atendimento\ (e) = \frac{Resultado\ do\ Questionário(e) + Fator\ de\ Ajuste(e)}{Faixa\ de\ Pontuação\ (e)} \quad (4)$$

A equação (4) tem como resultado um valor percentual que representa o nível de maturidade da empresa na área e. Dessa forma, os valores dos percentuais são alcançados em cada área analisada. Essa $Taxa\ de\ Atendimento\ (e)$ corresponde aos valores que irão enquadrar o resultado diagnóstico da empresa nos respectivos níveis de maturidade.

Há um fator multiplicativo (FM) atribuído a cada uma das questões. Esses fatores variam de -3 a 3, como observado na Tabela 4.1. Valores maiores e positivos representam as respostas que mais favorecem a segurança da informação. Além disso, cada questão possui um peso, que é relacionado aos áreas. Esses pesos indicam influência exercida pelo aspecto analisado sobre cada área, variando de 0 a 4, como apresentado na Tabela 4.2.

Tabela 4.1 – Exemplo de questão para a análise do fator multiplicativo.

1. Existe uma política de troca de *Hardware*?		
Alternativa		**FM**
A	Sim.	3
B	Parcial.	1
D	Não.	-3

Tabela 4.2 – Exemplo de análise dos pesos para a questão da Tabela 5.1.

Área	**Justificativa**	**Peso**
GAIA-MLIS *Hardware*	A existência da política afeta diretamente a área.	4
GAIA-MLIS *Software*	A existência da política influencia na área.	3
GAIA-MLIS Instalações/Espaços Físicos	A existência da política afeta indiretamente a área.	1
GAIA-MLIS Pessoas	A existência da política influencia nas pessoas/funcionários.	3
GAIA-MLIS Informação	A existência da política afeta diretamente a área.	4

Dessa forma, com relação aos níveis de maturidade em segurança da informação, destaca-se que os valores para cada nível e faixas de segurança da informação são apresentados na Tabela 4.3. Essas faixas de valores foram escolhidas para melhor adequarem-se à realidade das empresas e encontram-se em conformidade com as respostas e indicam de forma correta a real situação das organizações de acordo com o nível de segurança da informação. Vale salientar que o nível de maturidade da empresa é indicado pelo nível da área que atingiu o menor valor durante a avaliação diagnóstica. As características de cada nível de maturidade são detalhadas na seção 5.3.

Tabela 4.3 – Faixa de valores dos níveis de maturidade em segurança da informação.

Nível de Maturidade	Faixas de Valores
Não Seguro	0 até 30
Inicial	30,1 até 60
Parcial	60,1 até 80
Seguro	80,1 até 100

Os resultados obtidos durante a pesquisa ajudaram as empresas a verificarem quais são os pontos fortes e fracos nos processos operacionais. Fato este que indica a utilização e disseminação do GAIA-MLIS, como ferramenta auxiliadora, para gerentes e diretores tomarem as decisões que vão conceber os melhores resultados no planejamento e na execução operacional da segurança da informação. Os resultados foram analisados conforme a seção 5.1.

4.4 Nível de Maturidade GAIA-MLIS

O GAIA-MLIS possui quatro níveis de segurança da informação com métricas capazes de auxiliarem os gestores a identificarem pontos fortes e fracos na rede analisada. Esses níveis de segurança foram baseados nos níveis de segurança das normas ISO 27000 e COBIT 5. A Figura 4.7 mostra os níveis de maturidade em segurança da informação propostos no GAIA-MLIS e as informações que os definem.

Figura 4.7 – Níveis de segurança do GAIA-MLIS.

Como pode ser verificado, o nível mais baixo é o não seguro, conforme os processos e procedimentos forem melhorados, o nível de segurança da informação chega até o nível seguro. Abaixo são caracterizadas as métricas referente a cada nível.

- **Nível 0, Não Seguro**: Os processos não são definidos em segurança da informação. Há falta de responsabilidades definidas pelas políticas de segurança. Os funcionários e parceiros não têm conhecimento ou não são treinados com programas de conscientização sobre a importância da segurança da informação. Política de desligamento de funcionários e parceiros não são aplicadas após a rescisão. Não há um processo definido de controle de segurança ou de controle de acesso. As instalações físicas não possuem segurança explícita formalizada por meio de controles. Não há proteção do equipamento contra ameaças externas, sejam elas de cunho humano ou ambientais. Não há uma gestão eficiente para a rede, evitando ou minimizando perdas, danos ou roubo de ativos de informação. As informações sobre os ativos não são criptografadas. Não existe nenhuma política de *backup* com cópias armazenadas em ambientes monitorados com controle de acesso e protegido contra ameaças externas. Não existe inventários dos ativos de TIC.

- **Nível 1, Inicial**: Alguns processos são definidos em segurança da informação. Há falta de um conjunto definido de responsabilidades através de políticas de segurança da informação. Os funcionários e parceiros não têm conhecimento ou não são treinados com programas de conscientização sobre a importância da segurança da informação. Os funcionários e parceiros não enfrentam um processo disciplinar após a descoberta de um incidente de segurança. Política de desligamento de funcionários e parceiros são aplicadas a esmo após a rescisão. Não há um processo de controle de segurança ou de acesso definido. Instalações físicas são inseguras. Há alguma proteção dos equipamentos contra ameaças externas, sejam eles humanos ou ambientais. Há um gerenciamento básico para a rede sem processos definidos para evitarem ou minimizarem a perda, roubo ou danos aos ativos de informação. As informações sobre os ativos não são

criptografadas. Há alguma política de *backup*s, mas não há cópias armazenadas em ambientes monitorados com controle de acesso em um ambiente protegido contra ameaças externas. Inventário dos ativos de TIC não são estabelecidos nem documentados.

- **Nível 2, Parcial**: Os processos são definidos em segurança da informação, há conjuntos de responsabilidades definidas por meio de políticas de segurança. Os funcionários e os parceiros são treinados em programas de conscientização sobre a importância da segurança da informação. Os funcionários sofrem processos disciplinares quando há descoberta de um incidente de segurança. O desligamento de funcionários e parceiros são parcialmente aplicados e documentados após a rescisão. Há procedimentos de segurança e controle de acesso definidos. Instalações físicas são protegidas. Há alguma proteção do equipamento contra ameaças externas, sejam eles humanos ou ambientais. Há uma gerência de rede eficiente, com alguns processos definidos para evitarem ou minimizarem a perda, roubo ou danos aos ativos de informação. As informações sobre os ativos são criptografadas. Existem políticas de *backup* com cópias armazenadas em ambientes monitorados, com controle de acesso e ameaças externas ao meio ambiente. Os inventários dos ativos são identificados e estabelecidos, porém são parcialmente documentados.

- **Nível 3, Seguro**: Os processos são definidos através de um conjunto de políticas com responsabilidades na segurança da informação. A equipe e os parceiros são treinados em programas de conscientização sobre a importância da segurança da informação. Os funcionários e parceiros sofrem processos disciplinares após a descoberta de um incidente de segurança. Políticas de desligamento de funcionários e parceiros são aplicadas e totalmente documentados. Há segurança e controle de acesso definidos. Instalações físicas são garantidos. Há proteção do equipamento contra ameaças externas, sejam elas humanas ou ambientais. Há gerenciamento de rede eficiente, evitando ou minimizando perdas, danos ou roubo de ativos de informação. As

> informações sobre os ativos são criptografadas. Há políticas de *backups*, as cópias são armazenadas em ambientes monitorados com controle de acesso e do ambiente contra ameaças externas. Os inventários dos ativos são identificados, estabelecidos e registrados.

A forma de medir ou criar métricas para as cinco áreas não é uma tarefa fácil, muitos quesitos de segurança devem ser analisados com o objetivo de descrever quais são os processos deficientes e o que deve ser melhorado ou mantido. Para chegar aos resultados e verificar a real situação das empresas analisadas, foi proposto e utilizado um questionário para efetuar a coleta de dados sobre as áreas. Este questionário é composto ao todo de vinte e quatro questões. Elas foram desenvolvidas de forma objetiva com a finalidade de descrever situações específicas de cada área relacionada à segurança. O objetivo do questionário é tornar viável e simples a sua aplicação, uma vez que a pessoa que responde não necessita de um conhecimento amplo sobre governança de TI. O questionário completo pode ser visualizado no apêndice.

A avaliação do GAIA-MLIS fornece às empresas públicas ou privadas, a capacidade de medir, gerenciar e verificar as informações de ativos e usar métricas com o objetivo de melhorar a estruturação de seus processos relacionados à segurança. Desse modo, os resultados obtidos com a suplementação de dados pelas áreas fornecem maior controle dos processos utilizados em segurança da informação, bem como mapear os riscos que as organizações estão sujeitas a cada dia.

O capítulo 5 apresenta os resultados da aplicação do GAIA-MLIS em um conjunto de empresas de TI. Nessa análise é verificado o nível de maturidade das empresas nas cinco áreas estabelecidas pela abordagem. Além disso, são sugeridas ações a serem adotadas para auxiliar os diretores na tomada de decisões que levam a melhores resultados no planejamento e na execução operacional dos processos empresariais referente à segurança da informação.

5 RESULTADOS OBTIDOS

A avaliação diagnóstica tem como objetivo identificar pontos fortes e fracos dentro das cinco áreas analisadas e indicar qual o nível de segurança da informação nos setores e, como consequência, avaliar o nível total de segurança da informação da empresa. Com os dados obtidos por meio das respostas, ações e medidas são indicadas por meio das tabelas 5.4 à 5.8, para que as organizações possam identificar quais áreas e processos são mais propícios a eventos de segurança e tomar providências para melhorar o nível de maturidade a fim de promoverem uma governança de TI eficaz.

