VALDECI OTACILIO DOS SANTOS

"UM MODELO DE SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO BASEADO NAS NORMAS ABNT NBR ISO/IEC 27001:2006, 27002:2005 E 27005:2008"

CAMPINAS

2012

UNIVERSIDADE ESTADUAL DE CAMPINAS

FACULDADE DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO

VALDECI OTACILIO DOS SANTOS

"UM MODELO DE SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO BASEADO NAS NORMAS ABNT NBR ISO/IEC 27001:2006, 27002:2005 E 27005:2008"

Dissertação de Mestrado apresentada à Faculdade de Engenharia Elétrica e de Computação, como parte dos requisitos para a obtenção do título de Mestre em Engenharia Elétrica. Área de concentração: Telecomunicações e Telemática.

ORIENTADOR: PROF. DR. RENATO BALDINI FILHO

Este exemplar corresponde à versão final da Dissertação defendida pelo aluno Valdeci Otacilio dos Santos, e orientada pelo Prof. Dr. Renato Baldini Filho.

CAMPINAS

2012

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA E ARQUITETURA - BAE - UNICAMP

Santos, Valdeci Otacilio dos
Sa59m Um modelo de sistema de gestão da segurança da informação baseado nas normas ABNT NBR ISO/IEC 27001:2006, 27002:2005 e 27005:2008 / Valdeci Otacilio dos Santos. --Campinas, SP: [s.n.], 2012.

Orientador: Renato Baldini Filho.
Dissertação de Mestrado - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Informação. 2. Tecnologia da informação - Segurança. 3. Redes de informação. 4. Serviços de informação. I. Baldini Filho, Renato. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. III. Título.

Título em Inglês: A model of information security management system based in the NBR ISO/IEC 27001:2006, 27002:2005 e 27005:2008 ABNT standards
Palavras-chave em Inglês: Information, Information technology - Security, Information networks, Information services
Área de concentração: Telecomunicações e Telemática
Titulação: Mestre em Engenharia Elétrica
Banca examinadora: Luciano Leonel Mendes, Renato da Rocha Lopes
Data da defesa: 13-11-2012
Programa de Pós Graduação: Engenharia Elétrica

COMISSÃO JULGADORA - TESE DE MESTRADO

Candidato: Valdeci Otacilio dos Santos

Data da Defesa: 13 de novembro de 2012

Título da Tese: "Um Modelo de Sistema de Gestão da Segurança da Informação Baseado nas Normas ABNT NBR ISO/IEC 27001:2006, 27002:2005 e 27005:2008"

Prof. Dr. Renato Baldini Filho (Presidente): _____

Prof. Dr. Luciano Leonel Mendes: _____

Prof. Dr. Renato da Rocha Lopes: _____

Agradecimentos

Ao Professor Doutor Renato Baldini Filho, meu orientador, pela atenção dispensada e pela confiança em mim depositada.

Ao Professor Doutor Marco Aurélio Amaral Henriques, pelos conhecimentos e orientações.

À minha esposa Rita e meus filhos Caroline e Lucas, pelo apoio e compreensão.

Resumo

O crescimento constante de ameaças e vulnerabilidades nos sistemas de informação faz com que a preocupação por parte dos administradores sobre a segurança desses sistemas também seja intensificada. Na busca de um nível adequado de segurança da informação, estão sendo criadas e aperfeiçoadas, não somente no Brasil, mas em escala mundial, legislações e normatizações que tratam sobre esse tema tão importante nos dias atuais. Este trabalho tem como objetivo propor um modelo de sistema de gestão da segurança da informação, com modelagem de processos e descrição das atividades, que contemple as principais diretrizes preconizadas nas normas ABNT NBR ISO/IEC 27001:2006, 27002:2005 e 27005:2008. O modelo proposto visa guiar a implementação de um novo sistema de gestão da segurança da informação em uma organização ou verificar a conformidade de um sistema já existente. O trabalho compreende uma aplicação prática do modelo proposto, em que foi executado um levantamento do nível de aderência das atividades desenvolvidas nos diversos processos que compõem um sistema de gestão da segurança da informação de uma organização, com o que está previsto no modelo e, consequentemente, nas normas utilizadas como referência. Na avaliação dos resultados da verificação realizada foi possível obter uma visão geral da situação em que se encontra a gestão da segurança da informação da organização, bem como a verificação dos pontos que estão de acordo com a normatização e daqueles que necessitam aprimoramentos.

Palavras-chave: Informação. Segurança da informação. Gestão da segurança da informação.

Abstract

The steady growth of threats and vulnerabilities in the information systems causes an intensified concern among administrators about the security of these systems. In search of an appropriate level of information security are being created and improved, not only in Brazil but worldwide, laws and regulations that deal with this important issue. This work aims to propose a model of information security management system with process modeling and description of activities, covering the main guidelines recommended in the standards ABNT NBR ISO/IEC 27001:2006, 27002:2005 e 27005:2008. The proposed model aims to guide the implementation of a new system for managing information security in an organization or verify the conformity of an existing system. The work includes a practical application of the proposed model, that was carried out a survey on the level of activities adhesion in the various processes that comprise a information security management system within an organization, what is envisaged in the model and consequently, the standards used as reference. In assessing the results of the verification carried out was possible to obtain an overview of the situation in which the information security management system of the organization is, as well as the verification of the points that are in accordance with norms and those that need improvement.

Keywords: Information. Information security. Information security management.

Sumário

Lista de Figuras

Lista de Tabelas

Glossário

ABNT – Associação Brasileira de Normas Técnicas

BS – *British Standard*

BSI - *British Standard Institute*

COBIT – *Control Objectives for Information and Related Technology*

ETIR – Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais

GRSI – Gestão de Riscos de Segurança da Informação

IEC – *International Electrotechnical Commission*

ISO – *International Organization for Standardization*

ITGI – *Information Technology Governance Institute*

ITIL - *Information Technology Infrastructure Library*

NBR – Norma Brasileira

PCCSI – Programa Corporativo de Conscientização em Segurança da Informação

PDCA – *Plan - Do - Check – Act*

SGSI – Sistema de Gestão da Segurança da Informação

TI – Tecnologia da Informação

Capítulo 1

Introdução

1.1 Considerações Gerais

A informação constitui um bem de grande valor para a sociedade como um todo e, em particular, para as organizações públicas ou privadas. Devido à sua importância e ao crescimento das ameaças e vulnerabilidades nos sistemas de informação, surge a necessidade de adoção de medidas de proteção eficientes.

A segurança da informação é entendida como a preservação das propriedades de disponibilidade, integridade, confidencialidade, autenticidade, responsabilidade, não repúdio e confiabilidade da informação (ABNT, 2006, p. 2).

Segundo a ABNT (2005, p. 2), a segurança da informação protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar o risco aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio.

Conforme descrito em Brasil (2001, p. 4), a segurança da informação compreende um conjunto de medidas, normas e procedimentos destinados a proteger a informação em todo o seu ciclo de utilidade.

Para garantir a proteção da informação contra as ameaças existentes, tornam-se necessários o estabelecimento e a implementação de políticas, processos e procedimentos que

sejam, respectivamente, um conjunto de diretrizes, ações e instruções, que compreendem a chamada gestão da segurança da informação organizacional.

1.2 Motivação

Existem atualmente várias normas nacionais e internacionais que tratam da segurança da informação. Essas normas visam nortear as atividades a serem realizadas a fim de tornarem os sistemas de informação mais seguros. Em particular, destacamos as normas ISO/IEC da família 27000, que são padrões internacionais publicados pela *International Organization for Standardization* (ISO) e possuem suas versões brasileiras publicadas pela Associação Brasileira de Normas Técnicas (ABNT).

As diversas normas que compõem a família ISO/IEC 27000 abordam os vários enfoques voltados à segurança da informação de maneira particular, embora haja uma forte relação entre cada norma.

A velocidade do avanço tecnológico na área da informação e comunicações faz com que os requisitos de segurança da informação e comunicações organizacionais sejam muito dinâmicos, o que exige um acompanhamento e aprimoramento constante das políticas, processos e procedimentos de segurança. Nesse sentido, a criação de um mecanismo que consolide as orientações e abordagens contempladas nas principais normas e facilite o entendimento da constituição e relacionamentos existentes entre os diversos processos que são desenvolvidos com o objetivo alcançar um nível de segurança adequado contribuirá para que as organizações implementem ou verifiquem os seus sistemas de gestão da segurança da informação (SGSI) com menores custos, menor tempo e maior eficiência e eficácia.

1.3 Objetivos

O objetivo deste trabalho é propor um modelo de sistema de gestão da segurança da informação (SGSI), com mapeamento dos processos e descrição das atividades a serem realizadas, baseado nas normas ABNT NBR ISO/IEC 27001 (ABNT, 2006), 27002 (ABNT, 2005) e 27005 (ABNT, 2008). O modelo consolida as orientações previstas nas normas mencionadas anteriormente e fornece uma explicação sobre o conteúdo dos processos que

compõem o sistema de gestão da segurança da informação, bem como a interação existente entre eles.

A finalidade é constituir um guia prático de orientação, que possibilite a uma organização implementar ou averiguar a situação em que se encontra seu sistema de gestão da segurança da informação, em conformidade com as principais normas existentes.

1.4 Organização do Trabalho

Este trabalho está organizado em capítulos, conforme abaixo descrito:

No capítulo 1 é realizada uma introdução ao assunto com as considerações gerais, a motivação para realização do trabalho, os objetivos e a organização da dissertação.

O capítulo 2 apresenta os fundamentos conceituais, compondo um referencial teórico sobre os diversos assuntos relacionados à gestão da segurança da informação que serão abordados ao longo do trabalho.

O conteúdo do capítulo 3 refere-se ao modelo de sistema de gestão da segurança da informação proposto, contemplando a descrição das atividades a serem realizadas em cada processo do sistema.

No capítulo 4 é apresentado o resultado da aplicação prática do modelo proposto, em que foi verificado o nível de conformidade do sistema de gestão da segurança da informação de uma organização, em relação às normas tomadas como base para confecção do modelo.

O capítulo 5 apresenta a conclusão da dissertação e sugestões para trabalhos futuros.

Capítulo 2

Fundamentos Conceituais

2.1 Gestão da Segurança da Informação

A grande maioria das organizações atuais possui todos os seus processos baseados ou suportados por sistemas digitais de informação. Para que esses sistemas funcionem adequadamente, de modo a propiciar um serviço confiável e de qualidade aos seus clientes, torna-se necessária uma perfeita gestão da segurança da informação e comunicação, visando alinhá-la aos objetivos de negócio da organização.

Conforme descrito em Brasil (2008, p. 2), a gestão da segurança da informação e comunicações é entendida como: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações.

Segundo a ABNT (2006, p. 1), o sistema de gerenciamento da segurança da informação é projetado para assegurar a seleção de controles de segurança adequados para proteger os ativos de informação da organização.

Para Veneziano (2010, p. 7), um sistema de informação pode ser entendido como um conjunto de elementos inter-relacionados que coletam, processam, armazenam e disseminam

dados e informações.

Desta forma, determinados sistemas de informação possuem importância fundamental na consecução dos objetivos de negócio da organização e, consequentemente, para a sua sobrevivência ao longo do tempo. Portanto, tais sistemas de informação devem ser dotados de um nível de segurança que seja adequado às características e objetivos de negócio da organização.

Existe, atualmente, uma variedade de normas e legislação que norteiam o gerenciamento da segurança da informação e comunicações. A Tabela 2.1, abaixo, lista algumas normas técnicas relevantes relacionadas à segurança da informação e comunicações.

Tabela 2.1 – Nomas Técnicas sobre Segurança da Informação e Comunicações.

NORMA	TÍTULO
ABNT NBR ISO/IEC 27001:2006	Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos (ABNT, 2006)
ABNT NBR ISO/IEC 27002:2005	Tecnologia da informação - Técnicas de segurança - Código de pratica para a gestão de segurança da informação (ABNT, 2005)
ABNT NBR ISO/IEC 27004:2010	Tecnologia da informação - Técnicas de segurança - Gestão da segurança da informação - Medição (ABNT, 2010)
ABNT NBR ISO/IEC 27005:2008	Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação (ABNT, 2008)
ABNT NBR ISO/IEC 27011:2009	Tecnologia da informação - Técnicas de segurança - Diretrizes para gestão da segurança da informação para organizações de telecomunicações baseadas na ABNT NBR ISO/IEC 27002 (ABNT, 2009)
ABNT NBR ISO/IEC 27003:2011	Tecnologia da informação - Técnicas de segurança - Diretrizes para implantação de um sistema de gestão da segurança da informação (ABNT, 2011)

2.1.1 A Norma ABNT NBR ISO/IEC 27001:2006

A norma ABNT 27001 (ABNT, 2006) é uma evolução da norma BS 7799-2, que foi publicada pelo BSI (*British Standard Institute*) em 1999. Ela fornece um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). Essa norma utiliza o modelo "*Plan-Do-Check-Act*" (PDCA), que é aplicado na estruturação de processos de melhoria contínua. A Figura 2.1 ilustra o modelo PDCA e a Tabela 2.2 descreve os estágios do ciclo de tal modelo com suas respectivas

atividades.

Figura 2.1 – Modelo PDCA. Fonte: o autor, adaptação de Rocha, R. (2010).

Tabela 2.2 – Ciclo do modelo PDCA aplicado ao SGSI.

ESTÁGIO	**ATIVIDADES**
Plan (P) Planejar	Planejamento das ações de segurança a serem desenvolvidas, de acordo com as características, objetivos e requisitos da organização. Incluem o estabelecimento de políticas, processos e procedimentos de segurança, objetivos a serem alcançados e gestão de riscos.
Do (D) Fazer	Implementação das ações de segurança planejadas no estágio anterior.
Check (C) Verificar	Avaliação das ações de segurança implementadas e análise crítica dos resultados alcançados.
Act (A) Agir	Aperfeiçoamento das ações de segurança, de acordo com o monitoramento realizado ou novas informações obtidas, de modo que seja alcançada a melhoria contínua do sistema.

2.1.2 A Norma ABNT NBR ISO/IEC 27002:2005

A norma ABNT 27002 (ABNT, 2005) integra o conjunto de normas ISO/IEC 27000, voltadas para a gestão da segurança da informação. Essa norma teve origem na BS 7799-1, publicada pelo BSI (*British Standard Institute*) em 1995, que em 2000 tornou-se a norma ISO 17799. A norma 27002 estabelece um conjunto de controles, com as respectivas diretrizes de implementação, visando à gestão da segurança da informação. Os diversos controles sugeridos pela norma estão ordenados em onze seções descritas a seguir:

- Política de Segurança da Informação;
- Organizando a Segurança da Informação;
- Gestão de Ativos;
- Segurança em Recursos Humanos;
- Segurança Física e do Ambiente;
- Gestão das Operações e Comunicações;
- Controle de Acesso;
- Aquisição, Desenvolvimento e Manutenção dos Sistemas de Informação;
- Gestão de Incidentes de Segurança da Informação;
- Gestão da Continuidade do Negócio;
- Conformidade.

2.2 Infraestrutura de Tecnologia da Informação

Os processos que constituem os diversos sistemas de uma organização tornam-se cada vez mais dependentes dos recursos computacionais. Dessa forma, torna-se inevitável uma discussão sobre o tema denominado governança de TI (Tecnologia da Informação), uma vez que este tema tornou-se imprescindível na consecução dos objetivos estratégicos das organizações modernas.

É por meio da infraestrutura de TI que são disponibilizadas aos gestores grande parte das informações necessárias à tomada de decisão. Segundo Fagundes (2011), a criação e manutenção

de uma infraestrutura de TI requerem altos investimentos, mas pode ser um fator chave para o fracasso ou sucesso de um empreendimento.

A governança de TI destina-se ao alinhamento da infraestrutura de TI com os objetivos de negócio da organização. O *Control Objectives for Information and related Technology* (COBIT) e *Information Technology Infrastructure Library* (ITIL) são exemplos de *frameworks* que permitem o gerenciamento da infraestrutura de TI.

Uma das premissas para a implementação de um SGSI é o conhecimento da infraestrutura de TI da organização, pois essa infraestrutura exerce um papel relevante na gestão dos riscos de segurança da informação e, consequentemente, na determinação dos requisitos de segurança da informação da organização.

Como exemplo de elementos que compõem a infraestrutura de TI podemos citar as instalações prediais (com sistema de energia e climatização), *hardwares* (computadores, equipamentos de rede, de telecomunicações e outros equipamentos relacionados) e *softwares*.

2.3 Política de Segurança da Informação

A política de segurança da informação estabelece as diretrizes e atribui responsabilidades pela segurança da informação na organização. Para Silva, R. (2010, p. 1), política de segurança da informação é basicamente um manual de procedimentos que descreve como os recursos de TI da empresa devem ser protegidos e utilizados e é o pilar da eficácia da segurança da informação.

O estabelecimento de uma política de segurança da informação se constitui numa atitude essencial a fim de que se desenvolvam as ações de segurança da informação, já que ela visa normatizar processos e procedimentos para este fim. Segundo Neto, J. (2010, p. 19), a política de segurança da informação é a fundação da segurança de informação de uma organização. Uma política adequada e efetiva contém a orientação suficiente sobre o que deve ser feito para proteger a informação e as pessoas de uma organização.

A Norma ABNT 27002 estabelece que o objetivo da política de segurança da informação é prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes (ABNT, 2005, p. 8).

As etapas que envolvem o processo de implantação de uma política de segurança da

informação, segundo Neto, J. (2010, p. 19), são descritas na Tabela 2.3.

Tabela 2.3 – Etapas do processo de implantação da política de segurança da informação.

ETAPA	DESCRIÇÃO
Desenvolvimento	Definição dos requisitos corporativos e estabelecimento dos padrões para a documentação da política.
Aprovação	Gerenciamento da transição desde a identificação das necessidades da política até a obtenção da autorização pela direção da organização.
Implementação	Solicitação e recebimento de apoio executivo, com envolvimento das diversas áreas do negócio, e desenvolvimento de um programa de conscientização corporativa.
Conformidade	Avaliação da conformidade e eficácia da política estabelecida, com ações corretivas.
Manutenção	Condução de revisões formais da política e estabelecimento de um processo de gestão de mudanças.

Devido ao grau de importância que a política de segurança da informação representa para a segurança da informação organizacional, seu teor, bem como suas atualizações, devem ser do conhecimento de todas as pessoas que, de alguma maneira, se relacionam com os sistemas de informação da organização, tais como funcionários, terceirizados e demais colaboradores.

Dessa forma, a divulgação da política de segurança da informação é de fundamental importância para a sua eficácia. Ou seja, por meio da divulgação aumenta-se a probabilidade de que as diretrizes preconizadas na política sejam realmente seguidas.

2.4 Gerenciamento de Riscos de Segurança da Informação

As organizações possuem peculiaridades que determinam os requisitos de segurança da informação próprios, relacionados com os objetivos do negócio. A definição desses requisitos é feita no âmbito de um sistema de gestão de riscos de segurança da informação organizacional, onde são avaliados os riscos a que a organização está sujeita e quais os controles que podem ser adotados.

Risco de segurança da informação é a possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, prejudicando a organização (ABNT, 2008, p. 1).

Brasil (2009a, p. 2) define gestão de riscos de segurança da informação e comunicações,

como sendo: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

O processo de gestão de riscos, aliado a uma política de segurança da informação, constitui o alicerce que sustenta a gestão da segurança da informação na organização.

Devido ao dinamismo que os sistemas de informação apresentam em seu comportamento ao longo do tempo, com o aparecimento de novas tecnologias, ameaças e vulnerabilidades, surge a necessidade de que a gestão de riscos de segurança da informação seja realizada de maneira iterativa e contínua.

Entre as ações que integram a gestão de riscos de segurança da informação, o levantamento e a classificação dos ativos de informação da organização se constituem atividades básicas e imprescindíveis. É necessário que seja definido o que deve ser protegido, de modo que os investimentos em mecanismos de proteção de cada ativo estejam de acordo com o seu grau de importância para o negócio da organização.

Conforme definido em Brasil (2009a, p. 2), ativos de informação são os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

2.4.1 A Norma ABNT NBR ISO/IEC 27005:2008

A norma ABNT 27005 (ABNT, 2008) fornece as diretrizes para o processo de gestão de riscos de segurança da informação de uma organização. Essa norma foi originalmente publicada em 2005 como BS 7799-3.

O processo de gestão de riscos de segurança da informação proposto pela norma ABNT 27005 é executado de maneira iterativa, sendo constituído pelas seguintes atividades: definição do contexto, identificação de riscos, estimativa de riscos, avaliação de riscos, tratamento do risco, aceitação do risco, comunicação do risco e monitoramento e análise crítica do risco (ABNT, 2008).

A Figura 2.2 ilustra o fluxograma do processo de gestão de riscos de segurança da informação proposto pela referida norma e a Tabela 2.4 descreve as atividades que são

desenvolvidas nesse processo. Como pode ser observado pela análise da Figura 2.2, as atividades de identificação e estimativa de riscos constituem a análise de riscos. Observa-se, também, que ao final da fase de análise e avaliação de riscos e da fase de tratamento do risco, existe um ponto de decisão entre a continuidade do processo ou o retorno para alguma fase anterior, caso o resultado não esteja em um nível considerado satisfatório. O número de iterações a serem realizadas no processo dependerá do nível de adequação aos requisitos de segurança da informação da organização, alcançado ao término das fases de análise e avaliação de riscos e de tratamento do risco.

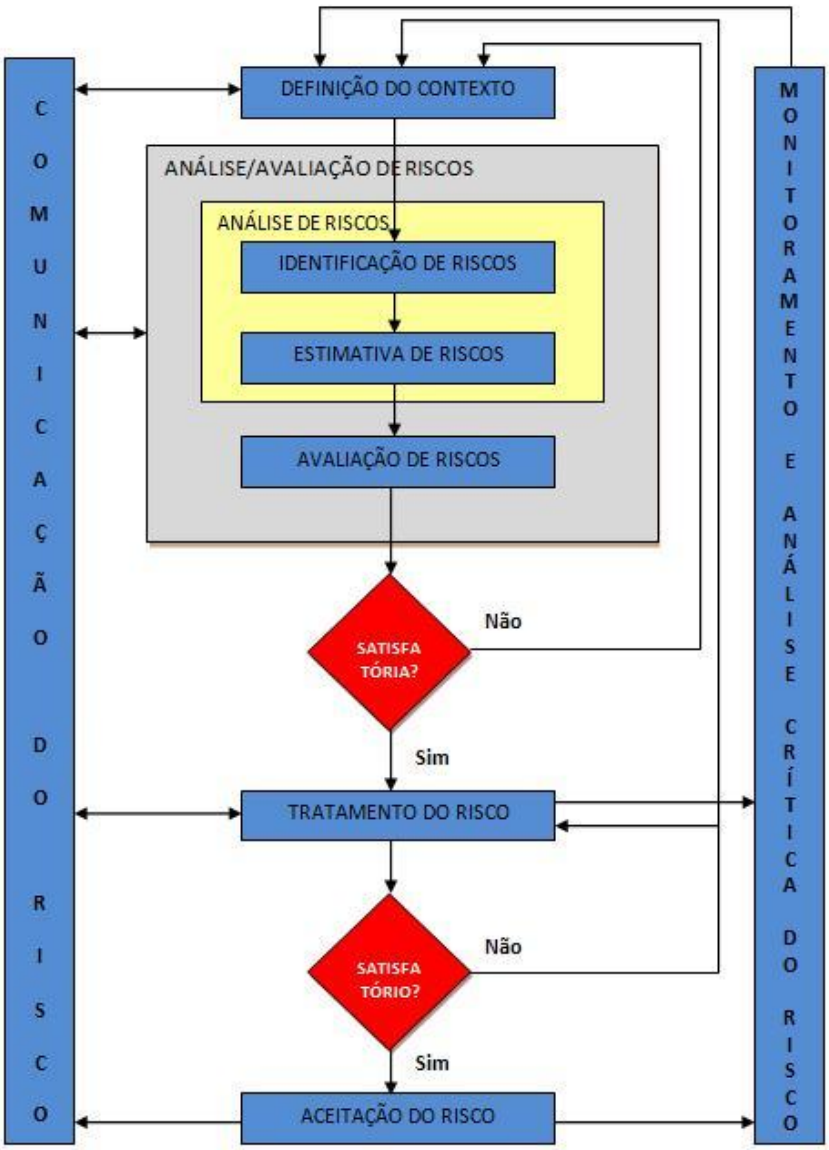

Figura 2.2 – Fluxograma do Processo de Gestão de Riscos de Segurança da Informação.
Fonte: o autor, adaptação de Cicco (2008).

Tabela 2.4 – Atividades do processo de Gestão de Riscos de Segurança da Informação.

ATIVIDADE	DESCRIÇÃO
Definição do contexto	- Definição de critérios básicos para a gestão de riscos (critérios para avaliação do risco, determinação dos impactos dos incidentes e aceitação do risco). - Definição do escopo e limites da gestão de riscos. - Estabelecimento de organização apropriada para operar a gestão de riscos.
Identificação de riscos	- Identificação dos ativos. - Identificação das ameaças. - Identificação dos controles existentes. - Identificação das vulnerabilidades. - Identificação das consequências dos incidentes de segurança sobre os ativos identificados.
Estimativa de riscos	Atribui valores aos riscos de acordo com as consequências que o risco pode causar e a sua probabilidade de ocorrência. A metodologia a ser utilizada pode ser qualitativa ou quantitativa.
Avaliação de riscos	Ordenação dos riscos por prioridade de acordo com os critérios de avaliação de riscos definidos no contexto.
Tratamento do risco	- Seleção dos controles para reduzir o risco (baixar o nível do risco para valor aceitável). - Reter o risco (quando o risco atende aos critérios de aceitação definidos na definição do contexto). - Evitar o risco (para riscos considerados demasiadamente elevados, compreende a eliminação da atividade ou mudança das condições de operação). - Transferir o risco (compartilhar ou transferir o risco para outra entidade). - Definição do plano de tratamento do risco.
Aceitação do risco	Registro formal da decisão de aceitar o risco por parte dos gestores
Comunicação do risco	Troca de informação sobre o risco entre o tomador de decisão e demais partes interessadas.
Monitoramento e análise crítica de riscos	Atividades que visam identificar mudanças no contexto organizacional e panorama de riscos (ativos, ameaças, vulnerabilidades, controles, impactos, probabilidade de ocorrência), visando aprimorar o processo de gestão de riscos.

O processo de gestão de riscos deve ser executado de maneira iterativa devido às modificações no cenário vivido pela organização, com o surgimento de novas ameaças e vulnerabilidades nos sistemas de informação.

Além da abordagem das diversas atividades constituintes do processo de gestão de riscos, a norma ABNT 27005 contempla, em seus anexos, informações como: detalhamento da definição

de contexto, identificação e valoração dos ativos, avaliação do impacto, exemplos de ativos, ameaças, vulnerabilidades comuns e diferentes abordagens sobre análise/avaliação de riscos de segurança da informação e restrições relativas à redução do risco (ABNT, 2008).

A busca da segurança da informação é realizada por meio da implementação de controles que visam minimizar os riscos existentes. Dessa forma, é possível perceber a importância que a gestão de riscos representa para a segurança da informação, pois o desconhecimento da magnitude dos riscos aos quais determinada organização está exposta certamente comprometerá a tarefa de decisão sobre investimentos em controles de segurança.

2.5 O Direito na Segurança da Informação

Muitos requisitos de segurança da informação de uma organização são de ordem jurídica, ou seja, os decorrentes de leis, estatutos, regulamentos e cláusulas contratuais. Por esse motivo, a participação do profissional da área de direito ganha importância na gestão da segurança da informação das organizações modernas. Segundo Machado (2008, p. v), a migração das corporações para o gerenciamento tecnológico de suas informações faz com que o profissional de direito seja a cada dia mais atuante e com maior grau de importância nessa área.

As diretrizes a serem seguidas na gestão da segurança da informação devem estar em conformidade com a legislação em vigor. Além disso, todas as ações de auditoria e monitoramento, bem como apuração de responsabilidades e processos disciplinares devem estar devidamente amparados. Dessa forma, pode-se perceber que o profissional de direito atua na gestão da segurança da informação de maneira proativa (preventiva) e reativa (apuração dos incidentes de segurança da informação ocorridos).

Segundo Machado (2010, p. 7), o profissional de direito pode atuar na organização de forma consultiva, orientando o gestor e colaboradores; de forma colaborativa, compondo grupos de trabalho, orientando equipes; ou mesmo contenciosa, assessorando a condução de processos administrativos e em matéria judicial.

A segurança da informação em uma organização envolve várias áreas do direito, o que torna imprescindível um assessoramento jurídico na condução da sua gestão. Ela possuirá maior chance de eficiência e eficácia se for composta por um trabalho em conjunto dos profissionais das

áreas de segurança, TI e direito.

2.6 Segurança em Recursos Humanos

As pessoas que integram a organização são fundamentais para a implementação das diretrizes estipuladas na política de segurança da informação. Portanto, o comportamento das pessoas deve estar alinhado com o que está previsto nas normas e diretrizes da organização. Sêmola (2003 apud NETO, A., 2007, p. 32) classifica a segurança da informação dividindo-a em três aspectos: tecnológicos, físicos e humanos.

Conforme descrito por Rocha, P. (2008, p. 10-29), o comportamento das pessoas é um ponto relevante na segurança da informação, pois elas estão sujeitas às ações realizadas pelos engenheiros sociais, que não envolvem necessariamente computadores. Os controles relacionados a esse tipo de risco são constituídos por meio da conscientização dos integrantes da organização sobre o problema e pelo estabelecimento de diretrizes e normatização de rotinas e procedimentos de segurança, que orientem suas atitudes. O autor salienta, também, que atualmente, mesmo com razoáveis investimentos em tecnologia, as organizações continuam vulneráveis, pois empregados despreparados, desinformados e mal intencionados, a ausência de políticas claras, normas e procedimentos bem definidos, ou a inadequação dos mesmos, e instalações impróprias tornam-se a porta de saída para informações estratégicas.

Para Silva, T. (2010, p. 7), a análise do comportamento das pessoas deve ser feita por meio de uma abordagem ergonômica, em que são levadas em consideração, além do contexto em que elas estão inseridas, suas reais necessidades, expectativas e dificuldades. Essa avaliação mais ampla facilita a compreensão das razões que levam ao comportamento inseguro das pessoas em seu trabalho. Para o autor, nem todos os comportamentos inseguros são dotados de má intenção ou incapacidade profissional. Alguns deles são frutos da impossibilidade de cumprimento dos protocolos de segurança prescritos.

Neto, J. (2010, p. 27) menciona que os aspectos culturais sobre segurança da informação de uma organização podem ser difundidos por meio de um Programa Corporativo de Conscientização em Segurança da Informação (PCCSI), sendo que o sucesso desse programa é dependente de um forte apoio da alta administração. As fases que compõem o PCCSI são

descritos na Tabela 2.5.

Tabela 2.5 – Fases do Programa Corporativo de Conscientização em Segurança da Informação (PCCSI).

FASE	DESCRIÇÃO
Definição do escopo preliminar do programa	Fornece o arcabouço para as discussões detalhadas com as partes interessadas. Descrito em termos de públicos-alvo e cronograma.
Engajamento do pessoal de negócio	Agendar reuniões com os líderes das unidades para identificação das questões de segurança, benefícios do PCCSI e impactos que a concretização das ameaças podem causar.
Construção do projeto PCCSI	Definição de objetivos, ações, com indicadores e metas e criação de um comitê.
Implementação do PCCSI	Realizar o treinamento do programa, iniciando com o corpo gerencial.
Medir e otimizar	Avaliar o programa, reconhecer sucesso e corrigir falhas. Utilização do ciclo de melhoria contínua.
Relatar o andamento do PCCSI	Manter as partes interessadas informadas sobre os resultados alcançados.

A norma ABNT 27002, em sua seção 8, aborda os controles de segurança em recursos humanos (funcionários, fornecedores e terceiros) a serem implementados antes, durante e no encerramento da contratação.

2.7 Segurança Física e Ambiental

Um sistema de proteção física e do ambiente consiste na combinação de elementos tais como: cercas, barreiras, sensores, câmeras de vídeo, catracas, leitores de cartão de identificação, alarmes, dispositivos de comunicação, sistema de proteção contra incêndio, climatizadores, pessoal de segurança, etc.

A proteção da informação é necessária não somente nos sistemas computacionais, mas também nas demais formas de armazenamento, tratamento e disseminação da mesma.

De acordo com Promon (2005, p. 6), as fronteiras da segurança da informação vão muito além da segurança lógica. Permeiam também a segurança física, que tem por objetivo prevenir acesso não autorizado, dano e interferência às informações, equipamentos e instalações físicas da

organização. O campo da segurança física inclui a utilização de dispositivos que interagem com o mundo físico, em contraste e complementação aos dispositivos lógicos.

A implementação de controles de segurança física e ambiental deve estar de acordo com um plano de tratamento de risco, em que os ativos e as áreas a serem protegidas foram devidamente analisadas e avaliadas.

A norma ABNT 27002 estabelece, em sua seção 9, os controles a serem implementados visando a obtenção da segurança física e ambiental. Essa norma aborda, além dos controles de segurança relativos às áreas e instalações, os destinados à segurança dos equipamentos, cabeamento (de energia e de dados) e utilidades (energia elétrica, água, climatização, etc.). Ela preconiza que os objetivos dos controles relacionados à segurança física e do ambiente são: prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização, bem como impedir perdas, danos, furto ou roubo, ou comprometimento de ativos e interrupção das atividades da organização (ABNT, 2005).

2.8 Gerenciamento das Operações e Comunicações

A estrutura de TI de uma organização deve possibilitar o gerenciamento dos recursos computacionais existentes, de modo que seja possível suprir, de forma eficiente e econômica, as necessidades corporativas de informação. Essa estrutura deve possuir unidades organizacionais com responsabilidades estabelecidas, documentadas e divulgadas, além de políticas de pessoal adequadas no que se refere à seleção, segregação de funções treinamento e avaliação de desempenho (BEAL, 2001, p. 3).

A Gerência da Tecnologia da Informação diz respeito às atividades, métodos, procedimentos e ferramentas pertinentes à operação, administração, manutenção e provisionamento de serviços e sistemas de informação e também da tecnologia que os suporta (GONDIM, 2010a, P. 7).

O gerenciamento de operações e comunicações, como integrante do gerenciamento da tecnologia da informação, tem como objetivo disponibilizar e manter todos os recursos de TI necessários ao funcionamento adequado da organização. Segundo Gondim (2010a, p. 11), uma possível definição para gerenciamento de operações e comunicações seria: o gerenciamento de

operações e comunicações diz respeito a atividades, processos, procedimentos e recursos que visam disponibilizar e manter serviços, sistemas e infraestrutura que os suporta, satisfazendo os acordos de níveis de serviço.

Conforme descrito por Bordim (2008, p. 12), a gestão das operações e comunicações tem como objetivo principal assegurar de forma correta a operação dos recursos de processamento da informação.

A norma ABNT 27002, em sua seção 10, estabelece uma série de controles a serem implementados visando à operação segura e correta dos recursos de processamento da informação. Esta seção da norma aborda em suas subseções os controles relacionados aos seguintes tópicos: procedimentos e responsabilidades operacionais, gerenciamento de serviços terceirizados, planejamento e aceitação dos sistemas, proteção contra códigos maliciosos e códigos móveis, cópias de segurança, gerenciamento da segurança em redes, manuseio de mídias, troca de informações, serviços de comércio eletrônico e monitoramento.

2.9 Controles de Acesso

Na busca pela segurança da informação, os controles de acesso aos ativos de informação da organização são uma das primeiras e mais importantes medidas a serem adotadas. Esses controles visam proteger tais ativos contra acessos por parte de pessoas e sistemas não autorizados, bem como permitir acesso àqueles que possuem autorização.