Ao todo 23 empresas foram verificadas pelo GAIA-MLIS. Essas corporações são do norte do Paraná na região metropolitana de Londrina, atuando no seguimento desde prestadoras de serviço em TI, instituições financeiras e instituições públicas. Essas instituições são de pequeno, médio e grande porte. Essas organizações responderam ao questionário e, por meio das respostas, o nível de maturidade em segurança da informação é verificado para cada área. Devido a um acordo de confidencialidade, os nomes das empresas não serão divulgados. Vale salientar, também, que os dados são usados para fins acadêmicos.

5.1 Resultados aplicando o GAIA-MLIS

Nesta seção, serão apresentados os resultados referente à aplicação do questionário no cenário organizacional. Além disso, as medidas adotadas para o aprimoramento do atual estado do questionário são analisadas e elucidadas. Será mostrada a média da taxa de atendimento por área de todas as organizações analisadas. Posteriormente, os resultados de duas empresas serão melhores investigados, as quais representam o pior e melhor caso encontrado durante a verificação do nível de maturidade.

Os resultados nas áreas analisadas de todas as empresas são observadas como se segue. Na área de *hardware* observa-se que há a necessidade da elaboração de política de troca de *hardware*, visto que 10 empresas não possuem esse tipo de política, 10 possuem parcialmente e somente em 3 empresas a política é aplicada. Com relação a política de manutenção em *hardware*, 4 empresas realizam tal política, 9 parcialmente e em 10 não existe essa prática. A análise em relação à existência de uma política de segurança voltada especificamente aos equipamentos de informática evidenciou que um total de 18 empresas dispensam a utilização de tal política, ao passo que 2 implementam parcialmente e apenas 3 a

incorporam aos processos organizacionais. Assim, há a necessidade da criação de políticas voltadas à troca e manutenção além de melhorias constantes na condução de tarefas das empresas que implementam parcialmente tais políticas.

Na área de *software*, 12 empresas utilizam antivírus com suporte 24 horas e 11 gratuito. É recomendado que as organizações invistam em antivírus pago, para que a segurança do ambiente computacional seja melhor efetuada. Todas as empresas usam firewall implementado no servidor de controle da rede de dados. Em relação às políticas destinadas à atualização de *software*, o diagnóstico das empresas analisadas foi expressivo. Cerca de 47% das instituições negligenciam essa prática, indicando que a implementação de políticas de atualização de *software* faz-se necessária para elevar o nível de maturidade dessa área. Sobre utilização de *software*s originais, 19 organizações usam e 4 não são adeptas aos *software*s originais. Com relação à política de instalação e manutenção de *software*, 4 empresas possuem a política, 12 implementam parcialmente e 7 não possuem. Para 8 empresas, a documentação de falha de *software* é dispensável, ao passo que 6 utilizam documentação para catalogar eventos de *software*s observados.

Na área de instalações, foi observado que 78% das empresas mantêm os seus servidores de rede em ambiente seguro e com controle de acesso. O restante das instituições apontaram que não possuem um ambiente específico para abrigar tais equipamentos. Em 5 organizações existe política de controle de acesso nas instalações, 10 parcialmente implementada e 8 não possuem tal política. Com relação aos ativos de redes, 18 empresas monitoram e controlam os espaços físicos onde encontra-se esses equipamentos, 3 implementam o monitoramento e controle de forma parcial e 2 não controlam nem monitoram. Para 18 empresas há o monitoramento por câmeras e alarmes no espaço físico/instalação, 3 utilizam de forma parcial e 2 não há monitoramento por câmeras e alarmes.

Na área de pessoas, 4 empresas possuem plano de contingência e equipe de infraestrutura de TI, em 15 existe a equipe de infraestrutura, porém o plano de contingência é inexistente e, por fim, 4 empresas não possuem equipe de infraestrutura nem plano de contingência. Com relação à política de segurança da informação, 18 empresas não possuem e 7 possuem, mas não é divulgado de forma total aos funcionários. Sobre os treinamentos em segurança da informação, 1 empresa treina seus funcionários semestralmente, 10 anualmente e 12 não efetuam treinamentos. A avaliação dos treinamentos dos funcionários é realizada semestralmente por 2 empresas, de forma anual para 11 e 10 não realizam avaliação dos treinamentos. Com base nos resultados obtidos é possível verificar uma grande defasagem das empresas em relação aos processos que propiciariam o aprimoramento do nível de maturidade

em relação à área de pessoas. De fato, essa área é a que teve menor desempenho durante a avaliação, como pode ser verificado na Tabela 5.1. Melhorias incluem o estabelecimento de uma equipe de infraestrutura de TI voltada especificamente à resolução e mitigação de pontos de melhoria de segurança, além de treinamento e avaliação constante dos funcionários quanto às políticas de segurança aplicadas pela empresa.

Na área da informação, 18 empresas possuem política de *backup*, 4 implementam parcialmente e 1 não realiza. Sobre a redundância dos servidores de rede, 16 empresas possuem tal recurso e 7 não. Com relação à criptografia dos sistemas, 11 implementam parcialmente, 7 criptografam o sistema de modo total, 5 não usam criptografia. No que diz respeito ao *backup*, 12 empresas deixam cópias em lugares separados e 11 guardam no mesmo local onde as informações são coletadas, isto é, nos servidores de rede. Para 2 empresas há uma política de tecnologia de mídias do *backup* e 21 não implantam tal política. Ao todo, 21 organizações implementam de forma parcial uma política de controle de acesso da informação com base no perfil de cada funcionário, 1 implementa de forma total e 1 não utiliza da política.

A Tabela 5.1 demonstra o valor médio da análise por área das 23 empresas verificadas pela abordagem GAIA-MLIS.

Tabela 5.1 – Taxa média de atendimento por área das 23 empresas analisadas.

Área	Índice de Atendimento em relação ao nível de maturidade	Nível de Maturidade
GAIA-MLIS *Hardware*	51,59	Inicial
GAIA-MLIS *Software*	54,79	Inicial
GAIA-MLIS Instalações/Espaços Físicos	56,02	Inicial
GAIA-MLIS Pessoas	51,13	Inicial
GAIA-MLIS Informação	55,80	Inicial

A maturidade média das 23 empresas analisadas pertence ao nível Inicial. As empresas devem melhorar os seus planejamentos estratégicos em todas as áreas verificadas, a fim de utilizarem de investimentos para que a segurança da informação seja mantida. Das 23 empresas, 4 encontram-se no nível Não Seguro, 13 empresas estão no nível Inicial, 4 estão no nível Parcial e 2 estão no nível Seguro. A Figura 5.1 demonstra a quantidade de empresas que estão em cada nível de segurança da informação conforme a área.

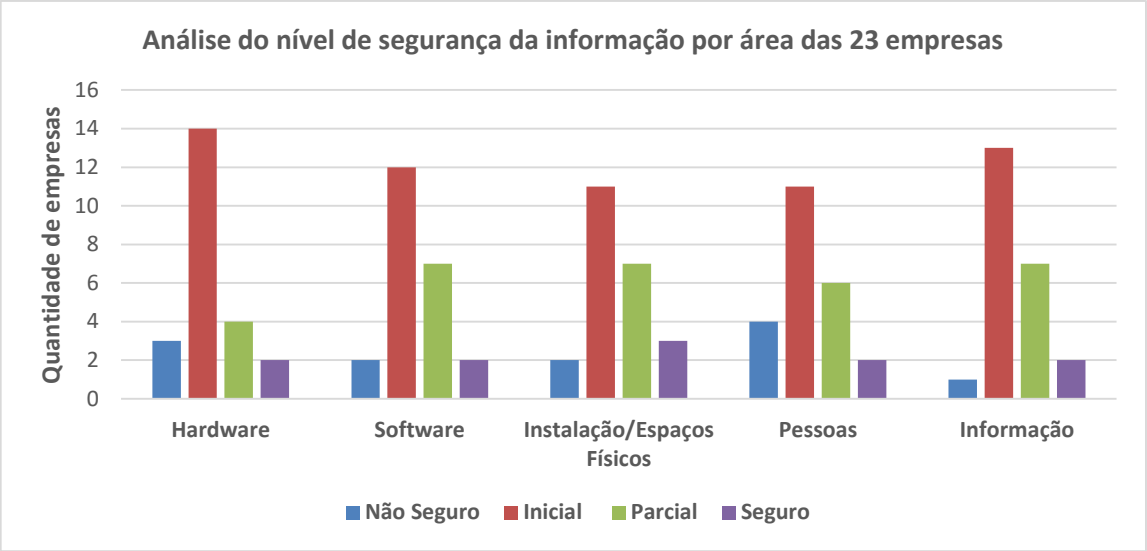

Figura 5.1 – Análise do nível de segurança por área.

Na média, o caso menos satisfatório corresponde a área de Pessoas com uma $Taxa\ de\ Atendimento\ (e) = 51{,}13$. Por sua vez, a área de Instalações/Espaços Físicos obteve o melhor desempenho com uma $Taxa\ de\ Atendimento\ (e) = 56{,}02$. Esses resultados indicam que a maioria das empresas precisa verificar todos os processos de segurança da informação conforme indicado na avaliação por meio do questionário. As ações da Tabela 5.5 até a Tabela 5.9 são determinantes para que a efetivação da governança de TI seja realizada de forma eficaz e plena.

5.1.1 Comparação entre o pior e melhor caso diagnosticado

Para demonstrar a eficiência da abordagem diagnóstica, dois casos serão verificados com mais minuciosidade. A empresa 1 representa a pior classificação do nível de maturidade em segurança da informação por área ao apresentar o menor nível entre as empresas.

A Figura 5.2 mostra os resultados dos níveis de maturidade em segurança da informação por área da empresa 1.

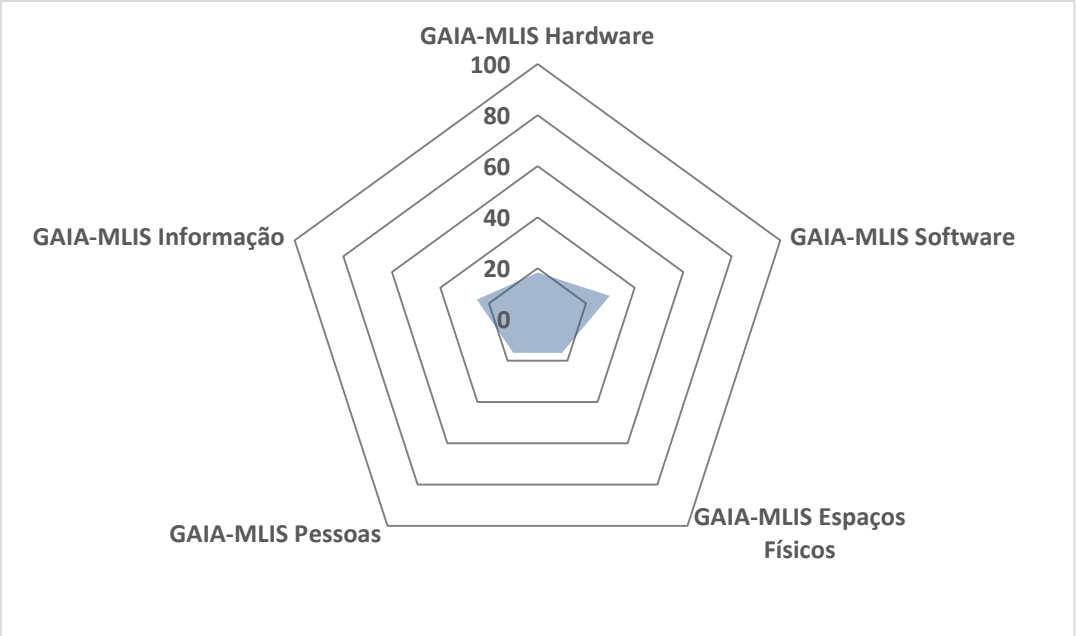

Figura 5.2 – Avaliação diagnóstica da empresa 1.

O resultado obtido pela pior empresa avaliada será mostrado para a validação do cálculo da abordagem. Como primeiro passo, os valores de máximo (VMX) e mínimo (VMN) foram calculados com base nas possíveis respostas no melhor e pior caso, respectivamente. Vale salientar que o valor mínimo corresponde às respostas menos condizentes com a segurança da informação, ao passo que o valor máximo representa a pontuação máxima alcançada quando as respostas mais propícias são escolhidas. Os resultados dos valores máximos e mínimos de cada área podem ser observados na Tabela 5.2.

Tabela 5.2 – Valor de máximo e mínimo das áreas.

Área	Valor Máximo (VMX)	Valor Mínimo (VMN)
GAIA-MLIS *Hardware*	180	-180
GAIA-MLIS *Software*	228	-228
GAIA-MLIS Instalações/Espaços Físicos	129	-129
GAIA-MLIS Pessoas	216	-216
GAIA-MLIS Informação	288	-288

O passo seguinte corresponde à contabilização das respostas fornecidas pela empresa durante a análise. Para tanto, é utilizada a equação 1. Como é sabido, cada questão está relacionada a um fator multiplicativo fi e a um peso de influência exercido sobre a área de *hardware*.

$$Resultado\ do\ Questionário\ (Hardware) = \sum_{i=1}^{Q} f_i * p_{i,e}$$

$$Resultado\ do\ Questionário\ (Hardware) = -72 - 45 - 3 + 2 + 4$$

$$Resultado\ do\ Questionário\ (Hardware) = -114$$

Após a resolução do questionário em *hardware* a faixa de pontuação é obtida com os valores de máximo e mínimo, por meio da equação 2.

$$Faixa\ de\ Pontuação\ (Hardware) = VMX(Hardware) - VMN(Hardware)$$
$$Faixa\ de\ Pontuação\ (Hardware) = 180 - (-180)$$
$$Faixa\ de\ Pontuação\ (Hardware) = 360$$

Após o cálculo da faixa de pontuação o fator de ajuste é usado para a normalização dos resultados obtidos por meio do questionário. A equação 3 descreve como o cálculo é realizado.

$$Fator\ de\ Ajuste\ (Hardware) = 0 - VMN(Hardware)$$
$$Fator\ de\ Ajuste\ (Hardware) = 0 - (-180)$$
$$Fator\ de\ Ajuste\ (Hardware) = 180$$

Por meio dos resultados obtidos dos cálculos acima, o valor do nível de maturidade em segurança da informação na área de *hardware* pode ser calculado como mostra a equação 4.

$$Taxa\ de\ Atendimento\ (Hardware) = \frac{Resultado\ do\ Questionário\ (Hardware) + Fator\ de\ Ajuste\ (Hardware)}{Faixa\ de\ Pontuação\ (Hardware)}$$
$$Taxa\ de\ Atendimento\ (Hardware) = \frac{-114 + 180}{360}$$
$$Taxa\ de\ Atendimento\ (Hardware) = \frac{66}{360}$$
$$Taxa\ de\ Atendimento\ (Hardware) = 18{,}33$$

A Taxa de Atendimento mostra a adequação da área em relação aos quesitos de segurança da informação. A taxa com valor 18,33 indica que a empresa se encontra no nível não seguro em relação aos equipamentos e políticas voltadas à área de *hardware*. O processo de cálculo é realizado de forma análoga nas demais áreas analisadas e, aquela que apresentar menor Taxa de Atendimento caracterizará o nível de maturidade em segurança da informação da empresa, como tratado na seção 4.3.

Os valores de máximo e mínimo da área de *software* foram calculados com base nas respostas do questionário no melhor e pior caso. A avaliação do questionário na área de *software.*

$$Resultado\ do\ Questionário\ (Software) = \sum_{i=1}^{Q} f_i * p_{i,e}$$

$$Resultado\ do\ Questionário\ (Software) = -63 - 24 + 8 - 12 - 3 + 2$$

$$Resultado\ do\ Questionário\ (Software) = -92$$

Após a avaliação do questionário em *software*, a faixa de pontuação é obtida com os valores de máximo e mínimo.

$$Faixa\ de\ Pontuação\ (Software) = VMX(Software) - VMN(Software)$$

$$Faixa\ de\ Pontuação\ (Software) = 228 - (-228)$$

$$Faixa\ de\ Pontuação\ (Software) = 456$$

Após o cálculo da faixa de pontuação, o fator de ajuste é usado para a normalização dos resultados obtidos por meio do questionário.

$$Fator\ de\ Ajuste\ (Software) = 0 - VMN(Software)$$

$$Fator\ de\ Ajuste\ (Software) = 0 - (-228)$$

$$Fator\ de\ Ajuste\ (Software) = 228$$

Por meio dos resultados obtidos dos cálculos acima, o valor do nível de maturidade em segurança da informação na área de *software* pode ser calculado.

$$Taxa\ de\ Atendimento\ (Software) = \frac{Resultado\ do\ Questionário\ (Software) + Fator\ de\ Ajuste\ (Software)}{Faixa\ de\ Pontuação\ (Software)}$$

$$Taxa\ de\ Atendimento\ (Software) = \frac{-92 + 228}{456}$$

$$Taxa\ de\ Atendimento\ (Software) = \frac{136}{456}$$

$$Taxa\ de\ Atendimento\ (Software) = 29{,}82$$

Os valores de máximo e mínimo da área de instalações foram calculados com base nas respostas do questionário no melhor e pior caso. A avaliação do questionário na área de instalações.

$$Resultado\ do\ Questionário\ (Instalações) = \sum_{i=1}^{Q} f_i * p_{i,e}$$

$$Resultado\ do\ Questionário\ (Instalações) = -9 - 84 + 2 + 4$$

$$Resultado\ do\ Questionário\ (Instalações) = -87$$

Após a resolução do questionário em instalações a faixa de pontuação é obtida com os valores de máximo e mínimo.

$$Faixa\ de\ Pontuação\ (Instalações) = VMX(Instalações) - VMN(Instalações)$$

$$Faixa\ de\ Pontuação\ (Instalações) = 129 - (-129)$$

$$Faixa\ de\ Pontuação\ (Instalações) = 258$$

Após o cálculo da faixa de pontuação o fator de ajuste é usado para a normalização dos resultados obtidos por meio do questionário.

$$Fator\ de\ Ajuste\ (Instalações) = 0 - VMN(Instalações)$$

$$Fator\ de\ Ajuste\ (Instalações) = 0 - (-129)$$

$$Fator\ de\ Ajuste\ (Instalações) = 129$$

Por meio dos resultados obtidos dos cálculos acima, o valor do nível de maturidade em segurança da informação na área de instalações pode ser calculado.

$$Taxa\ de\ Atendimento\ (Instalações) = \frac{Resultado\ do\ Questionário\ (Instalações) + Fator\ de\ Ajuste\ (Instalações)}{Faixa\ de\ Pontuação\ (Instalações)}$$

$$Taxa\ de\ Atendimento\ (Instalações) = \frac{-87 + 129}{258}$$

$$Taxa\ de\ Atendimento\ (Instalações) = \frac{43}{258}$$

$$Taxa\ de\ Atendimento\ (Instalações) = 16{,}28$$

Os valores de máximo e mínimo da área de pessoas foram calculados com base nas respostas do questionário no melhor e pior caso. A avaliação do questionário na área de pessoas.

$$Resultado\ do\ Questionário\ (Pessoas) = \sum_{i=1}^{Q} f_i * p_{i,e}$$

$$Resultado\ do\ Questionário\ (Pessoas) = -90 - 72 + 8 + 2 + 6$$
$$Resultado\ do\ Questionário\ (Pessoas) = -146$$

Após a resolução do questionário em pessoas a faixa de pontuação é obtida com os valores de máximo e mínimo.