Brasil (2010, p. 3) define controle de acesso como sendo: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso. Conforme Brasil (2010, p. 2), acesso é o ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade.

É conveniente que o acesso à informação, recursos de processamento das informações e processos de negócios sejam controlados com base nos requisitos de negócio e segurança da informação, em que as regras de controle de acesso levem em consideração as políticas para autorização e disseminação da informação e que a política de controle de acesso seja estabelecida, documentada e analisada criticamente, tomando-se como base tais requisitos (ABNT, 2005, p. 65).

A implementação de controle de acesso é realizada de acordo com o plano de tratamento de risco, o qual é fruto de um sistema de gestão de riscos de segurança da informação. Dessa forma, as áreas, instalações e ativos de informação devem ser identificados e relacionados de acordo com o grau de importância e criticidade, de modo que o acesso aos mesmos seja controlado.

A norma ABNT 27002 contempla, em sua seção 11, os controles de acesso à informação, com as respectivas diretrizes para a sua implementação. Essa norma preconiza a conveniência do estabelecimento de uma política de controle de acesso que esteja alinhada aos objetivos do negócio e a segurança da informação, onde são expressas as regras de controle de acesso e os direitos de cada usuário ou grupo de usuários.

Para Fernandes (2010, p. 7), os controles de acesso podem ser de três tipos: físicos (cercas, cadeados, humanos, etc...), técnicos ou lógicos (computadores e dispositivos digitais programáveis) e administrativos (políticas, processos e procedimentos organizacionais).

2.10 Aquisição, Desenvolvimento e Manutenção dos Sistemas de Informação

A governança corporativa está associada à gerência dos diversos ativos (humanos, financeiros, físicos, de informação, etc.) da organização. Segundo Ohtoshi (2008, p. xxxv), a estratégia de governança destina-se à implantação de sistemas que monitoram e registram atividades de negócio, a garantir a conformidade com as políticas e acordos e a realizar correções nos casos em que as regras foram ignoradas ou mal aplicadas.

Para que os sistemas de informação funcionem adequadamente torna-se necessária uma perfeita governança dos seus ativos de informação visando alinhá-los com os objetivos e com os negócios da organização. Dessa forma, a governança dos ativos de TI tornou-se um ramo da governança corporativa de grande relevância para as organizações.

Para Benz (2008, p. 37), uma governança de TI eficaz ajuda a garantir que a TI apoie efetivamente os objetivos de negócio, otimiza o investimento em TI e gerencia as oportunidades e ameaças relacionadas à TI.

Um *framework* de governança de TI amplamente utilizado pelas organizações é o COBIT (*Control Objectives for Information and related Technology*), o qual é constituído de um conjunto de práticas. Entre os diversos componentes da governança de TI, que são descritos no arcabouço teórico do COBIT como domínios, temos a aquisição, implementação, entrega e suporte dos serviços de TI. A Figura 2.3 ilustra os domínios do COBIT e seus relacionamentos.

Nesses domínios são tratados os processos relacionados à obtenção e gerenciamento da tecnologia necessária ao tratamento (produção, disseminação, armazenamento, etc.) das informações necessárias ao negócio da organização, seja por meio da contratação de soluções prontas ou pelo desenvolvimento próprio das soluções (ITGI, 2007).

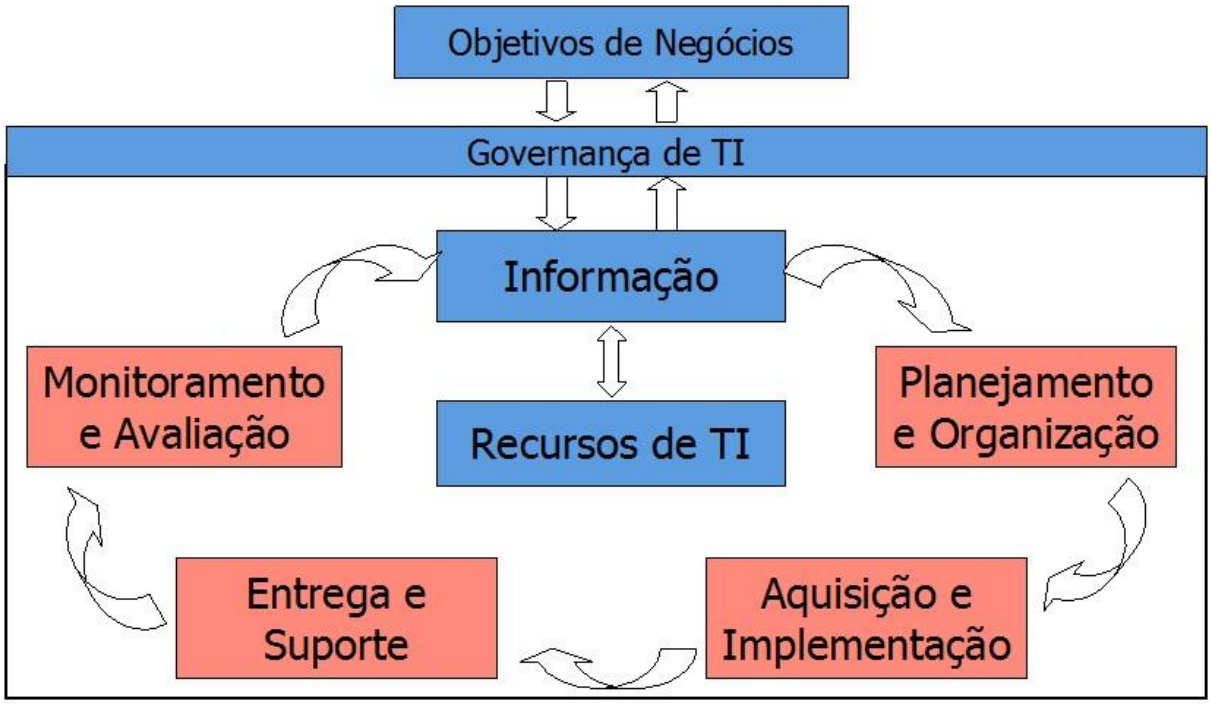

Figura 2.3 – Domínios do COBIT. Fonte: Durans (2010).

Muitas vulnerabilidades existentes em sistemas de informação estão embutidas no processo de desenvolvimento de s*oftware*, ou seja, na falta de preocupação com a segurança do *software* durante o seu desenvolvimento. As organizações muitas vezes desenvolvem *softwares* visando automatizar determinados processos organizacionais esquecendo-se de implementar controles que preservem os atributos de segurança da informação com a qual eles trabalham. Dessa forma, controles de segurança devem ser inseridos nos processos de desenvolvimento e manutenção dos sistemas de informação, bem como serem exigidos por ocasião das contratações

de soluções já prontas.

Segundo Batista (2007, p. 23), a segurança de *software* consiste na preservação dos atributos de segurança da informação dos ativos e recursos de informação que o *software* cria, armazena, processa ou transmite, incluindo a segurança do próprio programa. Para Holanda e Fernandes (2011, p. 22) um *software* seguro é aquele livre de vulnerabilidades e que funcione da maneira pretendida. Como a existência de um *software* totalmente seguro é utópica, o que busca-se é reduzir ao máximo suas vulnerabilidades, tornando-o o mais seguro possívelel.

Os controles de segurança atinentes à aquisição, desenvolvimento e manutenção dos sistemas de informação são tratados na seção 12 da norma ABNT 27002 (ABNT, 2005).

2.11 Gestão de Incidentes de Segurança da Informação

Os sistemas de informação das organizações estão sujeitos a incidentes de segurança da informação. Gondim (2010b, p. 6) define incidente de segurança computacional como sendo qualquer ação ilegal, não autorizada ou inaceitável que envolve um sistema computacional ou rede de computadores. O autor menciona ainda que os incidentes computacionais são ações executadas por pessoas ou computadores, de maneira intencional ou não, que causam algum tipo de dano.

Dessa forma, surge a necessidade da elaboração e implementação de um sistema de gestão de incidentes de segurança da informação, visando à coordenação das ações a serem realizadas no tratamento e resposta a tais incidentes.

Brasil (2009b, p. 3) define tratamento de incidentes de segurança em redes computacionais como sendo o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

É conveniente uma gestão total dos incidentes de segurança ocorridos na organização, com resposta, monitoramento e avaliação, constituindo um processo de melhoria contínua. Também é necessária a definição de responsabilidades e procedimentos para o tratamento dos eventos de segurança da informação e fragilidades detectadas (ABNT, 2005, p. 100).

A constituição de uma equipe de tratamento e resposta a incidentes de segurança, composta por profissionais capacitados, deve ser parte da gestão de incidentes de segurança da informação em uma organização. Brasil (2009b, p. 3) define a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) como sendo um grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

A resposta a um incidente envolve ações tipicamente reativas, porém, seu sucesso é fortemente dependente de ações realizadas antes que o incidente aconteça, ou seja, na preparação pré-incidente, quando são executadas ações que preparam a organização para a resposta a um incidente e define o Grupo de Resposta a Incidentes de Segurança Computacional (GONDIM, 2010b, P. 9).

A norma ABNT 27002, em sua seção 13, estabelece diretrizes e controles a serem implementados, no que se refere à gestão de incidentes de segurança da informação (ABNT, 2005).

2.12 Gestão de Continuidade do Negócio

Nenhuma organização está totalmente imune a incidentes de segurança ou qualquer outro tipo de desastre. Diante disso, torna-se necessária a implementação de mecanismos que possibilitem a continuidade das operações essenciais ao cumprimento de sua missão, mesmo em situações de crises.

Brasil (2009c, p. 3) define continuidade de negócios como sendo a capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido. Assim, a gestão de continuidade do negócio é um processo que desenvolve a resiliência organizacional, resguardando os interesses, a reputação, a marca da organização e suas atividades de valor agregado. Nesse processo são identificadas as ameaças potenciais para a organização, bem como os possíveis impactos decorrentes da concretização de tais ameaças.

A gestão de continuidade de negócio se constitui em um mecanismo muito mais

abrangente do que simplesmente as ações a serem executadas após o acontecimento de um desastre. Segundo Guindani (2008, p. 56), a gestão da continuidade do negócio visa garantir a recuperação de um ambiente de produção, independente de eventos ocorridos e de danos causados em tal ambiente.

O objetivo da gestão da continuidade do negócio, conforme preconizado em ABNT (2005, p. 103) é não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil.

O plano de continuidade de negócios se constitui no documento no qual são estabelecidas diretrizes a serem seguidas e definidas ações a serem executadas, com o objetivo de permitir que as atividades críticas mantenham-se em funcionamento. Para confecção desse plano é tomado como base a avaliação das atividades críticas da organização bem como o processo de avaliação do risco dessas atividades, em que o impacto da perda ou indisponibilidade dos ativos de informação foram analisados.

No que se refere à gestão da continuidade do negócio, a norma ABNT 27002, em sua seção 14, estabelece diretrizes e controles a serem implementados (ABNT, 2005).

2.13 Conformidade de Segurança da Informação

A conformidade de segurança da informação refere-se à situação em que a gestão da segurança da informação está de acordo com os requisitos legais e normatização interna da organização e que os controles de segurança estão sendo implementados de maneira eficiente e eficaz, conforme foi planejado.

Brasil (2007, p. 4) define conformidade como sendo o estado em que se constata a coerência esperada entre o previsto num controle e um elemento auditado.

Segundo Rodrigues (2004, p. 13), é conveniente que as organizações realizem periodicamente auditorias em seus sistemas de informação, com o objetivo de analisar e avaliar se as atividades desenvolvidas cumprem adequadamente as condições que lhes são exigidas. Esta auditoria deve confirmar, ou não, a existência de erros, omissões, duplicidades, faltas e/ou fraudes quer sejam nos procedimentos ou nos resultados.

Conforme definido por Brasil (2007, p. 4), auditoria de segurança da informação é o

processo em que é verificada a conformidade entre os controles estabelecidos e o estado dos elementos auditados e, além disso, o grau de efetividade dos processos analisados pela auditoria.

Para Bauer (2006, p. 56), as auditorias periódicas na empresa devem ser realizadas por um funcionário devidamente treinado ou por prestadores de serviço por ela contratados, com o objetivo de verificar se a segurança da empresa atende aos objetivos indicados na política de segurança.

A norma ABNT 27002, em sua seção 15, estabelece diretrizes e controles a serem implementados, no que se refere à conformidade de segurança da informação (ABNT, 2005).

2.14 Considerações sobre os Fundamentos Conceituais

Este capítulo abordou os principais conceitos relativos ao gerenciamento da segurança da informação. Os diversos enfoques abordados são tratados na normatização que estabelece padrões para implementação dos mesmos, como um conjunto de diretrizes voltadas para um tema específico. Como exemplos, podemos citar a norma ABNT 27001, que trata dos requisitos de um sistema de gestão da segurança da informação; a norma ABNT 27002, que versa sobre os controles de segurança da informação e a norma ABNT 27005, que aborda a gestão de riscos de segurança da informação.

Dessa forma, torna-se relevante a idealização de um modelo que contemple os principais enfoques que constituem a gestão da segurança da informação de uma maneira consolidada, de modo a proporcionar um melhor entendimento e implementação do sistema de gestão da segurança da informação como um todo.

Capítulo 3

Modelo de Sistema de Gestão da Segurança da Informação

Este capítulo apresenta um modelo de sistema de gestão da segurança da informação (SGSI) que procura abranger as diretrizes preconizadas nas normas ABNT NBR ISO/IEC 27001 (que trata dos requisitos de um sistema de gestão da segurança da informação), 27002 (código de prática com a descrição dos controles de segurança a serem implementados) e 27005 (gestão de riscos de segurança da informação). Nesse modelo, cada enfoque referente a um sistema de gestão da segurança da informação, conforme abordado no capítulo 2, é visto sob a perspectiva de um processo, cada qual com seus objetivos, que recebem entradas, executam atividades e oferecem saídas. Dessa forma, o SGSI é constituído por um conjunto de processos inter-relacionados. As Figuras 3.1 e 3.2 ilustram o modelo de gestão de segurança da informação proposto, onde são mapeados, respectivamente, os processos que interligam o SGSI com o ambiente externo e os processos que constituem o sistema propriamente dito, o qual denominamos núcleo do SGSI.

Analisando a Figura 3.1, percebe-se que interagem com o SGSI os seguintes componentes: a direção da organização, por meio dos processos de análise crítica do sistema e de sua implementação e manutenção, os intervenientes e a infraestrutura de tecnologia da informação. A seguir encontra-se uma descrição geral de cada componente da Figura 3.1:

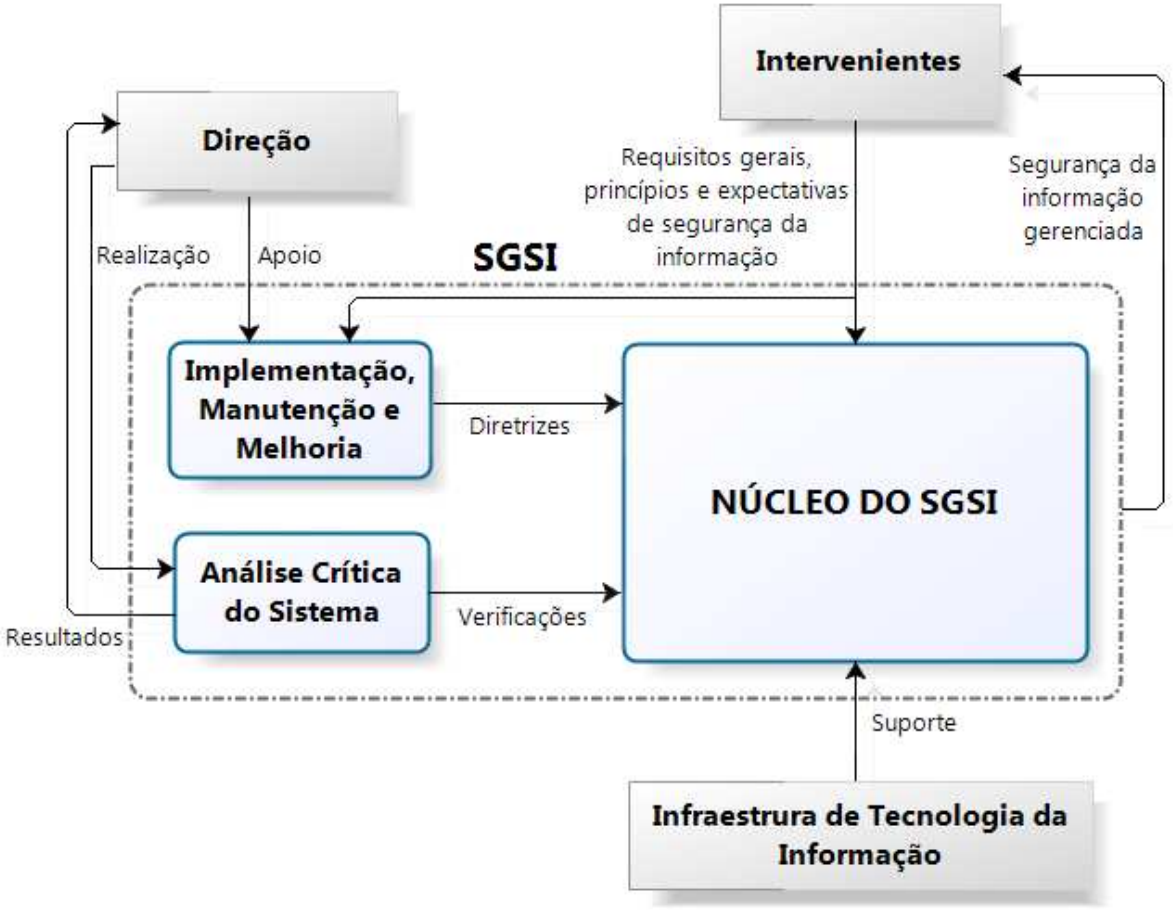

Figura 3.1 – Mapeamento do SGSI com o ambiente externo.

- **Direção:** responsável pelo estabelecimento e manutenção do SGSI, apoiando e manifestando seu comprometimento com a segurança da informação, bem como pela realização da análise crítica do sistema.
- **Análise Crítica do Sistema:** processo que consiste na verificação do SGSI, apontando suas deficiências, o que possibilita a implementando melhorias.
- **Implementação, Manutenção e Melhoria:** processo destinado a estabelecer, manter e melhorar o SGSI, de acordo com os princípios, requisitos gerais e expectativas de segurança da informação da organização.
- **Intervenientes:** são as partes interessadas, representados pelos sócios de uma organização privada ou a sociedade em geral, para uma organização pública. Fornecem ao sistema os requisitos gerais de segurança, os princípios que

norteiam tal organização, bem como as expectativas em relação à segurança da informação.

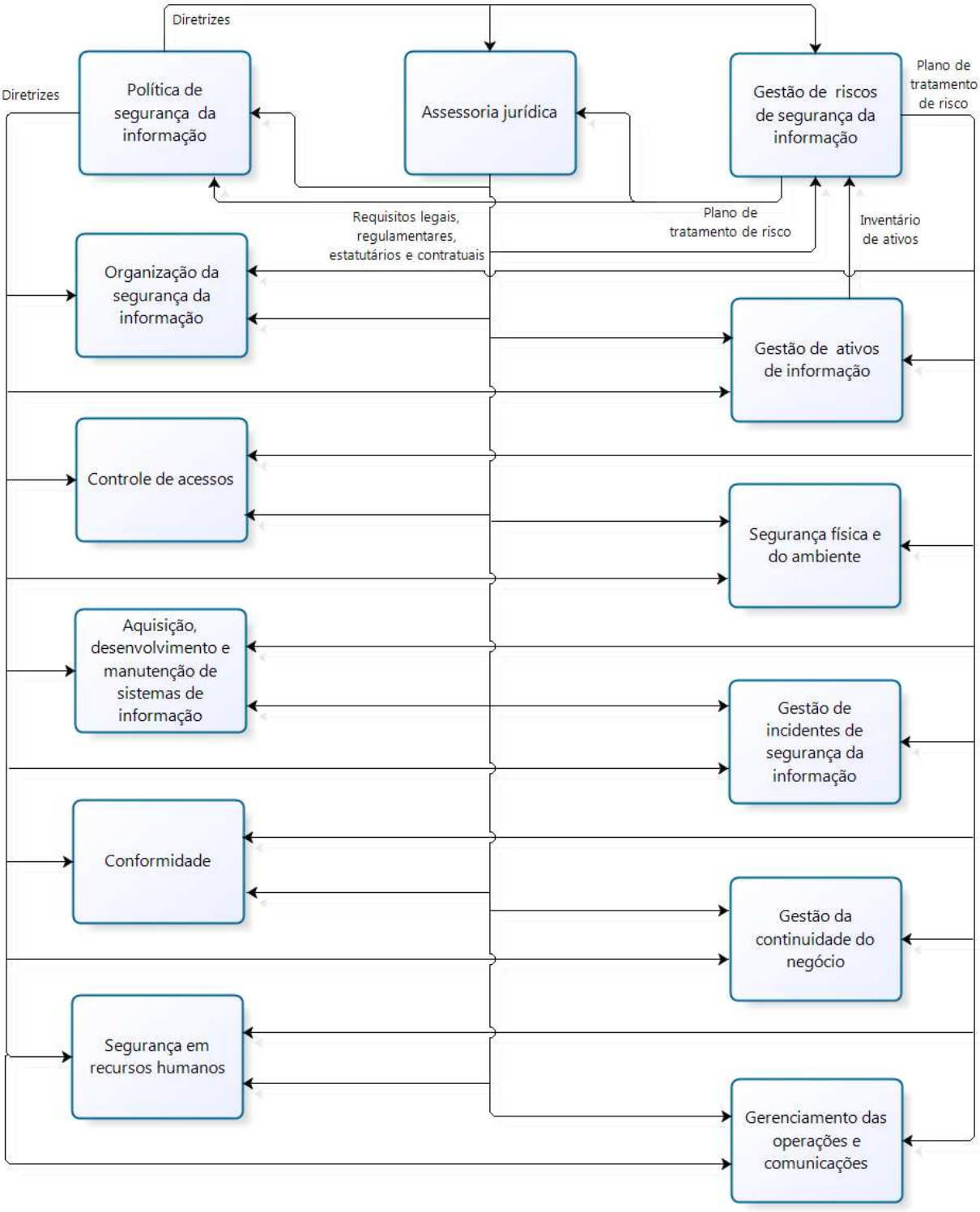

Figura 3.2 – Mapeamento dos processos integrantes do núcleo do SGSI.

- **Infraestrutura de Tecnologia da Informação:** conforme abordado no capítulo 2 deste trabalho, todo o sistema de gestão de segurança da informação se desenvolve tendo como base a infraestrutura que o suporta. Portanto ainfraestrutura de tecnologia da informação é o alicerce para todos os demais elementos do sistema.

A Figura 3.2 apresenta os diversos processos que constituem o SGSI e que implementam os controles visando a busca da segurança da informação, onde se desenvolvem os seguintes processos básicos: política de segurança da informação, assessoria jurídica e gestão de riscos de segurança da informação. Esta figura mostra como entradas e saídas de cada processo, apenas aquelas destinadas a facilitar o entendimento do sistema, sendo que a discriminação das entradas e saídas em sua totalidade é contemplada na próxima seção.

norteiam tal organização, bem como as expectativas em relação à segurança da informação.

3.1 Descrição dos Processos que compõem o SGSI

Esta seção descreve cada processo integrante do sistema, indicando seus objetivos, as entradas recebidas, as atividades realizadas e as saídas fornecidas.

3.1.1 Implementação, Manutenção e Melhoria do Sistema de Gestão da Segurança da Informação (SGSI)

Objetivos do processo: assegurar a seleção de controles de segurança adequados para proteger os ativos de informação e propiciar confiança às partes interessadas.

Entradas do processo:

- Requisitos gerais, princípios e expectativas de segurança da informação.
- Requisitos legais, regulamentares e contratuais.
- Critérios básicos de gestão de riscos de segurança da informação.

Atividades Realizadas:

- Estabelecer o sistema de gestão da segurança da informação (SGSI), definindo seu escopo e limites.

- Definir e aprovar a política do SGSI, contemplando a definição dos objetivos, direcionamento e princípios para ações voltadas à segurança da informação, bem como os critérios de avaliação de riscos, de impacto e de aceitação do risco[1].
- Estabelecer uma estrutura que possibilite a implementação da segurança da informação dentro da organização.
- Aprovar e analisar criticamente a política de segurança da informação.
- Assegurar que as metas da segurança da informação estão identificadas e atendem aos requisitos da organização.
- Atribuir funções e responsabilidades para a segurança da informação. Prover os recursos necessários à segurança da informação.
- Coordenar a implementação da segurança da informação na organização.
- Comprometimento da direção, por meio de manifestação clara de apoio, com a segurança da informação.
- Implementar planos e programas de conscientização e treinamento quanto à segurança da informação.
- Assegurar que a implementação dos controles de segurança da informação sejam coordenados e permeiam toda a organização.
- Determinar as competências necessárias para o pessoal que executa tarefas que afetam o SGSI.
- Constituir o grupo responsável pelo gerenciamento da segurança da informação na organização.
- Aprovar a metodologia de gestão de riscos de segurança da informação.
- Aprovar metodologias e processos para a segurança da informação.
- Conduzir auditorias internas do SGSI em intervalos planejados, visando avaliar a conformidade dos objetivos de controle, dos controles e dos procedimentos adotados.
- Executar ações corretivas e preventivas no sistema de gestão de segurança da informação, tomando-se como base o resultado de auditorias, o resultado da análise crítica do sistema ou qualquer outra informação pertinente.

1 Conforme ABNT (2006, p. 4), a política do SGSI é o documento maior da política de segurança da informação, podendo estarem descritas em um documento.

- Definir e documentar os procedimentos para as ações corretivas, tais como:
  - Identificar a não-conformidade.
  - Determinar as causas da não-conformidade.
  - Avaliar a necessidade de ações para evitar a ocorrência da não-conformidade.
  - Determinar e implementar as ações corretivas necessárias.
  - Registrar os resultados das ações corretivas executadas.
- Obter autorização da direção para implementar e operar o SGSI.
- Proteger e controlar os documentos requeridos pelo SGSI.
- Estabelecer procedimentos documentados para definir ações a serem realizadas no gerenciamento de documentos.
- Estabelecer e manter os registros de desempenho dos processos e da ocorrência de incidentes de segurança no SGSI.

Saídas do processo:

- Metas, escopo, objetivos e importância da segurança da informação.
- Estrutura de implementação da segurança da informação da organização.
- Diretrizes e normas sobre a segurança da informação.
- Política de segurança da informação aprovada.
- Metodologia de gestão de riscos de segurança da informação aprovada.
- Metodologias e processos para a segurança da informação aprovados.
- Planos e programas de conscientização quanto à segurança da informação.
- Ações corretivas e preventivas do sistema de gestão de segurança da informação.
- Procedimentos para as ações corretivas.

3.1.2 Organização da Segurança da Informação

Objetivos do processo: gerenciar a segurança da informação dentro da organização, bem como manter a segurança dos ativos e recursos de informação que são acessados ou operados por partes externas.

Entradas do processo:

- Requisitos gerais e expectativas de segurança da informação.
- Metas, escopo, objetivos e importância da segurança da informação.
- Requisitos legais, regulamentares, estatutários e contratuais.
- Plano de tratamento de riscos (requisitos de segurança).

Atividades Realizadas:

- Elaborar a política de segurança da informação.
- Garantir que as atividades de segurança da informação sejam realizadas de acordo com a política de segurança da informação, identificando como conduzir as não-conformidades.
- Definir metodologias e processos para a segurança da informação.
- Avaliar a adequação e coordenar a implementação dos controles, processo e procedimentos de segurança da informação.
- Promover a educação, treinamento e conscientização em segurança da informação na organização.
- Avaliar as informações recebidas sobre incidentes de segurança da informação, recomendando as ações a serem executadas como resposta.
- Definir claramente as responsabilidades pela segurança da informação.
- Definir e implementar um processo de gestão de autorização para novos recursos de processamento da informação.
- Identificar e analisar criticamente os requisitos para a confidencialidade e os acordos de não divulgação, de acordo com as necessidades de proteção das informações da organização.
- Manter contatos com pessoal externo (especialistas, grupos e autoridades) visando o tratamento de assuntos relacionados à segurança da informação.
- Analisar criticamente a segurança da informação organizacional, registrando os resultados de tal análise.
- Controlar o acesso de partes externas aos ativos de informação da organização.
- Verificar o atendimento aos requisitos de segurança da informação da organização nos acordos realizados com terceiros.

Saídas do processo:

- Diretrizes e normas sobre a segurança da informação.
- Política de segurança da informação.
- Metodologias e processos para a segurança da informação aprovados.
- Planos e programas de conscientização quanto à segurança da informação.
- Constituição do processo de gestão de autorização para novos recursos de processamento da informação.
- Resultados da análise crítica da segurança da informação.

3.1.3 Política de Segurança da Informação

Objetivo do processo: prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes.

Entradas do processo:

- Requisitos gerais e expectativas de segurança da informação.
- Princípios objetivos e requisitos do negócio.
- Requisitos legais, regulamentares, estatutários e contratuais.
- Plano de tratamento de riscos (requisitos de segurança).

Atividades realizadas:

- Estabelecer a política de segurança da informação.
- Definir metas, escopo, objetivos e importância da segurança da informação.
- Definir a estrutura de estabelecimento dos objetivos de controles e controles de segurança da informação.
- Definir critérios de segurança.
- Definir a estrutura e metodologia do sistema de gestão de riscos.
- Definir requisitos de conformidade da segurança da informação.
- Definir responsabilidades na gestão da segurança da informação.
- Realizar a abordagem das políticas, princípios, normas e requisitos de segurança da informação da organização.
- Abordar as consequências das violações da política de segurança da informação.
- Documentar a política de segurança da informação.

- Submeter a política de segurança da informação à aprovação por parte da direção.
- Publicar e comunicar a política de segurança da informação às partes interessadas.
- Analisar criticamente a política de segurança da informação.
- Melhorar a política de segurança da informação.

Saídas do processo:

- Diretrizes e normas sobre a segurança da informação.
- Metas, escopo, objetivos e importância da segurança da informação.
- Estrutura e metodologia do sistema de gestão de riscos.
- Estrutura de estabelecimento dos objetivos de controle e controles de segurança da informação.
- Comprometimento da organização com a segurança da informação.
- Política de segurança da informação documentada e aprovada.

3.1.4 Gestão de Riscos de Segurança da Informação

Objetivo do processo: identificar as necessidades da organização em relação aos requisitos de segurança da informação para um sistema de gestão da segurança da informação.

Entradas do processo:

- Política de segurança da informação.
- Diretrizes e normas sobre a segurança da informação.
- Informações sobre a organização, metas, escopo, objetivos e importância da segurança da informação.
- Requisitos legais, regulamentares, estatutários e contratuais.
- Estrutura e metodologia do sistema de gestão de riscos.
- Inventário de ativos de informação.
- Estrutura de estabelecimento dos objetivos de controle e controles de segurança da informação.

Atividades realizadas:

- Definir o contexto da gestão de riscos de segurança da informação.
  - Definição do escopo e limites do processo de gestão de riscos de segurança

da informação.

- Definir os critérios de avaliação de riscos.
- Definir os critérios de impacto.
- Definir os critérios de aceitação do risco.
- Estabelecer a organização e responsabilidades para operar o processo de gestão de riscos.
- Verificar a disponibilidade de recursos para operar o processo de gestão de riscos.

- Analisar os riscos
  - Identificar os riscos.
    - Identificar os ativos.
    - Identificar as ameaças.
    - Identificar os controles existentes.
    - Identificar as vulnerabilidades.
    - Identificar as consequências.
  - Estimar os riscos.
    - Avaliar as consequências.
    - Avaliar a probabilidade dos incidentes.
    - Estimar o nível do risco.
- Avaliar os riscos.
- Elaborar o relatório de análise e avaliação de riscos.
- Aceitar os riscos.
- Elaborar a lista de ricos aceitos, incluindo uma justificativa para aqueles que não satisfaçam os critérios normais para aceitação do risco.
- Obter autorização da direção sobre os riscos residuais propostos.
- Definir o plano de tratamento de riscos.
- Obter aprovação do plano de tratamento de riscos.
- Preparar uma declaração de aplicabilidade contendo os objetivos de controle e os controles selecionados, os objetivos de controles e controles já implementados e a justificativa para exclusão de qualquer objetivo de controle e controle constantes da norma ABNT 27002.

- Implementar mecanismos que possibilitem a comunicação dos riscos.
- Monitorar e analisar criticamente os riscos.
- Manter e melhorar o processo de gestão de riscos de segurança da informação.

Saídas do processo:

- Critérios de avaliação de riscos.
- Critérios de impacto.
- Critérios de aceitação do risco.
- Escopo e limites do processo de gestão de riscos.
- Organização e responsáveis pelo processo de gestão de riscos.
- Plano de tratamento de riscos.
- Declaração de aplicabilidade.
- Relatório da análise e avaliação de riscos.
- Lista de riscos aceitos com justificativa para aqueles que não satisfaçam os critérios normais para aceitação do risco.

3.1.5 Assessoria Jurídica

Objetivo do processo: fornecer suporte jurídico ao sistema de gestão da segurança da informação, contribuindo para conformidade do sistema em relação às leis, estatutos, regulamentações ou obrigações contratuais.

Entradas do processo:

- Política da segurança da informação.
- Diretrizes e normas sobre a segurança da informação.
- Metas, escopo, objetivos e importância da segurança da informação.
- Leis, estatutos, regulamentos e contratos.
- Plano de tratamento de riscos (requisitos de segurança).

Atividades realizadas:

- Receber as diretrizes gerais e objetivos da segurança da informação da organização, descritos na política de segurança da informação.
- Reunir as leis, estatutos, regulamentos e contratos atinentes às atividades de

negócio da organização.

- Receber as informações constantes do plano de tratamento do risco.
- Atuar de forma consultiva orientando gestor e colaboradores sobre questões jurídicas.
- Atuar de forma colaborativa compondo grupos de trabalhos, assessorando o gestor e orientando equipes.
- Atuar de forma contenciosa em processos administrativos e em matéria judicial.

Saídas do processo:

- Requisitos legais, estatutários, regulamentares e contratuais.
- Orientações aos demais componentes do SGSI.

3.1.6 Gestão de Ativos de Informação

Objetivo do processo: alcançar e manter a proteção adequada dos ativos da organização.

Entradas do processo:

- Política de segurança da informação.
- Diretrizes e normas sobre a segurança da informação.
- Metas, escopo, objetivos e importância da segurança da informação.
- Requisitos legais, regulamentares, estatutários e contratuais.
- Plano de tratamento de riscos (requisitos de segurança).

Atividades realizadas:

- Identificar os ativos.
- Estruturar e manter o inventário de todos os ativos importantes.
- Documentar a importância de cada ativo.
- Realizar a valoração dos ativos.
- Avaliar o impacto causado pelo incidente de segurança ocorrido em cada ativo.
- Assegurar a existência de um proprietário, responsável por cada ativo identificado.
- Identificar, documentar e implementar regras quanto ao uso das informações e de seus ativos associados.
- Classificar a informação de acordo com o seu valor, requisitos legais, sensibilidade e criticidade.

- Definir e implementar procedimentos para rotulação e tratamento da informação de acordo com a sua classificação.

Saídas do processo:

- Inventário de ativos de informação.
- Regras de uso dos ativos de informação.
- Informação classificada.
- Procedimentos para rotulação e tratamento da informação.

3.1.7 Segurança em Recursos Humanos

Objetivos do processo: assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e obrigações, estejam de acordo com os seus papéis, conscientes das ameaças e preocupações relativas à segurança da informação e estejam preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos normais, bem como reduzir o risco de erro humano, roubo, fraude ou mau uso de recursos, além de assegurar que essas pessoas deixem a organização ou mudem de trabalho de forma ordenada.