$$Faixa\ de\ Pontuação\ (Pessoas) = VMX(Pessoas) - VMN(Pessoas)$$
$$Faixa\ de\ Pontuação\ (Pessoas) = 216 - (-216)$$
$$Faixa\ de\ Pontuação\ (Pessoas) = 432$$

Após o cálculo da faixa de pontuação o fator de ajuste é usado para a normalização dos resultados obtidos por meio do questionário.

$$Fator\ de\ Ajuste\ (Pessoas) = 0 - VMN(Pessoas)$$
$$Fator\ de\ Ajuste\ (Pessoas) = 0 - (-216)$$
$$Fator\ de\ Ajuste\ (Pessoas) = 216$$

Por meio dos resultados obtidos dos cálculos acima, o valor do nível de maturidade em segurança da informação na área de instalações pode ser calculado.

$$Taxa\ de\ Atendimento\ (Pessoas) = \frac{Resultado\ do\ Questionário\ (Pessoas) + Fator\ de\ Ajuste\ (Pessoas)}{Faixa\ de\ Pontuação\ (Pessoas)}$$
$$Taxa\ de\ Atendimento\ (Pessoas) = \frac{-146 + 216}{432}$$
$$Taxa\ de\ Atendimento\ (Pessoas) = \frac{70}{432}$$
$$Taxa\ de\ Atendimento\ (Pessoas) = 16{,}20$$

Os valores de máximo e mínimo da área de informação foram calculados com base nas respostas do questionário no melhor e pior caso. A avaliação do questionário na área de informação.

$$Resultado\ do\ Questionário\ (Informação) = \sum_{i=1}^{Q} f_i * p_{i,e}$$
$$Resultado\ do\ Questionário\ (Informação) = -156 + 12$$
$$Resultado\ do\ Questionário\ (Informação) = -144$$

Após a resolução do questionário em informação a faixa de pontuação é obtida com os valores de máximo e mínimo.

$$Faixa\ de\ Pontuação\ (Informação) = VMX(Informação) - VMN(Informação)$$
$$Faixa\ de\ Pontuação\ (Informação) = 288 - (-288)$$
$$Faixa\ de\ Pontuação\ (Informação) = 576$$

Após o cálculo da faixa de pontuação o fator de ajuste é usado para a normalização dos resultados obtidos por meio do questionário.

$$Fator\ de\ Ajuste\ (Informação) = 0 - VMN(Informação)$$
$$Fator\ de\ Ajuste\ (Informação) = 0 - (-288)$$
$$Fator\ de\ Ajuste\ (Informação) = 288$$

Por meio dos resultados obtidos dos cálculos acima, o valor do nível de maturidade em segurança da informação na área de instalações pode ser calculado.

$$Taxa\ de\ Atendimento\ (Informação) = \frac{Resultado\ do\ Questionário\ (Informação) + Fator\ de\ Ajuste\ (Informação)}{Faixa\ de\ Pontuação\ (Informação)}$$
$$Taxa\ de\ Atendimento\ (Informação) = \frac{-144 + 288}{576}$$
$$Taxa\ de\ Atendimento\ (Informação) = \frac{144}{576}$$
$$Taxa\ de\ Atendimento\ (Pessoas) = 25$$

A empresa 1 apresenta o menor nível de maturidade em segurança da informação na área de Pessoas. Além disso, as demais áreas possuem complicações significativas, sendo fortemente recomendada a verificação dos procedimentos e processos de segurança relacionados a esses pontos de melhoria. Desse modo, o nível total em segurança da informação da empresa 1 é a $Taxa\ de\ Atendimento\ (e) = 16{,}20$, o que corresponde ao nível Não Seguro.

A melhor área avaliada na empresa 1 é a de *Software* com uma $Taxa\ de\ Atendimento\ (e) = 29{,}82$, seguida pelas áreas de Informação, *Hardware*,

Instalações/Espaços Físicos. Todas as áreas estão no nível Não Seguro de segurança da informação da abordagem GAIA-MLIS.

Na área de *hardware* observa-se que a empresa 1 não possui as políticas relacionadas a essa área. Não existem políticas destinadas à atualização, instalação ou manutenção de *software*. As falhas são reportadas e documentadas parcialmente. Em instalações físicas, nenhuma resposta foi satisfatória. Os servidores de rede não ficam em ambiente seguro, não há política de controle de acesso nas instalações, os ativos de redes não são monitorados nem as instalações. Na área de pessoas, a respostas mais significativa é a da equipe de infraestrutura de TI, mas a equipe não tem preparo para evento de segurança da informação. As demais questões dessa área foram negativas. Na área de informação, destaca-se somente a política de *backup* que é implementada pela organização. A política de controle de acesso da informação com base no perfil de cada funcionário é implementada parcialmente. As demais respostas foram negativas. As ações, por área, deverão ser tomadas para melhorar o nível de maturidade em segurança da informação segundo as medidas descritas nas Tabelas 5.5, 5.6, 5.7, 5.8 e 5.9. A Tabela 5.3 mostra a taxa de atendimento por área da empresa 1.

Tabela 5.3 – Taxa de atendimento por área da empresa 1.

Área	Índice de Atendimento em relação ao nível de maturidade	Nível de Maturidade
GAIA-MLIS *Hardware*	18,33	Não Seguro
GAIA-MLIS *Software*	29,82	Não Seguro
GAIA-MLIS Instalações/Espaços Físicos	16,28	Não Seguro
GAIA-MLIS Pessoas	16,20	Não Seguro
GAIA-MLIS Informação	25,00	Não Seguro

Como forma de análise será visualizado o resultado do melhor caso dentre as empresas verificadas. Assim, será elucidado a área que obteve a melhor avaliação. A empresa 2 obteve uma taxa de atendimento superior por área dentre as demais, e como consequência, apresentou o melhor nível de segurança da informação. A Figura 5.3 descreve os valores dos níveis de segurança da informação por área da empresa 2.

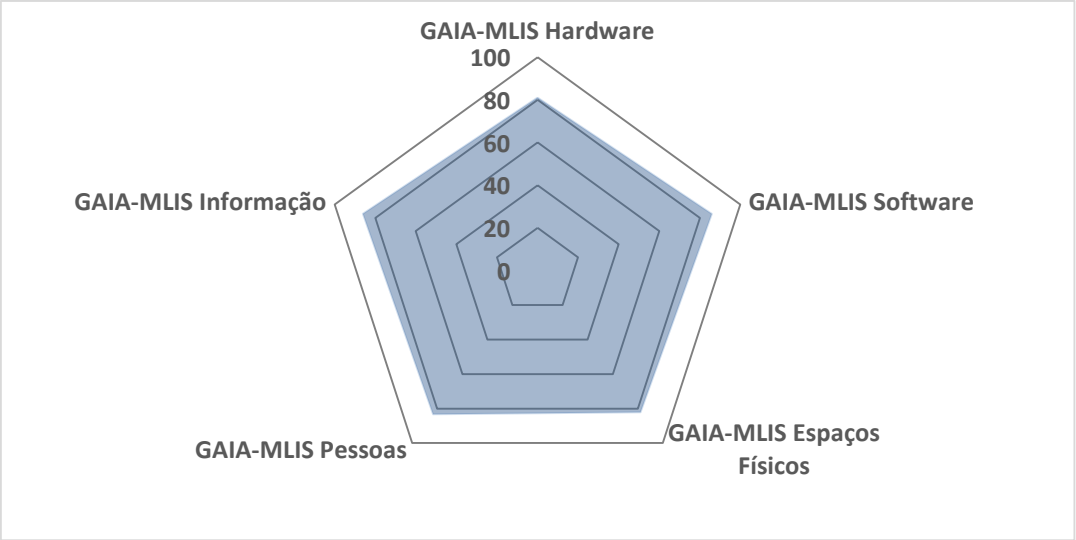

Figura 5.3 – Avaliação diagnóstica da empresa 2.

A empresa avaliada tem como maior deficiência as políticas implementas para troca e manutenção de *hardware*. O nível de maturidade alcançado por tal área é $Taxa\ de\ Atendimento\ (e) = 81{,}11$, o que corresponde ao limite inferior do nível de maturidade Seguro. Embora, tal nível descreva a situação geral da empresa, é importante salientar que manter constante avaliação e aprimoramento das políticas relacionados aos equipamentos são imprescindíveis para que a segurança se mantenha atuante e proativa perante aos diversos eventos de segurança que possam ocorrer.

A área com melhor avaliação na empresa 2 corresponde a da Informação com uma $Taxa\ de\ Atendimento\ (e) = 86{,}11$, seguida pelas áreas de *Software*, Pessoas e Instalações/Espaços físicos. As taxas de atendimentos das áreas indicam que todas estão no nível seguro, porém os processos ainda necessitam de vistorias contínuas para que a governança de TI em segurança da informação seja efetivada.

Na área de *hardware* observa-se que a empresa 2 possui todas as políticas. Com relação a área de *software* todas as respostas foram satisfatórias. Em instalações uma política de controle de acesso é aplicada de forma parcial. Na área de pessoas, a política de segurança da informação é divulgada parcialmente aos funcionários. O treinamento sobre a segurança da informação e as avaliações dos treinamentos são realizados anualmente. Na área de informação, destaca-se a falta de um sistema de avaliação diagnóstica em segurança da informação. As demais questões foram respondidas de forma positiva. As ações, por área, deverão ser tomadas conforme descritos nas Tabelas 5.5, 5.6, 5.7, 5.8 e 5.9. A Tabela 5.4 mostra a taxa de atendimento por área da empresa 2.

Tabela 5.4 – Taxa de atendimento por área empresa 2.

Área	Índice de Atendimento em relação ao nível de maturidade	Nível de Maturidade
GAIA-MLIS *Hardware*	81,11	Seguro
GAIA-MLIS *Software*	85,96	Seguro
GAIA-MLIS Instalações/Espaços Físicos	82,17	Seguro
GAIA-MLIS Pessoas	83,33	Seguro
GAIA-MLIS Informação	86,11	Seguro

Após analisar os valores dos níveis de maturidade em segurança da informação, será apresentado descrições de medidas e ações conforme as respostas obtidas.