Entradas do processo:

- Política de segurança da informação.
- Diretrizes e normas sobre a segurança da informação.
- Metas, escopo, objetivos e importância da segurança da informação.
- Requisitos legais, regulamentares, estatutários e contratuais.
- Plano de tratamento de riscos (requisitos de segurança).

Atividades realizadas antes da contratação:

- Definir e documentar, de acordo com a política de segurança da informação da organização, os papéis e responsabilidades pela segurança da informação de funcionários, fornecedores e terceiros.
- Comunicar aos candidatos ao cargo os papéis e responsabilidades de segurança da informação.
- Realizar verificações de controle dos candidatos a emprego, fornecedores e terceiros, de acordo com a ética, legislação e regulamentos pertinentes.

Atividades realizadas durante a contratação:

- Assegurar que funcionários, fornecedores e terceiros concordem e assinem os termos e condições de sua contratação, bem como declarem suas responsabilidades em relação à segurança da informação da organização.
- Solicitar dos funcionários, fornecedores e terceiros a prática da segurança da informação conforme estabelecido nas políticas e procedimentos da organização.

Atividades realizadas após a contratação:

- Propiciar treinamento, conscientização e atualizações regulares nas políticas e procedimentos organizacionais.
- Realizar processo disciplinar formal para funcionários que tenham cometido violação da segurança da informação.

Atividades realizadas no encerramento ou mudança da contratação:

- Definir e atribuir de forma clara a responsabilidade de realizar o encerramento ou mudança de um trabalho.
- Assegurar a devolução por parte dos funcionários, fornecedores e terceiros dos ativos da organização após o encerramento das atividades, contratos ou acordos.
- Retirar os direitos de acesso dos funcionários, fornecedores e terceiros aos ativos de informação da organização, após o encerramento das atividades, contratos ou acordos.

Saídas do processo:

- Papéis e responsabilidades pela segurança da informação de funcionários, fornecedores e terceiros.
- Termos e condições da contratação e declaração das responsabilidades em relação à segurança da informação da organização.
- Processos disciplinares.
- Atribuição de responsabilidade de realizar o encerramento ou mudança de um trabalho.
- Segurança dos recursos humanos gerenciada.

3.1.8 Segurança Física e do Ambiente

Objetivos do processo: prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações, bem como impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização.

Entradas do processo:

- Política de segurança da informação.
- Diretrizes e normas sobre a segurança da informação.
- Metas, escopo, objetivos e importância da segurança da informação.
- Requisitos legais, regulamentares, estatutários e contratuais.
- Plano de tratamento de riscos (requisitos de segurança).

Atividades realizadas:

- Utilizar perímetros de segurança com barreiras para proteger as áreas que contenham informações e instalações de processamento da informação.
- Proteger as áreas seguras com controles de acesso apropriados.
- Proteger escritórios, salas e instalações.
- Projetar e aplicar proteção contra ameaças externas e do meio ambiente (desastres naturais ou causados pelo homem).
- Projetar e aplicar proteção física e diretrizes referentes ao trabalho em áreas seguras.
- Controlar os pontos de acesso público (áreas de entrega e carregamento, por exemplo) e, se possível, isolar essas áreas das instalações de processamento da informação.
- Proteger os equipamentos contra ameaças e perigos do meio ambiente, bem como do acesso não autorizado.
- Proteger os equipamento contra a falta de energia elétrica ou falhas em outras utilidades.
- Proteger o cabeamento de energia e de telecomunicações contra interceptações ou danos.
- Realizar a manutenção dos equipamentos de forma correta.
- Tomar medidas de segurança para equipamentos que operam fora das

dependências da organização.

- Realizar a reutilização e alienação dos equipamentos de forma segura, examinando, quando for o caso, as mídias de armazenamento de dados antes do descarte.
- Assegurar que equipamentos, informações ou *softwares* não sejam retirados do local sem autorização prévia.

Saídas do processo:

- Diretrizes para trabalho em áreas seguras.
- Segurança física e do ambiente gerenciada.

3.1.9 Gerenciamento das Operações e Comunicações

Objetivos do processo: garantir a operação correta e segura dos recursos de processamento da informação, gerenciar os serviços terceirizados quanto ao nível de segurança e entrega, minimizar os riscos de falhas nos sistemas, manter a integridade e a disponibilidade da informação e dos recursos de processamento, proteger as informações em rede e a infraestrutura de suporte, bem como detectar atividades não autorizadas de processamento da informação.

Entradas do processo:

- Política de segurança da informação.
- Diretrizes e normas sobre a segurança da informação.
- Metas, escopo, objetivos e importância da segurança da informação.
- Requisitos legais, regulamentares, estatutários e contratuais.
- Plano de tratamento de riscos (requisitos de segurança).

Atividades realizadas:

- Documentar, atualizar e disponibilizar aos usuários os procedimentos de operação dos sistemas.
- Controlar as mudanças nos sistemas e nos recursos de processamento da informação.
  - Identificar e registrar as mudanças significativas.
  - Planejar e testar as mudanças.
  - Avaliar os impactos das mudanças.

- Obter aprovação formal das mudanças propostas.
- Comunicar os detalhes das mudanças a todas as pessoas envolvidas.
- Incluir procedimentos e responsabilidades pela interrupção e recuperação das mudanças para os casos de insucessos ou ocorrência de eventos inesperados.
- Manter registro de auditoria de todas as informações relevantes, quando mudanças forem realizadas.

- Segregar funções e áreas de responsabilidade para preservar o uso correto dos ativos de informação.
- Separar os recursos de desenvolvimento, teste e de produção.
  - Definir e documentar regras para a transferência do *software* da situação de desenvolvimento para a de produção.
  - Executar em diferentes sistemas ou processadores e em diferentes domínios ou diretórios, o *software* em desenvolvimento e o *software* em produção.
  - Manter as ferramentas de desenvolvimento ou utilitários de sistema inacessíveis aos sistemas operacionais, quando não se fizer necessário.
  - Emular o ambiente de teste o mais próximo possível do de produção.
  - Diferenciar os perfis de usuários para sistemas em teste e de produção, com mensagens apropriadas de identificação.
  - Utilizar em ambiente de testes, dados que não sejam sensíveis.
- Garantir que os controles de segurança, as definições de serviço e os níveis de entrega incluídos no acordo de entrega de serviços terceirizados sejam implementados, executados e mantidos pelo terceiro.
- Monitorar e analisar criticamente os serviços, relatórios e registros fornecidos por terceiros.
  - Monitorar níveis de desempenho do serviço, verificando a aderência aos acordos.
  - Analisar criticamente os relatórios de serviços produzidos por terceiros e agendar reuniões de progresso.
  - Fornecer informações sobre os incidentes de segurança da informação.
  - Analisar criticamente as trilhas de auditoria de terceiro, registros de

eventos de segurança e problemas ocorridos com o serviço entregue.

- Resolver e gerenciar os problemas identificados.
- Atribuir responsabilidade sobre o gerenciamento do relacionamento com terceiros.
- Disponibilizar habilidades técnicas e recursos para monitorar se os requisitos de segurança estão sendo atendidos.

- Gerenciar as mudanças para serviços terceirizados.
- Monitorar e sincronizar os recursos existentes, bem como projetar necessidade de capacidade futura visando atender a demanda requerida pelos sistemas.
- Estabelecer critérios para a aceitação de novos sistemas, atualizações e novas versões, realizando testes apropriados.
- Implementar controles de proteção (detecção, prevenção e recuperação) contra códigos maliciosos, bem como procedimentos para conscientização dos usuários.
  - Estabelecer uma política formal proibindo o uso de *softwares* não autorizados.
  - Estabelecer uma política formal com orientações sobre a importação de arquivos e *softwares* oriundos de redes externas ou qualquer outro meio.
  - Conduzir análises críticas regulares dos *softwares* e dados dos sistemas que suportam processos críticos de negócio.
  - Instalar e atualizar regularmente *softwares* de detecção e remoção de códigos maliciosos.
  - Definir procedimentos de gerenciamento e respectivas responsabilidades para tratar da proteção de códigos maliciosos nos sistemas.
  - Preparar planos de continuidade do negócio adequados para a recuperação em caso de ataques por códigos maliciosos.
  - Implementar procedimentos para regularmente coletar informações sobre novos códigos maliciosos.
- Controlar a utilização dos códigos móveis autorizados.
- Impedir a execução de códigos móveis não autorizados.
- Realizar e testar regularmente, cópias de segurança das informações e de *softwares*.

- Definir os níveis necessários da cópias de segurança das informações.
- Registrar as cópias de segurança e documentar os procedimentos de restauração da informação.
- Definir a frequência de geração das cópias de segurança.
- Armazenar as cópias de segurança em localidades remotas.
- Proteger as cópias de segurança.
- Testar regularmente as mídias das cópias de segurança, bem como os procedimentos de restauração da informação.

- Gerenciar e controlar as redes.
  - Separar, onde apropriado, a responsabilidade operacional pela rede da operação dos recursos computacionais.
  - Estabelecer responsabilidades e procedimentos sobre o gerenciamento de equipamentos remotos.
  - Estabelecer controles especiais de proteção dos dados que trafegam sobre as redes públicas e sem fio (*wireless*), bem como dos sistemas e aplicações a elas conectados.
  - Aplicar mecanismos de registro e monitoração que habilite a gravação de ações relevantes de segurança.
  - Gerenciar os serviços de rede e assegurar que os controles estejam aplicados de forma consistente.
- Identificar e incluir nos acordos de serviço de rede as características de segurança, os níveis de serviço e os requisitos de gerenciamento.
- Implementar procedimentos visando o gerenciamento das mídias removíveis.
- Realizar o descarte das mídias desnecessárias de forma segura e por meio de procedimentos formais.
- Estabelecer procedimentos para o tratamento e armazenamento das informações.
- Proteger a documentação dos sistemas contra acessos não autorizados.
- Estabelecer e formalizar políticas, procedimentos e controles visando proteger a troca de informações em todos os recursos de comunicação.
- Estabelecer acordos para troca de informações e *softwares* entre a organização e entidades externas.

- Proteger mídias em trânsito contra acesso não autorizado, uso impróprio ou alteração indevida.
- Proteger as mensagens eletrônicas.
- Desenvolver e implementar políticas e procedimentos visando proteger as informações associadas com a interconexão dos sistemas de informação do negócio.
  - Identificar e tratar as vulnerabilidades existentes nos sistemas que compartilham informações com outros setores da organização.
  - Identificar e tratar as vulnerabilidades nos sistemas de comunicação do negócio.
  - Estabelecer política e controles para gerenciar o compartilhamento de informações.
  - Restringir o acesso às informações sensíveis.
  - Categorizar as pessoas autorizadas a utilizarem os sistemas, bem como determinar os locais de onde poderão realizar tal acesso.
  - Restringir os recursos selecionados para categorias específicas de usuários.
  - Gerenciar a retenção e cópias de segurança das informações mantidas no sistema.
  - Estabelecer requisitos e procedimentos para recuperação e contingência.
- Proteger as informações de comércio eletrônico que transitam em redes públicas de atividades fraudulentas, disputas contratuais, e divulgação e modificações não autorizadas.
  - Identificar o nível de confiança que cada parte requer na suposta identidade de outros.
  - Realizar processos de autorização com quem pode determinar preços, emitir ou assinar documentos-chave de negociação.
  - Garantir que parceiros comerciais estejam completamente informados de suas autorizações.
  - Determinar e atender requisitos de confidencialidade, integridade, evidências de emissão e recebimento de documentos-chave, e a não-repudiação de contratos.

- Estabelecer o nível de confiança requerido na integridade das listas de preços anunciadas.
- Prevenir contra perda ou duplicação de informação de transações.
- Imputar responsabilidades associadas com quaisquer transações fraudulentas.
- Estabelecer os requisitos de seguro.
- Realizar acordo formal que comprometa ambas as partes aos termos da transação.

- Proteger informações envolvidas em transações on-line.
  - Utilizar assinaturas eletrônicas para cada uma das partes envolvidas na transação.
  - Validar e verificar as credenciais de usuário para todas as partes.
  - Manter a confidencialidade da transação.
  - Manter a privacidade de todas as partes envolvidas.
  - Criptografar o caminho de comunicação entre todas as partes envolvidas.
  - Utilizar protocolos de comunicação seguros.
  - Armazenar detalhes da transação em locais onde não esteja publicamente acessível.
- Proteger a integridade das informações disponibilizadas em sistemas publicamente acessíveis.
  - Testar os sistemas acessíveis publicamente antes da disponibilização da informação.
  - Realizar processo formal de aprovação antes que uma informação seja publicada.
  - Controlar os sistemas de publicação eletrônica.
- Monitorar os sistemas e registrar os eventos de segurança da informação.
- Utilizar os registros (*log*) de operador e de falhas para identificar problemas nos sistemas de informação.
- Realizar as atividades de registro de monitoramento de acordo com os requisitos legais.
- Produzir e manter por um período acordado os registros (*log*) de auditoria

contendo as atividades dos usuários, exceções e outros eventos de segurança da informação.

- Estabelecer procedimentos para o monitoramento do uso dos recursos de processamento da informação, analisando criticamente os resultados de tal monitoramento.
- Proteger os recursos e informações de registros (*log*) contra falsificação e acesso não autorizado.
- Registrar as atividades dos administradores e operadores.
- Registrar e analisar as falhas ocorridas, adotando ações apropriadas.
- Estabelecer regras claras para o tratamento de falhas informadas.
- Sincronizar, de acordo com uma hora oficial, todos os relógios dos sistemas de processamento das informações relevantes.

Saídas do processo:

- Procedimentos de operação dos sistemas.
- Regras para a transferência do *software* da situação de desenvolvimento para a de produção.
- Critérios para a aceitação de novos sistemas, atualizações e novas versões.
- Política proibindo o uso de *software* não autorizado.
- Política com orientações sobre a importação de arquivos e *softwares* oriundos de redes externas ou qualquer outro meio.
- Planos de continuidade do negócio adequados para a recuperação em caso de ataques por códigos maliciosos.
- Procedimentos visando o gerenciamento das mídias removíveis.
- Procedimentos para o descarte de mídias.
- Procedimentos para o tratamento e armazenamento das informações.
- Frequência de geração das cópias de segurança.
- Políticas, procedimentos e controles visando proteger a troca de informações em todos os recursos de comunicação.
- Acordos para troca de informações e *softwares* entre a organização e entidades externas.

- Políticas e procedimentos visando proteger as informações associadas com a interconexão dos sistemas de informação do negócio.
- Política e controles para gerenciar o compartilhamento de informações.
- Requisitos e procedimentos para recuperação e contingência.
- Procedimentos para o monitoramento do uso dos recursos de processamento da informação.
- Regras para o tratamento de falhas informadas.
- Operações e comunicações gerenciadas.

3.1.10 Controle de Acessos

Objetivos do processo: controlar o acesso à informação, assegurar acesso de usuário autorizado e prevenir acesso não autorizado aos sistemas de informação, bem como evitar o comprometimento ou roubo da informação e dos recursos de processamento da informação.

Entradas do processo:

- Política de segurança da informação.
- Diretrizes e normas sobre a segurança da informação.
- Metas, escopo, objetivos e importância da segurança da informação.
- Requisitos legais, regulamentares, estatutários e contratuais.
- Plano de tratamento de riscos (requisitos de segurança).

Atividades realizadas:

- Estabelecer, documentar e analisar criticamente a política de controle de acessos.
- Estabelecer procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços.
- Restringir e controlar a concessão e uso dos privilégios.
- Controlar, por meio de processo de gerenciamento formal, a concessão de senhas.
- Conduzir em intervalos regulares, por meio de processo formal, a análise crítica dos direitos de acesso dos usuários.
- Solicitar aos usuários que sigam as boas práticas de segurança da informação na seleção e uso de senhas.
- Assegurar que os equipamentos não monitorados tenham proteção adequada.

- Adotar política de mesa limpa e tela limpa.
- Formular uma política relativa ao uso de redes e serviços de rede.
- Utilizar métodos apropriados de autenticações para controlar acesso de usuários remotos.
- Considerar as identificações automáticas de equipamentos como um meio de autenticar conexões vindas de localizações e equipamentos específicos.
- Controlar o acesso físico e lógico das portas de diagnóstico e configuração.
- Segregar em redes os grupos de serviços de informação, usuários e sistemas de informação.
- Restringir a capacidade de conexão dos usuários à rede, de acordo com a política de controle de acessos e os requisitos das aplicações.
- Implementar controle de roteamento na rede.
- Controlar o acesso aos sistemas operacionais por um procedimento seguro de entrada (*log-on*).
- Escolher e utilizar uma técnica adequada de identificação e autenticação dos usuários.
- Implementar o sistema de gerenciamento de senhas que sejam interativos e assegurem senhas de qualidade.
- Restringir e controlar o uso de programas utilitários de sistema.
- Encerrar seções após um período definido de inatividade.
- Restringir os horários de conexão.
- Restringir e controlar, de acordo com a política de acessos, o acesso à informação e às funções dos sistemas de aplicações por usuários e pessoal de suporte.
- Isolar o ambiente computacional dos sistemas sensíveis.
- Estabelecer uma política e implementar medidas de proteção contra os riscos do uso dos recursos de computação e comunicações móveis.
- Desenvolver e implementar política, planos operacionais e procedimentos para atividades de trabalho remoto.

Saídas do processo:

- Política de controle de acessos.

- Procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços.
- Política de mesa limpa e tela limpa.
- Política de uso de redes e serviços de rede.
- Política, planos operacionais e procedimentos para atividades de trabalho remoto.
- Política e medidas de proteção contra os riscos do uso dos recursos de computação e comunicações móveis.
- política, planos operacionais e procedimentos para atividades de trabalho remoto.
- Acessos controlados.

3.1.11 Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

Objetivos do processo: garantir que a segurança é parte integrante dos sistemas de informação; prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações; proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos; garantir a segurança de arquivos de sistema; manter a segurança de sistemas aplicativos e da informação e reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.