5.1.2 Descrição de Medidas e Ações

Por meio dos resultados obtidos nas análises com o questionário, ações deverão ser tomadas por área. Essas ações contribuem para a realização de uma governança de TI voltada para a segurança da informação. Tabela 5.5 refere-se às questões de *hardware* e quais são as medidas a serem adotadas conforme a necessidade da empresa.

Tabela 5.5 – Questões de *hardware* e medidas/ações.

Questões de *Hardware* – Medidas/Ações	
Perguntas	**Medidas/Ações**
Existe uma política de troca de *Hardware*?	Implementar uma Política de troca de equipamentos; Implementar Política para equipe técnica especializada através de treinamentos.
Existe uma política de manutenção em *Hardware*?	Implementar política de manutenção em *Hardware*; Implementar Política para equipe técnica especializada através de treinamentos.
Há uma política de segurança para os equipamentos de informática?	Planejar políticas de segurança; Definir responsabilidades dos departamentos e das pessoas.

As medidas destacadas na tabela acima, conforme as respostas das empresas, representam ações que podem ser realizadas de acordo com a necessidade da organização. Essas medidas indicam procedimentos a serem realizados para que a segurança da informação seja efetivada. Também, destaca-se que a análise da área de *hardware* produz uma documentação de normas, procedimentos e responsabilidades, a fim de padronizar procedimentos para a

segurança da informação nessa área. Tabela 5.6 refere-se as questões de *software* e quais são as medidas a serem adotadas conforme a necessidade da empresa.

Tabela 5.6 – Questões de *software* e medidas/ações.

Questões de *Software* – Medidas/Ações	
Perguntas	**Medidas/Ações**
Há antivírus nos computadores da empresa?	Implementar Política de antivírus com suporte 24 horas; Elaborar Política de treinamento para equipe técnica especializada.
Há firewall instalado no servidor da empresa?	Elaborar Política para implantação de firewall; Manter firewall atualizado; Implementar Política de Treinamento para funcionários.
Existe uma política de atualização para *software*?	Implementar Política de atualização de *software*; Implementar Política de treinamento para equipe técnica especializada.
Os *software*s utilizados são originais?	Elaborar Política de instalação de *software*s originais; Implementar Política de treinamento para equipe técnica especializada.
Existe uma política em segurança para instalação e manutenção de *software* na empresa?	Implementar Política para instalação e manutenção em *software*; Elaborar Política de treinamento para equipe técnica especializada.
As falhas nos *software*s são documentadas?	Implementar Política para base de dados com histórico de falhas documentadas; Elaborar Política de catalogação da base de dados de falhas como eventos de segurança da informação.

Como pode ser verificado, há procedimentos que são capazes de auxiliar nas tomadas de decisões. Portanto, o gestor é capaz de, por meio dessas medidas, realizar ajuste nos processos de TI na parte de segurança da informação com relação a área de *software*. A Tabela 6.7 refere-se as questões de instalações e quais são as medidas a serem adotadas conforme a necessidade da empresa.

Tabela 5.7 – Questões de instalações e medidas/ações.

Questões de Instalações/Espaços Físicos – Medidas/Ações	
Perguntas	**Medidas/Ações**
Os servidores de rede ficam em ambiente seguro e com controle de acesso?	Implementar Política de controle de acesso aos servidores de rede em Instalações/Espaços Físicos.
Há uma política de controle de acesso nas instalações?	Elaborar Política de controle de acesso nas instalações.
Os ativos de redes ficam em lugares controlados e monitorados?	Implementar Política de controle e monitoramento das instalações/espaços físicos dos ativos de redes.
As instalações físicas são monitoradas por câmeras e alarmes?	Implementar Política de monitoramento por câmeras e alarmes de toda a área das instalações/espaços físicos.

As instalações físicas e do ambiente empresarial são partes importantes dentro do processo de segurança da informação. Dessa maneira, algumas medidas devem ser realizadas com a finalidade de garantir a proteção de funcionários e equipamentos presentes dentro da organização. Proteger todos os seus ativos é prioridade para o sucesso do planejamento estratégico de uma organização. Portanto, a segurança física do ambiente corporativo garante uma maior confiabilidade e controle de acesso de pessoas autorizadas, porém a segurança tecnológica não é somente garantia de sucesso. Os funcionários responsáveis pelo controle da segurança do ambiente empresarial devem ser treinados e saberem dos seus deveres perante a organização e devem saber como agir diante de um procedimento de risco a segurança da informação.

Tabela 5.8 refere-se as questões de pessoas e quais são as medidas a serem adotadas conforme a necessidade da empresa.

Tabela 5.8 – Questões de pessoas – medidas/ações.

Questões de Pessoas – Medidas/Ações	
Perguntas	**Medidas/Ações**
Equipe de infraestrutura de TI está preparada para um caso de contingência de evento de segurança da informação?	Implementar Política de treinamento da equipe de infraestrutura de TI para caso de contingência de evento de segurança da informação; Elaborar Política de avaliação da equipe de Infraestrutura de TI.
Existe uma política de segurança da informação e ela é divulgada para os seus funcionários?	Implementar Política de segurança da Informação; Elaborar Política de divulgação sobre normas de segurança aos funcionários; Estabelecer departamento

	responsável pela Elaboração da Política de Segurança da Informação e Divulgação.
Os funcionários recebem treinamentos sobre segurança da informação?	Implementar Política de treinamento aos funcionários sobre segurança da informação.
Os funcionários são avaliados em relação aos treinamentos?	Implementar Política de avaliação de treinamento.

A parte mais sensível de um processo de controle de segurança da informação são as pessoas. Funcionários que não possuem um comprometimento ou não sabem as suas obrigações e nem possuem treinamentos adequados, estão sujeitos a cometerem algum delito que pode causar danos as informações da empresa. Dessa maneira, algumas medidas, como as da Tabela 5.9, devem ser tomadas para evitarem problemas de segurança da informação, intencional ou não, gerados pelos funcionários. A Tabela 5.9 refere-se as questões de informações e quais são as medidas a serem adotadas conforme a necessidade da empresa.

Tabela 5.9 – Questões de informação e medidas/ações.

Questões de Informação – Medidas/Ações	
Perguntas	**Medidas/Ações**
Existe política de *backup* para as informações?	Elaborar Política de *backup*.
Existe redundância dos servidores de rede da empresa?	Elaborar Política de redundância dos servidores de rede da empresa.
As informações dos sistemas são criptografadas?	Implementar Política de Criptografia.
Os *backup*s são armazenados em lugares separados?	Elaborar Política de armazenamento das mídias de *backup* em instalações/espaços físicos.
Existe uma política tecnológica das mídias?	Implementar Política tecnológica das mídias.
Existe uma política de controle de acesso da informação com base no perfil de cada funcionário?	Implementar Política de controle de acesso da informação com base no perfil de cada funcionário.
Existe um sistema de avaliação diagnóstica em segurança da informação?	Utilizar o GAIA-MLIS como abordagem diagnóstica.

A informação dentro do ambiente organizacional deve ser íntegra, mantida e transmitida de forma segura até o seu destino. A Tabela 5.9 evidencia algumas medidas a serem tomadas em relação à informação. Todo o processo que determina como a informação deve ser segura passa por medidas como as citadas na tabela.

A contribuição do GAIA-MLIS constitui-se na determinação de medidas conforme as perguntas realizadas no questionário. Assim, com essas indicativas, as empresas podem melhorar os seus processos de negócios, visando uma governança de TI eficaz com a ênfase na segurança da informação.

6 CONCLUSÃO

A segurança da informação é imprescindível para comunicação e armazenamento de dados, sobretudo para o meio organizacional. É constituída por medidas que buscam preservar o valor que a informação possui para um indivíduo ou uma empresa, tendo como base a confiabilidade, a integridade e a disponibilidade. Vazamento de dados sigilosos das organizações podem contribuir para a degradação da imagem empresarial das companhias perante ao mercado e clientes, bem como, causar instabilidade financeira, falta de credibilidade e ainda podendo gerar problemas que prejudicam a continuidade dos negócios.

Com a adesão de um método de controle para a segurança da informação, com foco na Governança de TI, a finalidade de obter uma documentação formal centrada em responsabilidades, plano de contigência e ações capazes de evitar ou solucionar um evento de segurança da informação são necessárias. Dessa maneira, a elaboração de ações, ou contramedidas podem contribuir diretamente para a proteção das informações, além de evitarem problemas com o planejamento estratégico das empresas, especificações de produtos e serviços, como qualquer informação que possa ser modificada, submetida e utilizada por criminosos.

Para um planejamento estratégico corporativo, a conformidade e a interação entre as áreas de *hardware*, *software*, instalação, pessoas e informação devem contribuir para a definição de papéis, funções, atividades e processos que são desenvolvidos pela empresa. Dessa forma, ao investigar o inter-relacionamento entre essas áreas, pode-se verificar se o gerenciamento de riscos em segurança da informação está de acordo com parâmetros mínimos de segurança requeridos para aquela organização.

Este trabalho apresentou uma abordagem com o objetivo de avaliar o nível de maturidade em segurança da informação, denominado GAIA-MLIS, cuja composição visa o diagnóstico da área de *hardware*, *software*, instalações, pessoas e informação com o intuito de colaborar com as organizações para formalização de procedimentos, responsabilidades e planos de contigência diante de um evento de segurança da informação. As seguintes contribuições do trabalho podem ser destacadas:

1. Aplicação de uma abordagem com a finalidade de avaliar o nível de maturidade em segurança da informação, capaz de analisar cinco áreas: *hardware*, *software*, instalação, pessoas e informação;

2. Questionário composto de 24 questões que proporciona uma avaliação nos níveis de maturidade em segurança da informação, indicando pontos fortes e fracos para os processos de negócio em conformidade com a segurança da informação;
3. Contextualização das normas ISO 27000 e COBIT 5 para a elaboração de um documento formal em governança de TI voltado para a segurança da informação;
4. Proposta de quatro níveis de maturidade (não Seguro, Inicial, Parcial e Seguro), que representam os patamares evolutivos nos processos de segurança da informação e possibilitam a implantação de políticas e procedimentos pela empresa analisada;
5. Mapeamento de parâmetros diagnosticados e os respectivos pontos de melhoria para as áreas analisadas de *hardware*, *software*, pessoas, instalações e informação.

Diante dos resultados obtidos pela abordagem proposta neste trabalho, é possível indicar parâmetros que visam auxiliar na verificação, planejamento e implementação de melhorias na segurança da informação, tendo como base o questionário elaborado. A formalização conjunta desses aspectos gera medições periódicas dos riscos, definição de responsabilidades e planejamento para evitar ou tratar um evento de segurança.

A abordagem de nível de maturidade GAIA-MLIS, com o diagnóstico nas cinco áreas estudas, e através do inter-relacionamento entre elas, consegue identificar os pontos de melhorias presentes nessas áreas e indicar quais são as reais necessidades da empresa para a formalização de uma documentação voltada à governança de TI em segurança da informação.

Ainda é possível avançar nesse campo de governança de TI voltada à segurança da informação, a qual o GAIA-MLIS se propõe a atuar. Como trabalhos futuros, pode-se criar uma base de dados para a verificação do nível de segurança da informação nas empresas, conforme as cinco áreas analisadas, com o objetivo de mapear ações com base em tipos de atuações. Mecanismos de aprendizagem automatizados e aptos a tomarem decisões com base nas respostas das empresas podem ser implementados para indicar melhores políticas de gerenciamento de riscos a fim de efetivar a governança de TI e a segurança da informação. Também, será analisado e discutido o conceito de *bring your own device*, que consiste na utilização de dispositivos pessoais conectados em ambientes corporativos. Essa prática proporciona maior produtividade, porém pode ocasionar novos tipos de ameaças à segurança

da informação. Outro ponto de análise é a viabilidade da abordagem separando as empresas em pequenas, médias e grandes adotando pesos diferentes ao fator multiplicativo conforme a realidade de cada subdivisão.

REFERÊNCIAS

[1] TANENBAUM, A.S e WETHERALL, D. Redes de Computadores, 5ª Edição, Pearson, São Paulo, 2011.

[2] SENGUPTA, A., MAZUMDAR, C. e BAGCHI, A., *A Methodology for Conversion of Enterprise-Level Information Security Policies to Implementation-Level Policies/Rule*, Proc IEEE ICEAIT, IEEE Press, 2011, pp 280-283.

[3] GHORFI, R. E., OUADOU, M., ABOUTAJDINE, D. e AROUSSI, M. E., *A Modeling Approach for IT Governance Basics Application on IT Progects and IT Goals*, Proc IEEE ICAIMS, IEEE Press 2014, pp 211 - 216.

[4] WEILL, P. e ROSS, J.W., Governança de TI: Tecnologia da Informação. M. Books. 1ed. 2005.

[5] RIGON, E. A., WESTPHALL, C. M. e SANTOS, D. R., *A Cyclical Evaluation Model of Information Security*, Information Management & Computer Security, Emerald, 2014, pp 1 - 14.

[6] G.KAROKOLA, G., KOWALSKI, S. e YNGSTROM, L., *Secure e-government services: Towards a framework for integrating it security services into e-government maturity models*, Proc IEEE ISSA, IEEE Press 2011, pp 1 - 9.

[7] BRIGANÓ, G. U. *Um Framework para Desenvolvimento de Governança de TIC*. Dissertação de Mestrado em Ciência da Computação. Universidade Estadual de Londrina - UEL. 2012.

[8] TACONI, L. H. GAIA Catálogo de Serviços de TI: Um *Framework* para Construção de Catálogos de Serviços de Tecnologia da Informação. Dissertação de Mestrado em Ciência da Computação. Universidade Estadual de Londrina - UEL. 2014.

[9] GAFFO, F. H. GAIA RISCOS: *Framework* para o Gerenciamento de Riscos no Processo de Desenvolvimento de *Software*. Dissertação de Mestrado em Ciência da Computação. Universidade Estadual de Londrina – UEL. 2013.

[10] GÓES, A. S. GAIA Lições Aprendidas: Um *Framework* para Gerência de Lições Aprendidas no Processo de Desenvolvimento de *Software*. Dissertação de Mestrado em Ciência da Computação. Universidade Estadual de Londrina – UEL. 2014.

[11] MOHAMMED A. A., *Information Security Culture Critical Success Factors*, Proc. IEEE ITNG, Apr 2015, pp 731 - 735.

[12] MAYER, J. e FAGUNDES, L. L., *Risk Management Process in Information Security*, Proc. IEEE IFIP, IEEE Press, Aug 2009, pp 61-70.

[13] HUA, H., *Valuation of Information security concept Methods*, Proc. IEEE CCTAE, IEEE Press, 2010, pp 230-233.

[14] WANG, P. A., *Information Security Knowledge and Behavior*, Proc. IEEE ICETC, IEEE Press, 2010, pp 364-367.

[15] PANGALOS, G., ILIOUDIS, C. e PAGKALOS, I., *The Importance of Corporate Forensic Readiness in the Information Security Framework*, Proc. IEEE WETICE, IEEE Press, 2010, pp 12-16.

[16] CHUNYING, W., *Analysis on the Inforation Security Education for the Public Security Active Forces Academy*, Proc. IEEE IFITA, IEEE Press, 2010, pp 355-357.

[17] SAJKO, M., HADJINA, N. e SEDINIC, I., *Information Security Governance and how to accomplish it*, Proc IEEE MIPRO 2011, IEEE Press, May 2011, pp 1516-1521.

[18] NAKAMURA, E. T. e GEUS, P. L., Segurança de Redes em Ambientes Cooperativos, Futura, Press, 2003.

[19] Akamai Real-Time Internet Monitoring. Dispoível em: https://www.akamai.com/us/en/solutions/intelligent-platform/visualizing-akamai/real-time-web-monitor.jsp. Acesso: 27 de maio de 2016.

[20] CERT.br. Disponível em: http://www.cert.br/stats/incidentes/2013-jan-dec/tipos-ataque-acumulado.html. Acesso: 09 de março de 2015.

[21] SHEN, H. e LI, Z., *Leveraging Social Networks for Effective Spam Filtering*, IEEE Transactions on Computers, vol. 63, no. 11, IEEE Press, Nov 2014, pp 2743-2759.

[22] LARIBEE, L., BARNES, D. S., ROWE, N. C. e MARTELL, C. H., *Analysis and Defensive Tools for Social-Engineering Attacks on Computer Systems*, Proc. IEEE IAW, IEEE Press, Jun 2006, pp 388-389.

[23] MOUTON, F., MALAN, M. M. e VENTER, H. S., *Social Engineering from a Normative Ethics Perspective*, Proc IEEE ISSA, IEEE Press, Aug 2013, pp 1-8.

[24] LEVY, E. e ARCE, I., *Learning from Information Security History*, Proc IEEE Security & Privacy vol 4, IEEE Press 2006, pp 77 - 79.

[25] GOLUCH, G., EKELHART, A., FENZ, S., JAKOUBI, S., TJOA, S. e MUCK, T., *Integration of an Ontological Information Security Concept in Risk-Aware Business Process Management*, Proc IEEE HICSS, IEEE Press, Jan 2008, pp 1-9.

[26] CHA, S., LIU, L. e YU, B., *Process-Oriented Approach for Validating Asset Value for Evaluating Information Security Risk*, Proc IEEE CSE , IEEE Press, Aug 2009, pp 379-385.

[27] SAMY, G. N., AHMAD, R. e ISMAIL Z., *A framework for integrated Risk Management Process using Survival Analysis Approach in Information Security*, Proc IEEE ICIAS, IEEE Press, Aug 2010, pp 185-190.

[28] KHIDZIR, N. Z., MOHAMED, A. e ARSHAD, N. H. H., *Information Security Risk Management: An Empirical Study on the Difficulties and Practices in ICT Outsourcing*, Proc IEEE ICNAPS, IEEE Press, Sept 2010, pp 234-239.

[29] SIPONEN, M., PAHNILA, S. e MAHMOOD, M. A., *Compliance with Information Security Policies: An Empirical Investigation*, Proc IEEE Computer v43, IEEE Press, Feb 2010, pp 64-71.

[30] SENGUNPTA, A., MAZUMDAR, C. e BAGCHI, A., *A Methodology for Conversion of Enterprise-Level Information Security Policies to Implementation-Level Policies/Rule*, Proc IEEE ICEAIT, IEEE Press, 2011, pp 280-283.

[31] HOSSEINBEIG, S., MOGHADAM, D. K., VAHDAT, D. e MOGHADAM, R. A., *IT Strategic Alignment Maturity and IT Governance*, Proc IEEE ICIS, IEEE Press 2011, pp 67-72.

[32] ELAGHA, H., *The Use of Partial Least Squares Path Modeling in IT Governance Discipline*, Proc IEEE ICIT, IEEE Press 2014, pp 624 - 626.

[33] ZHU, D. e LI, F., *The IT Governance: Operating Model and Governance Framework: Methodology and Practice in Group-wide Corporation*, Proc IEEE ICMeCG, IEEE Press 2014, pp 291-294.

[34] MAHARDIKO, R., *IT Value Analysis: Case Study of PT. Express Transindo Utama*, Proc IEEE ICITSI, IEEE Press 2014, pp 224-229.

[35] HUNTER, R. e WESTERMAN, G., O Verdadeiro Valor de TI, M.Books, Press, 2011.