Entradas do processo:

- Política de segurança da informação.
- Diretrizes e normas sobre a segurança da informação.
- Metas, escopo, objetivos e importância da segurança da informação.
- Requisitos legais, regulamentares, estatutários e contratuais.
- Plano de tratamento de riscos (requisitos de segurança).

Atividades realizadas:

- Especificar e analisar os requisitos para controles de segurança em novos sistemas de informação ou melhorias em sistemas existentes.
- Validar os dados de entrada das aplicações, visando garantir que são corretos e apropriados.
- Incorporar, nas aplicações, checagem de validação, visando detectar informações corrompidas.

- Identificar os requisitos para garantir a autenticidade e proteger a integridade das mensagens em aplicações, bem como identificar e implementar os controles apropriados.
- Realizar a validação dos dados de saída das aplicações.
- Desenvolver e implementar uma política para o uso de controles criptográficos para a proteção da informação.
- Implantar um processo de gerenciamento de chaves criptográficas.
- Proteger as chaves criptográficas contra modificação, perda e destruição.
- Implementar procedimentos para controlar a instalação de *software* em sistemas operacionais.
- Selecionar com cuidado, proteger e controlar os dados de teste.
- Restringir o acesso ao código-fonte de programa.
- Controlar a implementação de mudanças por meio de procedimentos formais de controle de mudanças.
- Analisar criticamente e testar as aplicações críticas de negócios, quando sistemas operacionais são mudados.
- Controlar as modificações em pacotes de *softwares*.
- Prevenir as oportunidades para vazamento de informações.
- Supervisionar e monitorar o desenvolvimento terceirizado de *software*.
- Obter informação em tempo hábil sobre vulnerabilidades técnicas dos sistemas de informação em uso, avaliar a exposição da organização a estas vulnerabilidades e tomar as medidas apropriadas para lidar com os riscos associados.

Saídas do processo:

- Política para o uso de controles criptográficos.
- Processo de gerenciamento de chaves.
- Procedimentos formais de controle de mudanças.
- Aquisição, desenvolvimento e manutenção dos sistemas de informação, controlados.

3.1.12 Gestão de Incidentes de Segurança da Informação

Objetivos do processo: assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil, bem como aplicar um enfoque consistente e efetivo à gestão de incidentes de segurança da informação.

Entradas do processo:

- Política de segurança da informação.
- Diretrizes e normas sobre a segurança da informação.
- Metas, escopo, objetivos e importância da segurança da informação.
- Requisitos legais, regulamentares, estatutários e contratuais.
- Plano de tratamento de riscos (requisitos de segurança).

Atividades realizadas:

- Estabelecer canais apropriados e procedimentos para que os eventos de segurança da informação sejam relatados formalmente.
- Estabelecer procedimentos de resposta a incidentes notificados.
- Instruir funcionários, fornecedores e terceiros a registrar e notificar qualquer fragilidade em sistemas ou serviços.
- Estabelecer responsabilidades e procedimentos de gestão, visando assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação.
- Estabelecer mecanismos para permitir que tipos, quantidades e custos dos incidentes de segurança da informação sejam quantificados e monitorados.
- Coletar, armazenar e apresentar as evidências, de acordo com a normatização existente para este fim, nos casos de acompanhamento após um incidente de segurança da informação.

Saídas do processo:

- Canais e procedimentos de notificação de eventos de segurança e fragilidades detectadas.
- Procedimentos de resposta a incidentes notificados.
- Responsabilidades e procedimentos de gestão dos incidentes de segurança da

informação.

- Mecanismos para quantificar e monitorar os incidentes de segurança da informação.
- Incidentes de segurança da informação gerenciados.

3.1.13 Gestão da Continuidade do Negócio

Objetivos do processo: não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso.

Entradas do processo:

- Política de segurança da informação.
- Diretrizes e normas sobre a segurança da informação.
- Metas, escopo, objetivos e importância da segurança da informação.
- Requisitos legais, regulamentares, estatutários e contratuais.
- Plano de tratamento de riscos (requisitos de segurança).

Atividades realizadas:

- Incluir a segurança da informação no processo de gestão de continuidade do negócio, contemplando os requisitos de segurança da informação necessários.
  - Entender os riscos a que a organização está exposta, identificando e priorizando os processos críticos do negócio.
  - Identificar os ativos envolvidos nos processos críticos do negócio.
  - Entender o impacto que incidentes de segurança da informação provavelmente terão sobre os negócios.
  - Considerar a contratação de seguro compatível como parte integrante do processo de continuidade do negócio.
  - Identificar e considerar a implementação de controles preventivos e de mitigação.
  - Identificar os recursos financeiros, organizacionais, técnicos e ambientais suficientes para identificar os requisitos de segurança da informação.
  - Garantir a segurança de pessoal e proteção de recursos de processamento

das informações e bens da organização.

  - Detalhar e documentar os planos de continuidade de negócio que contemplem os requisitos de segurança da informação alinhados com a estratégia da continuidade do negócio estabelecida.
  - Testar e atualizar regularmente os planos e processos implantados.
  - Garantir que a gestão da continuidade do negócio esteja incorporada aos processos e estrutura da organização.
  - Atribuir responsabilidade pela coordenação do processo de gestão de continuidade de negócios em um nível adequado dentro da organização.

- Identificar os eventos que podem causar interrupções aos processos de negócio, a probabilidade de ocorrência, o impacto de tais interrupções e as consequências para a segurança de informação.
- Desenvolver e implementar planos para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos do negócio.
- Manter uma estrutura básica dos planos de continuidade do negócio que contemplem os requisitos de segurança da informação.
- Testar e atualizar regularmente os planos de continuidade do negócio.

Saídas do processo:

- Responsabilidades pela coordenação do processo de gestão de continuidade de negócios.
- Planos de continuidade do negócio.
- Continuidade do negócio gerenciada.

3.1.14 Conformidade

Objetivos do processo: evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação, bem como garantir a conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação.

Entradas do processo:

- Política de segurança da informação.
- Diretrizes e normas sobre a segurança da informação.
- Metas, escopo, objetivos e importância da segurança da informação.
- Requisitos legais, regulamentares, estatutários e contratuais.
- Plano de tratamento de riscos (requisitos de segurança).

Atividades realizadas:

- Definir, documentar e manter atualizados, para cada sistema de informação da organização, os requisitos legais, estatutários, regulamentares e contratuais relevantes, bem como o enfoque da organização para atender a esses requisitos.
- Definir e documentar controles específicos e as responsabilidades individuais para atender aos requisitos legais, estatutários, regulamentares e contratuais.
- Implementar procedimentos apropriados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais no uso de material, em relação aos quais pode haver direitos de propriedade intelectual e sobre o uso de produtos de *software* proprietários.
    - Divulgar uma política de conformidade com os direitos de propriedade intelectual que defina o uso legal de produtos de *software* e de informação.
    - Adquirir *software* somente por meio de fontes conhecidas e de reputação.
    - Manter conscientização das políticas para proteger os direitos de propriedade intelectual e notificar a intenção de tomar ações disciplinares contra pessoas que violarem essas políticas.
    - Manter de forma adequada os registros de ativos e identificar todos os ativos com requisitos para proteger os direitos de propriedade intelectual.
    - Manter provas e evidências da propriedade de licenças.
    - Implementar controles para assegurar que o número máximo de usuários permitidos não excede o número de licenças adquiridas.
    - Conduzir verificações para que somente produtos de *software* autorizados e licenciados sejam instalados.
    - Estabelecer uma política para a manutenção das condições adequadas de licenças.

- Estabelecer uma política para disposição ou transferência de *software* para outros.
- Utilizar ferramentas de auditoria apropriadas.
- Cumprir termos e condições para *software* e informação obtidos a partir de redes públicas.

- Proteger os registros importantes da organização contra perda, destruição e falsificação, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio.
  - Emitir diretrizes gerais para retenção, armazenamento, tratamento e disposição de registros e informações.
  - Elaborar uma programação para retenção, identificando os registros essenciais e o período que cada um deve ser mantido.
  - Manter um inventário das fontes de informações-chave.
  - Implementar controles apropriados para proteger registros e informações contra perda, destruição e falsificação.
- Assegurar a privacidade e proteção de dados conforme exigido nas legislações relevantes, regulamentações e, se aplicável, nas cláusulas contratuais.
- Prevenir o mau uso dos recursos de processamento da informação.
  - Conscientizar os usuários do escopo preciso de suas permissões de acesso e da monitoração realizada para detectar o uso não autorizado.
- Utilizar controles de criptografia em conformidade com todas as leis, acordos e regulamentações relevantes.
- Garantir que todos os procedimentos de segurança da informação estão sendo executados corretamente para atender à conformidade com as normas e políticas de segurança da informação.
- Registrar e manter os resultados das análises críticas e das ações corretivas realizadas.
- Verificar periodicamente os sistemas de informação em sua conformidade técnica com as normas de segurança da informação implementadas.
- Planejar e acordar os requisitos e atividades de auditoria envolvendo verificação nos sistemas operacionais, visando minimizar os riscos de interrupção dos

processos do negócio.

- Proteger o acesso às ferramentas de auditoria de sistema de informação.
- Planejar e implementar um programa de auditorias, visando verificar os objetivos de controle, controles, processos e procedimentos do sistema de gestão da segurança da informação.
- Definir e documentar as responsabilidades e os requisitos para planejamento e para execução de auditorias e para relatar os resultados e a manutenção dos registros.

Saídas do processo:

- Requisitos estatutários, regulamentares e contratuais relevantes, bem como o enfoque da organização para atender a esses requisitos, para cada sistema de informação.
- Controles específicos e as responsabilidades individuais para atender aos requisitos estatutários, regulamentares e contratuais.
- Procedimentos apropriados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais no uso de material, em relação aos quais pode haver direitos de propriedade intelectual e sobre o uso de produtos de *software* proprietários.
- Política de conformidade com os direitos de propriedade intelectual.
- Controles para assegurar que o número máximo de usuários permitidos não excede o número de licenças adquiridas.
- Política para a manutenção das condições adequadas de licenças.
- Política para disposição ou transferência de *software* para outros.
- Diretrizes gerais para retenção, armazenamento, tratamento e disposição de registros e informações.
- Programação para retenção, identificando os registros essenciais e o período que cada um deve ser mantido.
- Inventário das fontes de informações-chave.
- Controles para proteger registros e informações contra perda, destruição e falsificação.
- Programa de auditorias.

- Relatórios de auditorias realizadas.

3.1.15 Análise Crítica do Sistema de Gestão da Segurança da Informação (SGSI)

Objetivo do processo: assegurar a contínua pertinência, adequação e eficácia do SGSI.

Entradas do processo:

- Resultados de auditorias do SGSI e análises críticas.
- Realimentação das partes interessadas.
- Técnicas, produtos ou procedimentos que podem ser usados na organização para melhorar o desempenho e a eficácia do SGSI.
- Situação das ações preventivas e corretivas.
- Vulnerabilidades ou ameaças não contempladas adequadamente nas análises/avaliações de risco anteriores.
- Resultados da eficácia das medições.
- Acompanhamento das ações oriundas de análises críticas anteriores pela direção.
- Quaisquer mudanças que possam afetar o SGSI.
- Recomendações para melhoria.

Atividades realizadas:

- Avaliar a política de segurança da informação.
- Avaliar os objetivos de segurança da informação.
- Avaliar a adequabilidade e eficácia dos controles de segurança da informação implementados.
- Avaliar a necessidade de mudanças no SGSI.
- Avaliar a oportunidade para melhorias do SGSI.
- Documentar e manter os registros dos resultados da análise crítica.

Saídas do processo:

- Melhoria da eficácia do SGSI.
- Atualização da análise/avaliação de riscos e do plano de tratamento de riscos.
- Modificação de procedimentos e controles que afetem a segurança da informação,

quando necessário, para responder a eventos internos ou externos que possam impactar no SGSI.

- Necessidade de recursos.
- Melhoria de como a eficácia dos controles está sendo medida.

3.2 Modos de Aplicação do Modelo de Sistema de Gestão da Segurança da Informação

O modelo apresentado serve de guia de orientação na implementação de um SGSI, bem como de verificação da conformidade de um sistema implementado, possibilitando analisar o nível de aderência, que representa o grau de conformidade dos processos existentes ao que está preconizado nas normas ABNT NBR ISO/IEC 27001, 27002 e 27005.

Portanto, a visão do sistema de maneira global e centralizada, com a descrição detalhada de cada processo, se constitui um elemento facilitador no gerenciamento da segurança da informação de uma organização.

Um exemplo de aplicação do modelo na verificação do nível de aderência do SGSI de uma organização às normas mencionadas acima, é contemplado no capítulo 4 deste trabalho.

Capítulo 4

Aplicação do Modelo de Sistema de Gestão da Segurança a Informação

O modelo de sistema de gestão da segurança da informação proposto foi aplicado na verificação do nível de aderência do gerenciamento da segurança da informação de uma organização às normas ABNT NBR ISO/IEC, que serviram de base para confecção do modelo.

A verificação da situação da organização foi realizada por meio da análise de documentos e arquivos, entrevista com pessoas que integram as diversas áreas da organização e observação direta dos sistemas de informação junto ao ambiente organizacional.

Para quantificar o nível de aderência da organização ao que está preconizado nas normas contempladas pelo modelo, as atividades que compõem os diversos processos que fazem parte do sistema de gestão da segurança da informação, descritas no capítulo 3, foram valoradas de duas maneiras, conforme abaixo descritas:

- **Ponderação quanto ao grau de relevância:** determina o valor que cada atividade representa para o negócio da organização, conforme especificado na Tabela 4.1.
- **Valoração quanto ao nível de implementação:** refere-se ao valor atribuído para cada atividade de acordo com seu nível de implementação por parte da organização, conforme discriminado na Tabela 4.2.

Tabela 4.1 – Ponderação do Grau de Relevância das Atividades.

GRAU DE RELEVÂNCIA	VALOR
Nenhuma relevância	0
Baixa relevância	1
Média relevância	2
Alta relevância	3

Tabela 4.2 – Valoração do Nível de Implementação das Atividades.

NÍVEL DE IMPLEMENTAÇÃO	VALOR
Não implementada	0
Implementação parcial baixa	1
Implementação parcial alta	2
Implementação total	3

Para tornar possível o cômputo do nível de aderência das atividades de cada processo, houve a necessidade de estabelecer um valor de referência (*VR*), que representa a situação julgada ideal para aquela organização específica. Tal valor de referência foi obtido por meio da seguinte equação:

$$VR = GR \times 3 \tag{4.1}$$

onde *GR* representa o grau de relevância da atividade para a organização (Tabela 4.1) e a constante 3 refere-se à valoração máxima possível da Tabela 4.2, ou seja, atividade com nível de implementação total.

Por meio da pesquisa junto ao ambiente organizacional, obteve-se o valor apurado (*VA*) para cada atividade, que foi calculado utilizando a equação a seguir:

$$VA = GR \times NI \tag{4.2}$$

onde *GR* representa o grau de relevância da atividade para a organização (Tabela 4.1) e *NI* refere-se ao nível de implementação da referida atividade (Tabela 4.2).

O nível de aderência da atividade (*NAa*) é obtido pela comparação do valor apurado (*VA*) com o valor de referência (*VR*), sendo expresso em termos percentuais por meio da equação abaixo:

$$NAa = \frac{VA}{VR} \times 100 \tag{4.3}$$

O nível de aderência de cada processo (*NAp*), em termos percentuais, foi calculado por meio da seguinte equação:

$$NAp = \frac{\sum VA}{\sum VR} \times 100 \quad (4.4)$$

4.1 Dados sobre a Organização

A organização avaliada possui 1.200 integrantes e com abrangência nacional.

Seus processos são suportados por sistemas de informação, que são gerenciados por um departamento de tecnologia da informação. Dessa forma, os sistemas de informação são críticos para que a organização continue a cumprir a missão para qual é destinada.

A organização trabalha com os mais diversos tipos de informação, que exigem requisitos de segurança diferenciados.

4.2 Situação Encontrada no SGSI da Organização

4.2.1 Processo de Implementação, Manutenção e Melhoria do SGSI

A Tabela 4.3 apresenta a situação do SGSI da organização no que se refere ao processo de implementação, manutenção e melhoria do sistema. Os dados sobre cada atividade integrante deste processo foram obtidos por meio de consulta a documentos e entrevista com pessoas relacionadas com a segurança da informação da organização.

Tabela 4.3 - Implementação, Manutenção e Melhoria do Sistema de Gestão da Segurança da Informação (SGSI).

Atividade	Grau de relevância	Nível de implementação	Valor de referência	Valor apurado	Nível de aderência
Estabelecer o sistema de gestão da segurança da informação (SGSI), definindo seu escopo e limites	3	2	9	6	66,66%

Definir e aprovar a política do SGSI, contemplando a definição dos objetivos, direcionamento e princípios para ações voltadas à segurança da informação, bem como os critérios de avaliação de riscos, de impacto e de aceitação do risco	3	2	9	6	66,66%
Estabelecer uma estrutura que possibilite a implementação da segurança da informação dentro da organização	3	2	9	6	66,66%
Aprovar e analisar criticamente a política de segurança da informação	3	1	9	3	33,33%
Assegurar que as metas da segurança da informação estão identificadas e atendem aos requisitos da organização	3	1	9	3	33,33%
Atribuir funções e responsabilidades para a segurança da informação	3	1	9	3	33,33%
Prover os recursos necessários à segurança da informação	3	2	9	6	66,66%
Coordenar a implementação da segurança da informação na organização	3	2	9	6	66,66%
Comprometimento da direção, por meio de manifestação clara de apoio, com a segurança da informação	3	1	9	3	33,33%
Implementar planos e programas de conscientização e treinamento quanto à segurança da informação	3	2	9	6	66,66%
Assegurar que a implementação dos controles de segurança da informação sejam coordenados e permeiam toda a organização	3	2	9	6	66,66%
Determinar as competências necessárias para o pessoal que executa tarefas que afeta os SGSI	3	2	9	6	66,66%
Constituir grupo responsável pelo gerenciamento da segurança da informação na organização	3	1	9	3	33,33%
Aprovar a metodologia de gestão de riscos de segurança da informação	3	0	9	0	0,00%
Aprovar metodologias e processos para a segurança da informação	3	2	9	6	66,66%

Conduzir auditorias internas do SGSI em intervalos planejados, visando avaliar a conformidade dos objetivos de controle, dos controles e dos procedimentos adotados	3	0	9	0	0,00%
Executar ações corretivas e preventivas no sistema de gestão de segurança da informação, tomando-se como base o resultado de auditorias, o resultado da análise crítica do sistema ou qualquer outra informação pertinente	3	1	9	3	33,33%
Definir e documentar os procedimentos para as ações corretivas	3	1	9	3	33,33%
Identificar a não-conformidade	3	1	9	3	33,33%
Determinar as causas da não-conformidade	3	3	9	9	100,00%
Avaliar a necessidade de ações para evitar a ocorrência da não-conformidade	3	3	9	9	100,00%
Determinar e implementar as ações corretivas necessárias	3	3	9	9	100,00%
Registrar os resultados das ações corretivas executadas	3	2	9	6	66,66%
Obter autorização da direção para implementar e operar o SGSI	3	3	9	9	100,00%
Proteger e controlar os documentos requeridos pelo SGSI	3	2	9	6	66,66%
Estabelecer procedimentos documentados para definir ações a serem realizadas no gerenciamento de documentos	3	1	9	3	33,33%
Estabelecer e manter os registros de desempenho dos processos e da ocorrência de incidentes de segurança no SGSI	3	1	9	3	33,33%
T O T A L			243	132	**54,32%**

Da análise do SGSI da organização referente a este processo, não foi possível verificar a existência de um sistema estabelecido formalmente, com políticas específicas para a organização, diretrizes, procedimentos e responsabilidades documentadas, visando o gerenciamento da segurança da organização. As ações voltadas para a segurança da informação são realizadas de forma empírica, sem um processo de gestão de riscos que o suporte.

4.2.2 Processo de Organização da Segurança da Informação

A situação do SGSI da organização, no que se refere ao processo de organização da segurança da informação é demonstrada na Tabela 4.4. Os dados relacionados às atividades deste processo foram obtidos por meio de consulta a documentos e arquivos, da realização de entrevista com pessoas que integram os diversos sistemas de informação e da observação direta destes sistemas.

Tabela 4.4 – Organização da Segurança da Informação.

Atividade	Grau de relevância	Nível de implementação	Valor de referência	Valor apurado	Nível de Aderência
Elaborar a política de segurança da informação	3	2	9	6	66,66%
Garantir que as atividades de segurança da informação são realizadas de acordo com a política de segurança da informação, identificando como conduzir as não-conformidades	3	2	9	6	66,66%
Definir metodologias e processos para a segurança da informação	3	2	9	6	66,66%
Avaliar a adequação e coordenar a implementação dos controles, processo e procedimentos de segurança da informação	3	2	9	6	66,66%
Promover a educação, treinamento e conscientização em segurança da informação na organização	3	2	9	6	66,66%
Avaliar as informações recebidas sobre incidentes de segurança da informação, recomendando as ações a serem executadas como resposta	3	2	9	6	66,66%
Definir claramente as responsabilidades pela segurança da informação	3	1	9	3	33,33%
Definir e implementar um processo de gestão de autorização para novos recursos de processamento da informação	3	1	9	3	33,33%

Identificar e analisar criticamente os requisitos para a confidencialidade e os acordos de não divulgação, de acordo com as necessidades de proteção das informações da organização	3	3	9	9	100,00%
Manter contatos com pessoal externo (especialistas, grupos e autoridades) visando o tratamento de assuntos relacionados à segurança da informação	3	2	9	6	66,66%
Analisar criticamente a segurança da informação organizacional, registrando os resultados de tal análise	3	1	9	3	33,33%
Controlar o acesso de partes externas aos ativos de informação da organização	3	3	9	9	100,00%
Verificar o atendimento aos requisitos de segurança da informação da organização nos acordos realizados com terceiros	2	3	6	6	100,00%
T O T A L			114	75	**65,79%**

Os pontos considerados relevantes em relação a este processo são:

- Ausência de definição formal de responsabilidades pela segurança da informação.
- Inexistência de um processo de gestão de autorização para novos recursos de processamento da informação.
- Falta de implementação de mecanismos que possibilitem uma análise crítica da segurança da informação da organização, bem como o registro dos resultados de tal análise.

4.2.3 Processo de Política de Segurança da Informação

Os dados sobre as atividades deste processo foram levantados por meio da consulta aos documentos e arquivos publicados por órgãos superiores e pela própria organização, com a finalidade de normatizar procedimentos e estabelecer diretrizes sobre a segurança da informação. A Tabela 4.5 demonstra a situação em que se encontra o processo de política de segurança da informação.

Tabela 4.5 – Política de Segurança da Informação.

Atividade	Grau de relevância	Nível de implementação	Valor de referência	Valor apurado	Nível de aderência
Estabelecer a política de segurança da informação	3	2	9	6	66,66%
Definir metas, escopo, objetivos e importância da segurança da informação	3	2	9	6	66,66%
Definir a estrutura de estabelecimento dos objetivos de controles e controles de segurança da informação	3	2	9	6	66,66%
Definir critérios de segurança	3	1	9	3	33,33%
Definir a estrutura e metodologia do sistema de gestão de riscos	3	0	9	0	0,00%
Definir requisitos de conformidade da segurança da informação	3	3	9	9	100,00%
Definir responsabilidades na gestão da segurança da informação	3	1	9	3	33,33%
Realizar a abordagem das políticas, princípios, normas e requisitos de segurança da informação da organização	3	3	9	9	100,00%
Abordar as consequências das violações da política de segurança da informação	3	3	9	9	100,00%
Documentar a política de segurança da informação	3	2	9	6	66,66%
Submeter a política de segurança da informação à aprovação por parte da direção	3	3	9	9	100,00%
Publicar e comunicar a política de segurança da informação às partes interessadas	3	3	9	9	100,00%
Analisar criticamente a política de segurança da informação	3	2	9	6	66,66%
Melhorar a política de segurança da informação	3	2	9	6	66,66%
T O T A L			126	87	**69,00%**

A organização não possui uma política de segurança da informação consolidada em um documento único e que tenha sido elaborada pela própria organização. As diretrizes estabelecidas, no que se refere à segurança da informação, estão dispersas em diversos documentos publicados por órgãos superiores e como parte de outros documentos confeccionados na própria organização.

Os critérios de segurança da informação, bem como as responsabilidades pela segurança da informação, não são definidos formalmente.

4.2.4 Processo de Gestão de Riscos de Segurança da Informação

As fontes dos dados sobre as atividades deste processo foram documentos (normas e políticas) publicados pela organização, bem como aqueles publicados por órgãos superiores aos quais a organização está subordinada. Os dados foram obtidos, também, por meio de entrevista com pessoas que integram os sistemas de informação da organização. A situação atual da organização neste processo é demonstrada na Tabela 4.6.

Tabela 4.6 – Gestão de Riscos de Segurança da Informação.

Atividade	Grau de relevância	Nível de implementação	Valor de referência	Valor apurado	Nível de Aderência
Definir o contexto da gestão de riscos de segurança da informação	3	1	9	3	33,33%
Definição do escopo e limites do processo de gestão de riscos de segurança da informação	3	1	9	3	33,33%
Definir os critérios de avaliação de riscos	3	0	9	0	0,00%
Definir os critérios de impacto	3	0	9	0	0,00%
Definir os critérios de aceitação do risco	3	0	9	0	0,00%
Estabelecer a organização e responsabilidades para operar o processo de gestão de riscos	3	1	9	3	33,33%
Verificar a disponibilidade de recursos para operar o processo de gestão de riscos	3	1	9	3	33,33%
Analisar os riscos	3	1	9	3	33,33%
Identificar os riscos	3	1	9	3	33,33%
Identificar os ativos	3	3	9	9	100,00%
Identificar as ameaças	3	1	9	3	33,33%
Identificar os controles existentes	3	2	9	6	66,66%
Identificar as vulnerabilidades	3	1	9	3	33,33%
Identificar as consequências	3	0	9	0	0,00%
Estimar os riscos	3	0	9	0	0,00%
Avaliar as consequências	3	0	9	0	0,00%
Avaliar a probabilidade dos incidentes	3	0	9	0	0,00%
Estimar o nível do risco	3	0	9	0	0,00%
Avaliar os riscos	3	0	9	0	0,00%

Elaborar o relatório de análise e avaliação de riscos	3	0	9	0	0,00%
Aceitar os riscos	3	0	9	0	0,00%
Elaborar a lista de ricos aceitos, incluindo uma justificativa para aqueles que não satisfaçam os critérios normais para aceitação do risco	3	0	9	0	0,00%
Obter autorização da direção sobre os riscos residuais propostos	3	0	9	0	0,00%
Definir o plano de tratamento de riscos	3	1	9	3	33,33%
Obter aprovação do plano de tratamento de riscos	3	1	9	3	33,33%
Preparar uma declaração de aplicabilidade contendo os objetivos de controle e os controles selecionados, os objetivos de controles e controles já implementados e a justificativa para exclusão de qualquer objetivo de controle e controle constantes da norma ABNT 27002	3	0	9	0	0,00%
Implementar mecanismos que possibilitem a comunicação dos riscos	3	0	9	0	0,00%
Monitorar e analisar criticamente os riscos	3	1	9	3	33,33%
Manter e melhorar o processo de gestão de riscos de segurança da informação	3	1	9	3	33,33%
T O T A L			261	51	**19,54%**

A gestão de riscos de segurança da informação não é tratada de maneira sistematizada e metódica no âmbito organizacional. Sua implementação se dá de maneira empírica, sem qualquer planejamento ou estudo prévio para este fim.

Este tema não é contemplado nas diretrizes e políticas internas da organização. Apenas instruções gerais publicadas pelas entidades superiores à organização trata, de maneira parcial, o assunto em questão.

4.2.5 Processo de Assessoria Jurídica

Os dados sobre as atividades deste processo foram obtidos por meio de consulta a documentos publicados, entrevista com pessoas que integram os sistemas de informação e pela

observação direta da seção de assessoria jurídica da organização. A Tabela 4.7 apresenta a situação atual do processo de assessoria jurídica.

Tabela 4.7 – Assessoria Jurídica.

Atividade	Grau de relevância	Nível de implementação	Valor de referência	Valor apurado	Nível de Aderência
Receber as diretrizes gerais e objetivos da segurança da informação da organização, descritos na política de segurança da informação	3	3	9	9	100,00%
Reunir as leis, estatutos, regulamentos e contratos atinentes às atividades de negócio da organização	3	3	9	9	100,00%
Receber as informações constantes do plano de tratamento do risco	3	0	9	0	0,00%
Atuar de forma consultiva orientando gestor e colaboradores sobre questões jurídicas	3	2	9	6	66,66%
Atuar de forma colaborativa compondo grupos de trabalhos, assessorando o gestor e orientando equipes	3	1	9	3	33,33%
Atuar de forma contenciosa em processos administrativos e em matéria judicial	3	3	9	9	100,00%
T O T A L			54	36	**66,66%**

A assessoria jurídica da organização atua de forma colaborativa, apenas, no assessoramento em processos administrativos e como órgão de consulta para determinadas situações. A seção de assessoria jurídica não participa de maneira ativa como parte integrante do sistema de gestão da segurança da informação da organização.

4.2.6 Processo de Gestão de Ativos de Informação

O resultado da análise deste processo é apresentado na Tabela 4.8. Os dados sobre as atividades que compõem o processo foram obtidos por meio de consulta a documentos e arquivos existentes na organização, entrevista com pessoas e pela observação direta dos diversos setores da organização.

Tabela 4.8 – Gestão de Ativos de Informação.

Atividade	Grau de relevância	Nível de implementação	Valor de referência	Valor apurado	Nível de aderência
Identificar os ativos	3	3	9	9	100,00%
Estruturar e manter o inventário de todos os ativos importantes	3	3	9	9	100,00%
Documentar a importância de cada ativo	3	0	9	0	0,00%
Realizar a valoração dos ativos	3	0	9	0	0,00%
Avaliar o impacto causado pelo incidente de segurança ocorrido em cada ativo	3	0	9	0	0,00%
Assegurar a existência de um proprietário, responsável por cada ativo identificado	3	3	9	9	100,00%
Identificar, documentar e implementar regras quanto ao uso das informações e de seus ativos associados	3	2	9	6	66,66%
Classificar a informação de acordo com o seu valor, requisitos legais, sensibilidade e criticidade	3	2	9	6	66,66%
Definir e implementar procedimentos para rotulação e tratamento da informação de acordo com a sua classificação	3	2	9	6	66,66%
T O T A L			81	45	**55,55%**

Os pontos relevantes levantados neste processo é a inexistência de documentação que aborde a importância de cada ativo, da valoração dos ativos e da avaliação do impacto que um incidente de segurança da informação ocorrido com o ativo poderia causar para o negócio da organização.

4.2.7 Processo de Segurança em Recursos Humanos

A Tabela 4.9 apresenta o resultado da análise deste processo. Os dados sobre as atividades que compõem o processo de segurança em recursos humanos foram obtidos por meio de consulta a documentos e arquivos existentes na organização, entrevista com pessoas e pela observação direta dos diversos setores da organização.

Tabela 4.9 – Segurança em Recursos Humanos.

Atividade	Grau de relevância	Nível de implementação	Valor de referência	Valor apurado	Nível de Aderência
Definir e documentar, de acordo com a política de segurança da informação da organização, papéis e responsabilidades pela segurança da informação de funcionários, fornecedores e terceiros	3	1	9	3	33,33%
Comunicar aos candidatos ao cargo os papéis e responsabilidades de segurança da informação	3	2	9	6	66,66%
Realizar verificações de controle dos candidatos a emprego, fornecedores e terceiros, de acordo com a ética, legislação e regulamentos pertinentes	1	0	3	0	0,00%
Assegurar que funcionários, fornecedores e terceiros concordem e assinem os termos e condições de sua contratação, bem como declarem suas responsabilidades em relação à segurança da informação da organização	1	0	3	0	0,00%
Solicitar dos funcionários, fornecedores e terceiros a prática da segurança da informação conforme estabelecido nas políticas e procedimentos da organização	3	2	9	6	66,66%
Propiciar treinamento, conscientização e atualizações regulares nas políticas e procedimentos organizacionais	3	2	9	6	66,66%
Realizar processo disciplinar formal para funcionários que tenham cometido violação da segurança da informação	3	3	9	9	100,00%
Definir e atribuir de forma clara a responsabilidade de realizar o encerramento ou mudança de um trabalho	3	2	9	6	66,66%
Assegurar a devolução por parte dos funcionários, fornecedores e terceiros dos ativos da organização após o encerramento das atividades, contratos ou acordos	3	3	9	9	100,00%

Retirar os direitos de acesso dos funcionários, fornecedores e terceiros aos ativos de informação da organização, após o encerramento das atividades, contratos ou acordos	3	3	9	9	100,00%
T O T A L			78	54	**69,23%**

As atividades deste processo que estão relacionadas à contratação de pessoal possuem baixo grau de relevância para a organização, haja vista que o ingresso de servidores na organização se dá mediante concurso público ou por transferência de outras organizações, não competindo à organização a elaboração de regras e condições para grande parte das contratações de pessoal.

Não é definido formalmente os papéis e responsabilidades dos integrantes da organização em relação à segurança da informação.

4.2.8 Processo de Segurança Física e do Ambiente

Os dados sobre as atividades que compõem o processo de segurança física e do ambiente foram obtidos por meio da observação direta dos diversos setores da organização. Os resultados da análise deste processo são apresentados na Tabela 4.10.

Tabela 4.10 – Segurança Física e do Ambiente.

Atividade	Grau de relevância	Nível de implementação	Valor de referência	Valor apurado	Nível de aderência
Utilizar perímetros de segurança com barreiras para proteger as áreas que contenham informações e instalações de processamento da informação	3	3	9	9	100,00%
Proteger as áreas seguras com controles de acesso apropriados	3	3	9	9	100,00%
Proteger escritórios, salas e instalações	3	3	9	9	100,00%
Projetar e aplicar proteção contra ameaças externas e do meio ambiente (desastres naturais ou causados pelo homem)	3	3	9	9	100,00%
Projetar e aplicar proteção física e diretrizes referentes ao trabalho em áreas seguras	3	2	9	6	66,66%

Controlar os pontos de acesso público (áreas de entrega e carregamento, por exemplo) e, se possível, isolar essas áreas das instalações de processamento da informação	3	3	9	9	100,00%
Proteger os equipamentos contra ameaças e perigos do meio ambiente, bem como do acesso não autorizado	3	3	9	9	100,00%
Proteger os equipamento contra a falta de energia elétrica ou falhas em outras utilidades	3	2	9	6	66,66%
Proteger o cabeamento de energia e de telecomunicações contra interceptações ou danos	3	1	9	3	33,33%
Realizar a manutenção dos equipamentos de forma correta	3	3	9	9	100,00%
Tomar medidas de segurança para equipamentos que operam fora das dependências da organização	1	3	3	3	100,00%
Realizar a reutilização e alienação dos equipamentos de forma segura, examinando, quando for o caso, as mídias de armazenamento de dados antes do descarte	3	2	9	6	66,66%
Assegurar que equipamentos, informações ou *softwares* não sejam retirados do local sem autorização prévia	3	3	9	9	100,00%
T O T A L			111	96	**86,49%**

Os pontos que se destacam neste processo referem-se ao baixo grau de relevância da atividade relacionada com equipamentos que operam fora da organização, tendo em vista que este tipo de situação dificilmente ocorre na organização, e a deficiência na proteção do cabeamento de energia elétrica e de telecomunicações.

A organização apresenta um alto nível de aderência ao que está previsto nas normas que serviram de base para o modelo, no que se refere à segurança física e do ambiente.