[36] BARTENS, Y., HAES, S., LAMOEN, Y., SCHULTE, F. e VOSS, S., *On the Way to a Minimum Baseline in IT Governance: Using Expert Views for Selective Implementation of COBIT 5*, Proc IEEE HICSS, IEEE Press 2015, pp 4554 - 4563.

[37] YOUSSFI, K., BUTAHAR, J. e ELGHAZI, S., *IT Governance Implementation: A Tool design of COBIT 5 Roadmap,* Proc IEEE WCCS, IEEE Press 2014, pp 115 - 121.

[38] COBIT 5, Modelo Corporativo para Governança de TI da Organização, ISACA. Disponível em: http://www.isaca.org.

[39] CIS, *The CIS Critical Security Controls for Effective Cyber Defense,* Version 6.0, October 2015.

[40] FERREIRA, L. N., CONSTANTE, S. M. S., ZEBRAL, A. M. M., BRAGA, R. Z., ALVARENGA, H. e FERREIRA, S. N., *ISO 27001certification process of eletronic invoice in the State of Minas Gerais, Proc IEEE ICCST, IEEE Press 2013, pp 1-4.*

[41] SHOJAIE, B., FEDERRATH, H. e SABERI, I., *The Effects of Cultural Dimensions on the Development of an ISMS Based on the ISO 27001*, Proc IEEE ICARS, IEEE Press 2015, pp 159 - 167.

[42] ISO/IEC, Tecnologia da informação - Técnicas de segurança – Sistemas de gestão de segurança da informação - Requisitos. ISO/IEC. 1ed. 2006.

[43] ALEBRAHIM, A., HATEBUR, D. e GOEKE, L., *Pattern-Based and ISO 27001 Compliant Risk Analysis for Claoud Systems*, Proc ESPRE, IEEE Press 2014, pp 42 - 47.

[44] SAHIBUDIN, S., SHARIFI, M. e AYAT, M., *Combining ITIL, COBIT and ISO/27002 in Order to Design a Comprehensive IT Framework in Organizations,* Proc AICMS, IEEE Press 2008, pp 749 - 753.

[45] ISO/IEC, Tecnologia da informação - Técnicas de segurança – Código de prática para a gestão da segurança da informação. ISO/IEC. 1ed. 2005.

[46] FONTES, E., Políticas e normas para segurança da informação, Brasport, Press, 2012.

[47] SUN, J. e CHEN, Y., *Intelligent Enterprise Information Security Architecture Based on Service Oriented Architecture,* Proc IEEE, IEEE Press 2008, pp 196 - 200.

[48] WOODHOUSE, S., *An ISMS (IM)-Maturity Capability Model,* Proc IEEE ICCITW, IEEE Press 2008, pp 242 - 247.

[49] MAYER, J. e FAGUNDES, L.L., *A Model to Assess the Maturity Level of the Risk Management Process in Information Security,* Proc IEEE IFIP, IEEE Press 2009, pp 61-70.

[50] REGULWAR, G.B., GULHANE, V.S. e JAWANDHIYA, P.M., *A Security Engineering Capability Maturity Model*, Proc IEEE ICEIT, IEEE Press 2010, pp 61-70.

[51] STAMBUL, M. A. M. e RAZALI, R., *An Assessment Model of Information Security Implementation Levels*, Proc IEEE ICEEI, IEEE Press 2011, pp 1-6.

[52] KASSOU, M. e KJIRI, L., *SOASMM: A novel oriented architecture Security Maturity Model,* Proc IEEE ICMCS, IEEE Press 2012, pp 912-918.

[53] ZHAO, W. e WHITE, G., *A collaborative information sharing framework for Community Cyber Security,* ICTHS, IEEE Press 2012, pp 457 - 462.

APÊNDICES

QUESTIONÁRIO DE AVALIAÇÃO DIAGNÓSTICA

Questionário: Nível de Segurança da Informação.

Descrição: Questionário para identificar e auxiliar na implantação de níveis de maturidade em segurança da informação, com a finalidade de auxiliar os diretores de TI para um aumento na qualidade da segurança da informação.

Dados da Organização

1. **Acordo de Confidencialidade**
2. **Nome da Empresa**

Questões

1. Existe uma política de troca de *Hardware*?		
Alternativa		**FM**
A	Sim.	3
B	Parcial.	1
D	Não.	-3

Área	**Justificativa**	**Peso**
GAIA-MLIS *Hardware*	A existência da política afeta diretamente a área.	4
GAIA-MLIS *Software*	A existência da política influencia a área.	3
GAIA-MLIS Instalações/Espaços Físicos	A existência da política afeta indiretamente a área.	1
GAIA-MLIS Pessoas	A existência da política influencia nas pessoas/funcionários.	3
GAIA-MLIS Informação	A existência da política afeta diretamente a área.	4

2. Existe uma política de manutenção em *Hardware*?		
Alternativa		**FM**
A	Sim.	3
B	Parcial.	1
C	Não.	-3

Área	Justificativa	Peso
GAIA-MLIS *Hardware*	A existência de processos afeta a área de *hardware*.	4
GAIA-MLIS *Software*	A existência do processo afeta diretamente a área.	3
GAIA-MLIS Instalações/Espaços Físicos	A existência do processo afeta indiretamente a área.	1
GAIA-MLIS Pessoas	A existência do processo afeta a área.	3
GAIA-MLIS Informação	A existência do processo afeta diretamente a área.	4

3. Há uma política de segurança para os equipamentos de informática?		
Alternativa		**FM**
A	Sim.	3
B	Parcial.	1
C	Não.	-3

Área	Justificativa	Peso
GAIA-MLIS *Hardware*	A existência da política influencia diretamente a área.	4
GAIA-MLIS *Software*	A existência da política influencia a área.	3
GAIA-MLIS Instalações/Espaços Físicos	A existência da política influencia indiretamente a área.	1
GAIA-MLIS Pessoas	A existência da política influencia a área.	3
GAIA-MLIS Informação	A existência da política afeta diretamente a área.	4

4. Há antivirus nos computadores da empresa?		
Alternativa		**FM**
A	Sim. Antivirus pago.	3
B	Sim. Antivirus gratuito.	1
C	Não.	-3

Área	Justificativa	Peso
GAIA-MLIS *Hardware*	A existência da política afeta indiretemente a área.	1
GAIA-MLIS *Software*	A existência da política afeta diretemente a área.	4
GAIA-MLIS Instalações/Espaços Físicos	Não há impacto.	0
GAIA-MLIS Pessoas	Não há impacto.	0
GAIA-MLIS Informação	A existência da política afeta diretemente a área.	4

5. Há firewall instalado na servidor da empresa?		
Alternativa		**FM**
A	Sim. Possui firewall instalado no servidor.	3
B	Sim. Possui firewall instalado em cada computador	1
C	Não.	-3

Área	Justificativa	Peso
GAIA-MLIS *Hardware*	A existência da política afeta a área.	3
GAIA-MLIS *Software*	A existência do política afeta diretamente a área.	4
GAIA-MLIS Instalações/Espaços Físicos	Não há impacto.	0

GAIA-MLIS Pessoas	Não há impacto.	0
GAIA-MLIS Informação	A existência da política afeta diretamente a área.	4

6. Existe uma política de atualização dos *softwares*?		
Alternativa		**FM**
A	Sim.	3
B	Parcial.	1
C	Não.	-3

Área	Justificativa	Peso
GAIA-MLIS *Hardware*	A existência da política influencia indiretamente a área.	1
GAIA-MLIS *Software*	A existência da política influencia diretamente a área.	4
GAIA-MLIS Instalações/Espaços Físicos	Não há impacto.	0
GAIA-MLIS Pessoas	A existência da política influencia a área.	3
GAIA-MLIS Informação	A existência da política influencia indiretamente a área.	4

7. Os *softwares* utilizados são originais?		
Alternativa		**FM**
A	Sim.	3
B	Não.	-3

Área	Justificativa	Peso
GAIA-MLIS *Hardware*	Não há impacto.	0
GAIA-MLIS *Software*	A política afeta diretamente a área.	4
GAIA-MLIS Instalações/Espaços Físicos	Não há impacto.	0
GAIA-MLIS Pessoas	A política afeta a área.	2
GAIA-MLIS Informação	A política afeta diretamente a área.	4

8. Existe uma política de segurança para instalação e manutenção de *software* na empresa?		
Alternativa		**FM**
A	Sim.	3
B	Parcial.	1
C	Não.	-3

Área	Justificativa	Peso
GAIA-MLIS *Hardware*	Não há impacto.	0
GAIA-MLIS *Software*	A existência da política influencia diretamente a área.	4
GAIA-MLIS Instalações/Espaços Físicos	Não há impacto.	0
GAIA-MLIS Pessoas	A existência da política influencia a área.	3
GAIA-MLIS Informação	A existência da política influencia diretamente a área.	4

9. As falhas nos *softwares* são documentadas?		
Alternativa		**FM**
A	Sim.	3
B	Parcialmente.	1
C	Não.	-3

Área	Justificativa	Peso
GAIA-MLIS *Hardware*	Não há impacto.	0
GAIA-MLIS *Software*	A política afeta diretamente a área.	4
GAIA-MLIS Instalações/Espaços Físicos	Não há impacto.	0
GAIA-MLIS Pessoas	A política afeta a área.	2
GAIA-MLIS Informação	A política afeta diretamente a área.	4

10. Os servidores de rede ficam em ambiente seguro e com controle de acesso?		
Alternativa		**FM**
A	Sim.	3
B	Não.	-3

Área	Justificativa	Peso
GAIA-MLIS *Hardware*	O ambiente seguro e com controle de acesso afeta a área.	3
GAIA-MLIS *Software*	O ambiente seguro e com controle de acesso afeta a área.	2
GAIA-MLIS Instalações/Espaços Físicos	O ambiente seguro e com controle de acesso afeta diretamente a área.	4
GAIA-MLIS Pessoas	O ambiente seguro e com controle de acesso afeta a área.	3
GAIA-MLIS Informação	O ambiente seguro e com controle de acesso afeta diretamente a área.	4

11. Há uma política de controle de acesso nas instalações?		
Alternativa		**FM**
A	Sim.	3
B	Parcialmente.	1
C	Não.	-3

Área	Justificativa	Peso
GAIA-MLIS *Hardware*	A política de controle de acesso afeta a área.	3
GAIA-MLIS *Software*	A política de controle de acesso afeta indiretamente a área.	1
GAIA-MLIS Instalações/Espaços Físicos	A política de controle de acesso afeta diretamente a área.	4
GAIA-MLIS Pessoas	A política de controle de acesso afeta a área.	3
GAIA-MLIS Informação	A política de controle de acesso afeta a diretamente área.	4

12. Os ativos de redes ficam em lugares controlados e monitorados?		
Alternativa		**FM**
A	Sim.	3
B	Parcial.	1
C	Não.	-3

Área	Justificativa	Peso
GAIA-MLIS *Hardware*	Os ativos de redes em lugares controlados e monitorados afetam a área.	3
GAIA-MLIS *Software*	Os ativos de redes em lugares controlados e monitorados afetam a área.	2
GAIA-MLIS Instalações/Espaços Físicos	Os ativos de redes em lugares controlados e monitorados afetam diretamente a área.	4
GAIA-MLIS Pessoas	Os ativos de redes em lugares controlados e monitorados afetam a área.	3
GAIA-MLIS Informação	Os ativos de redes em lugares controlados e monitorados afetam diretamente a área.	4

13. As instalações físicas são monitoradas por câmeras e alarmes?		
Alternativa		**FM**
A	Sim.	3
C	Parcial.	1
D	Não.	-3

Área	Justificativa	Peso
GAIA-MLIS *Hardware*	O monitoramento por câmeras e alarmes afetam a área.	3
GAIA-MLIS *Software*	Não há impacto.	0
GAIA-MLIS Instalações/Espaços Físicos	O monitoramento por câmeras e alarmes afetam diretamente a área.	4
GAIA-MLIS Pessoas	O monitoramento por câmeras e alarmes afetam a área.	3
GAIA-MLIS Informação	O monitoramento por câmeras e alarmes afetam diretamente a área.	4

14. Equipe de infraestrutura de TI está preparada para um caso de contingência de evento de segurança da informação?		
Alternativa		**FM**
A	Existe equipe de infraestrutura de TI e possui plano de contingência.	3
B	Existe equipe de infraestrutura de TI, mas não há preparo.	1
C	Não.	-3

Área	Justificativa	Peso
GAIA-MLIS *Hardware*	A equipe de infraestrutura de TI afeta a área.	2
GAIA-MLIS *Software*	A equipe de infraestrutura de TI afeta a área.	2

GAIA-MLIS Instalações/Espaços Físicos	A equipe de infraestrutura de TI afeta a área.	2
GAIA-MLIS Pessoas	A equipe de infraestrutura de TI afeta diretamente a área.	4
GAIA-MLIS Informação	A equipe de infraestrutura de TI afeta diretamente a área.	4

15. Existe uma política de segurança da informação e ela é divulgada para os seus funcionários?		
Alternativa		**FM**
A	Sim.	3
B	Parcial.	1
C	Não.	-3

Área	Justificativa	Peso
GAIA-MLIS *Hardware*	A existência da política afeta diretamente a área.	4
GAIA-MLIS *Software*	A existência da política afeta diretamente a área.	4
GAIA-MLIS Instalações/Espaços Físicos	A existência da política afeta diretamente a área.	4
GAIA-MLIS Pessoas	A existência da política afeta diretamente a área.	4
GAIA-MLIS Informação	A existência da política afeta diretamente a área.	4

16. Os funcionários recebem treinamentos sobre segurança da informação?		
Alternativa		**FM**
A	Semestral.	3
B	Anual.	1
C	Não.	-3

Área	Justificativa	Peso
GAIA-MLIS *Hardware*	Os treinamentos sobre segurança da informação afeta a área.	3
GAIA-MLIS *Software*	Os treinamentos sobre segurança da informação afeta a área.	3
GAIA-MLIS Instalações/Espaços Físicos	Os treinamentos sobre segurança da informação afeta a área.	3
GAIA-MLIS Pessoas	Os treinamentos sobre segurança da informação afeta diretamente a área.	4
GAIA-MLIS Informação	Os treinamentos sobre segurança da informação afeta diretamente a área.	4

17. Os funcionários são avaliados em relação aos treinamentos?		
Alternativa		**FM**
A	Semestral.	3
B	Anual.	1
C	Não.	-3

Área	Justificativa	Peso
GAIA-MLIS *Hardware*	Não há impacto.	0
GAIA-MLIS *Software*	A avaliação afeta a área.	3
GAIA-MLIS Instalações/Espaços Físicos	Não há impacto.	0
GAIA-MLIS Pessoas	A avaliação afeta diretamente a área.	4
GAIA-MLIS Informação	A avaliação afeta diretamente a área.	4

18. Existe política de *backup* para as informações?		
Alternativa		**FM**
A	Sim.	3
B	Parcial.	1
C	Não.	-3

Área	Justificativa	Peso
GAIA-MLIS *Hardware*	A política afeta a área.	3
GAIA-MLIS *Software*	A política afeta diretamente a área.	4
GAIA-MLIS Instalações/Espaços Físicos	A política afeta a área.	3
GAIA-MLIS Pessoas	A política afeta a área.	3
GAIA-MLIS Informação	A política afeta diretamente a área.	4

19. Existe redundância dos servidores de rede na empresa?		
Alternativa		**FM**
A	Sim.	3
B	Não.	-3

Área	Justificativa	Peso
GAIA-MLIS *Hardware*	A redundância dos servidores de rede afeta a área.	3
GAIA-MLIS *Software*	A redundância dos servidores de rede afeta diretamente a área.	4
GAIA-MLIS Instalações/Espaços Físicos	Não há impacto.	0
GAIA-MLIS Pessoas	A redundância dos servidores de rede afeta a área.	3
GAIA-MLIS Informação	A redundância dos servidores de rede afeta diretamente a área.	4

20. As informações dos sistemas são criptografadas?		
Alternativa		**FM**
A	Sim.	3
B	Parcial.	1
C	Não.	-3

Área	Justificativa	Peso
GAIA-MLIS *Hardware*	A criptografia das informaões afeta indiretamente a área.	1
GAIA-MLIS *Software*	A criptografia das informaões afeta diretamente a área.	4
GAIA-MLIS Instalações/Espaços Físicos	Não há impacto.	0
GAIA-MLIS Pessoas	A criptografia das informaões afeta diretamente a área.	4
GAIA-MLIS Informação	A criptografia das informaões afeta diretamente a área.	4

21. Os *backup*s são armazenados em lugares separados?		
Alternativa		**FM**
A	Sim.	3
B	Não.	-3

Área	Justificativa	Peso
GAIA-MLIS *Hardware*	O armazenamento em local separado afeta a área.	3
GAIA-MLIS *Software*	O armazenamento em local separado afeta a área.	3
GAIA-MLIS Instalações/Espaços Físicos	O armazenamento em local separado afeta diretamente a área.	4
GAIA-MLIS Pessoas	O armazenamento em local separado afeta diretamente a área.	4
GAIA-MLIS Informação	O armazenamento em local separado afeta diretamente a área.	4

22. Existe uma política tecnológica das mídias de armazenamento de *backup*?		
Alternativa		**FM**
A	Sim.	3
B	Não.	-3

Área	Justificativa	Peso
GAIA-MLIS *Hardware*	A política tecnológica afeta diretamente a área.	4
GAIA-MLIS *Software*	A política tecnológica afeta a área.	3
GAIA-MLIS Instalações/Espaços Físicos	Não há impacto.	0
GAIA-MLIS Pessoas	A política tecnológica afeta diretamente a área.	3
GAIA-MLIS Informação	A política tecnológica afeta diretamente a área.	4

23. Existe uma política de controle de acesso da informação com base no perfil de cada funcionário?		
Alternativa		**FM**
A	Sim.	3
B	Parcial.	1
C	Não.	-3

Área	Justificativa	Peso
GAIA-MLIS *Hardware*	A política afeta diretamente a área.	4
GAIA-MLIS *Software*	A política afeta diretamente a área.	4
GAIA-MLIS Instalações/Espaços Físicos	A política afeta diretamente a área.	4
GAIA-MLIS Pessoas	A política afeta diretamente a área.	4
GAIA-MLIS Informação	A política afeta diretamente a área.	4

24. Existe um sistema de avaliação diagnóstica em segurança da informação?		
Alternativa		**FM**
A	Sim.	3
B	Não.	-3

Área	Justificativa	Peso
GAIA-MLIS *Hardware*	O sistema de avaliação diagnóstica afeta diretamente a área.	4
GAIA-MLIS *Software*	O sistema de avaliação diagnóstica afeta diretamente a área.	4
GAIA-MLIS Instalações/Espaços Físicos	O sistema de avaliação diagnóstica afeta diretamente a área.	4
GAIA-MLIS Pessoas	O sistema de avaliação diagnóstica afeta diretamente a área.	4
GAIA-MLIS Informação	O sistema de avaliação diagnóstica afeta diretamente a área.	4

Trabalhos publicados pelo Autor

1. COÊLHO, Roger W.; FERNANDES JUNIOR, G; PROENÇA JR, Mario Lemes. **GAIA-MLIS: A Maturity Model for Information Security**. In: The Eighth International Conference on Emerging Security Information Systems and Technologies, 2014, Lisbon. Proceeding of SECURWARE, 2014. **(Qualis B3, Conferência CC, 2012)**.