4.2.9 Processo de Gerenciamento das Operações e Comunicações

Os dados sobre as atividades que compõem este processo foram obtidos por meio da consulta a documentos e arquivos (planos e diretrizes), entrevista com integrantes das diversas áreas da organização que trabalham com os sistemas de informação e observação direta dos

sistemas. A Tabela 4.11 apresenta os resultados encontrados neste processo.

Tabela 4.11 – Gerenciamento das Operações e Comunicações.

Atividade	Grau de relevância	Nível de implementação	Valor de referência	Valor apurado	Nível de aderência
Documentar, atualizar e disponibilizar aos usuários os procedimentos de operação dos sistemas	3	1	9	3	33,33%
Controlar as mudanças nos sistemas e nos recursos de processamento da informação	3	3	9	9	100,00%
Identificar e registrar as mudanças significativas	3	2	9	6	66,66%
Planejar e testar as mudanças	3	2	9	6	66,66%
Avaliar os impactos das mudanças	3	1	9	3	33,33%
Obter aprovação formal das mudanças propostas	3	3	9	9	100,00%
Comunicar os detalhes das mudanças a todas as pessoas envolvidas	3	3	9	9	100,00%
Incluir procedimentos e responsabilidades pela interrupção e recuperação das mudanças para os casos de insucessos ou ocorrência de eventos inesperados	3	2	9	6	66,66%
Manter registro de auditoria de todas as informações relevantes, quando mudanças forem realizadas	3	1	9	3	33,33%
Segregar funções e áreas de responsabilidade para preservar o uso correto dos ativos de informação	3	3	9	9	100,00%
Separar os recursos de desenvolvimento, teste e de produção	3	3	9	9	100,00%
Definir e documentar regras para a transferência do *software* da situação de desenvolvimento para a de produção	3	2	9	6	66,66%
Executar em diferentes sistemas ou processadores e em diferentes domínios ou diretórios, o *software* em desenvolvimento e o *software* em produção	3	3	9	9	100,00%

Manter as ferramentas de desenvolvimento ou utilitários de sistema inacessíveis aos sistemas operacionais, quando não se fizer necessário	3	3	9	9	100,00%
Emular o ambiente de teste o mais próximo possível do de produção	3	3	9	9	100,00%
Diferenciar os perfis de usuários para sistemas em teste e de produção, com mensagens apropriadas de identificação	3	3	9	9	100,00%
Utilizar em ambiente de testes, dados que não sejam sensíveis	3	3	9	9	100,00%
Garantir que os controles de segurança, as definições de serviço e os níveis de entrega incluídos no acordo de entrega de serviços terceirizados sejam implementados, executados e mantidos pelo terceiro	1	3	3	3	100,00%
Monitorar e analisar criticamente os serviços, relatórios e registros fornecidos por terceiros	1	3	3	3	100,00%
Monitorar níveis de desempenho do serviço, verificando a aderência aos acordos	1	3	3	3	100,00%
Analisar criticamente os relatórios de serviços produzidos por terceiros e agendar reuniões de progresso	1	3	3	3	100,00%
Fornecer informações sobre os incidentes de segurança da informação	1	3	3	3	100,00%
Analisar criticamente as trilhas de auditoria de terceiro, registros de eventos de segurança e problemas ocorridos com o serviço entregue	1	3	3	3	100,00%
Resolver e gerenciar os problemas identificados	1	3	3	3	100,00%
Atribuir responsabilidade sobre o gerenciamento do relacionamento com terceiros	1	3	3	3	100,00%
Disponibilizar habilidades técnicas e recursos para monitorar se os requisitos de segurança estão sendo atendidos	1	3	3	3	100,00%
Gerenciar as mudanças para serviços terceirizados	1	3	3	3	100,00%

Monitorar e sincronizar os recursos existentes, bem como projetar necessidade de capacidade futura visando atender a demanda requerida pelos sistemas	3	3	9	9	100,00%
Estabelecer critérios para a aceitação de novos sistemas, atualizações e novas versões, realizando testes apropriados	3	2	9	6	66,66%
Implementar controles de proteção (detecção, prevenção e recuperação) contra códigos maliciosos, bem como procedimentos para conscientização dos usuários	3	2	9	6	66,66%
Estabelecer uma política formal proibindo o uso de *softwares* não autorizados	3	2	9	6	66,66%
Estabelecer uma política formal com orientações sobre a importação de arquivos e *softwares* oriundos de redes externas ou qualquer outro meio	3	2	9	6	66,66%
Conduzir análises críticas regulares dos *softwares* e dados dos sistemas que suportam processos críticos de negócio	3	2	9	6	66,66%
Instalar e atualizar regularmente *softwares* de detecção e remoção de códigos maliciosos	3	3	9	9	100,00%
Definir procedimentos de gerenciamento e respectivas responsabilidades para tratar da proteção de código malicioso nos sistemas	3	2	9	6	66,66%
Preparar planos de continuidade do negócio adequados para a recuperação em caso de ataques por códigos maliciosos	3	0	9	0	0,00%
Implementar procedimentos para regularmente coletar informações sobre novos códigos maliciosos	3	0	9	0	0,00%
Controlar a utilização dos códigos móveis autorizados	3	3	9	9	100,00%
Impedir a execução de códigos móveis não autorizados	3	3	9	9	100,00%
Realizar e testar regularmente, cópias de segurança das informações e de *softwares*	3	2	9	6	66,66%

Definir os níveis necessários das cópias de segurança das informações	3	1	9	3	33,33%
Registrar as cópias de segurança e documentar os procedimentos de restauração da informação	3	1	9	3	33,33%
Definir a frequência de geração das cópias de segurança	3	1	3	3	33,33%
Armazenar as cópias de segurança em localidades remotas	3	0	9	0	0,00%
Proteger as cópias de segurança	3	1	9	3	33,33%
Testar regularmente as mídias das cópias de segurança, bem como os procedimentos de restauração da informação	3	1	9	3	33,33%
Gerenciar e controlar as redes	3	2	9	6	66,66%
Separar, onde apropriado, a responsabilidade operacional pela rede da operação dos recursos computacionais	3	3	9	9	100,00%
Estabelecer responsabilidades e procedimentos sobre o gerenciamento de equipamentos remotos	3	2	9	6	66,66%
Estabelecer controles especiais de proteção dos dados que trafegam sobre as redes públicas e sem fio (*wireless)*, bem como dos sistemas e aplicações a elas conectados	3	2	9	6	66,66%
Aplicar mecanismos de registro e monitoração que habilite a gravação de ações relevantes de segurança	3	3	9	9	100,00%
Gerenciar os serviços de rede e assegurar que os controles estejam aplicados de forma consistente	3	3	9	9	100,00%
Identificar e incluir nos acordos de serviço de rede as características de segurança, os níveis de serviço e os requisitos de gerenciamento	2	3	6	6	100,00%
Implementar procedimentos visando o gerenciamento das mídias removíveis	3	1	9	3	33,33%
Realizar o descarte das mídias desnecessárias de forma segura e por meio de procedimentos formais	3	1	9	3	33,33%
Estabelecer procedimentos para o tratamento e armazenamento das informações	3	2	9	6	66,66%

Proteger a documentação dos sistemas contra acessos não autorizados	3	3	9	9	100,00%
Estabelecer e formalizar políticas, procedimentos e controles visando proteger a troca de informações em todos os recursos de comunicação	3	2	9	6	66,66%
Estabelecer acordos para troca de informações e *softwares* entre a organização e entidades externas	1	3	3	3	100,00%
Proteger mídias em trânsito contra acesso não autorizado, uso impróprio ou alteração indevida	1	3	3	3	100,00%
Proteger as mensagens eletrônicas	3	3	9	9	100,00%
Desenvolver e implementar políticas e procedimentos visando proteger as informações associadas com a interconexão dos sistemas de informação do negócio	3	2	9	6	66,66%
Identificar e tratar as vulnerabilidades existentes nos sistemas que compartilham informações com outros setores da organização	3	2	9	6	66,66%
Identificar e tratar as vulnerabilidades nos sistemas de comunicação do negócio	3	2	9	6	66,66%
Estabelecer política e controles para gerenciar o compartilhamento de informações	3	2	9	6	66,66%
Restringir o acesso às informações sensíveis	3	3	9	9	100,00%
Categorizar as pessoas autorizadas a utilizarem os sistemas, bem como determinar os locais de onde poderão realizar tal acesso	3	3	9	9	100,00%
Restringir os recursos selecionados para categorias específicas de usuários	3	3	9	9	100,00%
Gerenciar a retenção e cópias de segurança das informações mantidas no sistema	3	3	9	9	100,00%
Estabelecer requisitos e procedimentos para recuperação e contingência	3	2	9	6	66,66%

Proteger as informações de comércio eletrônico que transitam em redes públicas de atividades fraudulentas, disputas contratuais, e divulgação e modificações não autorizadas	0	0	0	0	100,00%
Identificar o nível de confiança que cada parte requer na suposta identidade de outros	0	0	0	0	100,00%
Realizar processos de autorização com quem pode determinar preços, emitir ou assinar documentos-chave de negociação	0	0	0	0	100,00%
Garantir que parceiros comerciais estão completamente informados de suas autorizações	0	0	0	0	100,00%
Determinar e atender requisitos de confidencialidade, integridade, evidências de emissão e recebimento de documentos-chave, e a não-repudiação de contratos	0	0	0	0	100,00%
Estabelecer o nível de confiança requerido na integridade das listas de preços anunciadas	0	0	0	0	100,00%
Prevenir contra perda ou duplicação de informação de transações	0	0	0	0	100,00%
Imputar responsabilidades associadas com quaisquer transações fraudulentas	0	0	0	0	100,00%
Estabelecer os requisitos de seguro	0	0	0	0	100,00%
Realizar acordo formal que comprometa ambas as partes aos termos da transação	0	0	0	0	100,00%
Proteger informações envolvidas em transações on-line	3	2	9	6	66,66%
Utilizar assinaturas eletrônicas para cada uma das partes envolvidas na transação	2	2	6	4	66,66%
Validar e verificar as credenciais de usuário para todas as partes	3	3	9	9	66,66%
Manter a confidencialidade da transação	3	3	9	9	100,00%
Manter a privacidade de todas as partes envolvidas	3	3	9	9	100,00%
Criptografar o caminho de comunicação entre todas as partes envolvidas	3	3	9	9	100,00%
Utilizar protocolos de comunicação seguros	3	3	9	9	100,00%

Armazenar detalhes da transação em locais onde não esteja publicamente acessível	3	3	9	9	100,00%
Proteger a integridade das informações disponibilizadas em sistemas publicamente acessíveis	3	3	9	9	100,00%
Testar os sistemas acessíveis publicamente antes da disponibilização da informação	3	3	9	9	100,00%
Realizar processo formal de aprovação antes que uma informação seja publicada	3	3	9	9	100,00%
Controlar os sistemas de publicação eletrônica	3	3	9	9	100,00%
Monitorar os sistemas e registrar os eventos de segurança da informação	3	3	9	9	100,00%
Utilizar os registros (*log*) de operador e de falhas para identificar problemas nos sistemas de informação	3	3	9	9	100,00%
Realizar as atividades de registro de monitoramento de acordo com os requisitos legais	3	3	9	9	100,00%
Produzir e manter por um período acordado os registros (*log*) de auditoria contendo as atividades dos usuários, exceções e outros eventos de segurança da informação	3	2	9	6	66,66%
Estabelecer procedimentos para o monitoramento do uso dos recursos de processamento da informação, analisando criticamente os resultados de tal monitoramento	3	2	9	6	66,66%
Proteger os recursos e informações de registros (*log*) contra falsificação e acesso não autorizado	3	3	9	9	100,00%
Registrar as atividades dos administradores e operadores	3	2	9	6	66,66%
Registrar e analisar as falhas ocorridas, adotando ações apropriadas	3	2	9	6	66,66%
Estabelecer regras claras para o tratamento de falhas informadas	3	1	9	3	33,33%
Sincronizar, de acordo com uma hora oficial, todos os relógios dos sistemas de processamento das informações relevantes	3	3	9	9	100,00%
T O T A L			744	577	**77,55%**

Devido às características e objetivos de negócio da organização, algumas atividades deste processo apresentam baixo grau ou até mesmo nenhuma relevância, pelo fato do serviço onde as mesmas seriam aplicadas não serem implementados pela organização. São eles:

- Atividades relacionadas ao gerenciamento de serviços terceirizados.
- Atividades referentes aos acordos para a troca de informações.
- Atividades que tratam das mídias em trânsito.
- Atividades voltadas para as trocas de informações.
- Atividades relacionadas aos serviços de comércio eletrônico.

Analisando a Tabela 4.11, percebe-se um baixo nível de implementação das atividades relacionadas ao tratamento contra códigos maliciosos, ao gerenciamento das cópias de segurança e das mídias removíveis e ao tratamento das falhas ocorridas.

4.2.10 Processo de Controle de Acessos

O levantamento dos dados sobre este processo foi realizado por meio de consulta a documentos, entrevista com pessoas responsáveis pela implementação dos controles de acessos e observação direta dos diversos sistemas de informação da organização. Os resultados da análise das atividades deste processo são contemplados na Tabela 4.12

Tabela 4.12 – Controle de Acessos.

Atividade	Grau de relevância	Nível de implementação	Valor de referência	Valor apurado	Nível de Aderência
Estabelecer, documentar e analisar criticamente a política de controle de acessos	3	1	9	3	33,33%
Estabelecer procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços	3	3	9	9	100,00%
Restringir e controlar a concessão e uso dos privilégios	3	3	9	9	100,00%
Controlar, por meio de processo de gerenciamento formal, a concessão de senhas	3	3	9	9	100,00%
Conduzir em intervalos regulares, por meio de processo formal, a análise crítica dos direitos de acesso dos usuários	3	2	9	6	66,66%

Solicitar aos usuários que sigam as boas práticas de segurança da informação na seleção e uso de senhas	3	3	9	9	100,00%
Assegurar que os equipamentos não monitorados tenham proteção adequada	3	3	9	9	100,00%
Adotar política de mesa limpa e tela limpa	3	1	9	3	33,33%
Formular uma política relativa ao uso de redes e serviços de rede	3	1	9	3	33,33%
Utilizar métodos apropriados de autenticações para controlar acesso de usuários remotos	3	3	9	9	100,00%
Considerar as identificações automáticas de equipamentos como um meio de autenticar conexões vindas de localizações e equipamentos específicos	3	3	9	9	100,00%
Controlar o acesso físico e lógico das portas de diagnóstico e configuração	3	3	9	9	100,00%
Segregar em redes os grupos de serviços de informação, usuários e sistemas de informação	3	3	9	9	100,00%
Restringir a capacidade de conexão dos usuários à rede, de acordo com a política de controle de acessos e os requisitos das aplicações	3	3	9	9	100,00%
Implementar controle de roteamento na rede	3	3	9	9	100,00%
Controlar o acesso aos sistemas operacionais por um procedimento seguro de entrada (*log-on*)	3	3	9	9	100,00%
Escolher e utilizar uma técnica adequada de identificação e autenticação dos usuários	3	3	9	9	100,00%
Implementar o sistema de gerenciamento de senhas que sejam interativos e assegurem senhas de qualidade	3	3	9	9	100,00%
Restringir e controlar o uso de programas utilitários de sistema	3	3	9	9	100,00%
Encerrar seções após um período definido de inatividade	3	3	9	9	100,00%
Restringir os horários de conexão	3	3	9	9	100,00%

Restringir e controlar, de acordo com a política de acessos, o acesso à informação e às funções dos sistemas de aplicações por usuários e pessoal de suporte	3	3	9	9	100,00%
Isolar o ambiente computacional dos sistemas sensíveis	3	3	9	9	100,00%
Estabelecer uma política e implementar medidas de proteção contra os riscos do uso dos recursos de computação e comunicações móveis	3	2	9	6	66,66%
Desenvolver e implementar política, planos operacionais e procedimentos para atividades de trabalho remoto	1	1	3	1	33,33%
T O T A L			219	193	**88,13%**

Os pontos mais destacados referentes aos resultados encontrados neste processo são a baixa relevância das atividades voltadas ao gerenciamento dos trabalhos remotos, já que a organização não implementa este tipo de serviço, e a baixa implementação das atividades relacionadas com a implementação e documentação de políticas que tratam dos controles de acessos, de mesa limpa e tela limpa e da utilização dos serviços de rede.

4.2.11 Processo de Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

Os dados deste processo foram obtidos por meio da consulta a documentos (políticas, planos e diretrizes), entrevista com pessoas integrantes das áreas atinentes às atividades do processo e observação direta dos diversos sistemas de informação da organização. A Tabela 4.13 apresenta os resultados da análise das atividades deste processo.

Tabela 4.13 – Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação.

Atividade	Grau de relevância	Nível de implementação	Valor de referência	Valor apurado	Nível de Aderência
Especificar e analisar os requisitos para controles de segurança em novos sistemas de informação ou melhorias em sistemas existentes	3	3	9	9	100,00%
Validar os dados de entrada das aplicações, visando garantir que são corretos e apropriados	3	3	9	9	100,00%

Incorporar, nas aplicações, checagem de validação, visando detectar informações corrompidas	3	3	9	9	100,00%
Identificar os requisitos para garantir a autenticidade e proteger a integridade das mensagens em aplicações, bem como identificar e implementar os controles apropriados	3	3	9	9	100,00%
Realizar a validação dos dados de saída das aplicações	3	3	9	9	100,00%
Desenvolver e implementar uma política para o uso de controles criptográficos para a proteção da informação	3	1	9	3	33,33%
Implantar um processo de gerenciamento de chaves criptográficas	3	1	9	3	33,33%
Proteger as chaves criptográficas contra modificação, perda e destruição	3	3	9	9	100,00%
Implementar procedimentos para controlar a instalação de *software* em sistemas operacionais	3	3	9	9	100,00%
Selecionar com cuidado, proteger e controlar os dados de teste	3	3	9	9	100,00%
Restringir o acesso ao código-fonte de programa	3	3	9	9	100,00%
Controlar a implementação de mudanças por meio de procedimentos formais de controle de mudanças	3	3	9	9	100,00%
Analisar criticamente e testar as aplicações críticas de negócios, quando sistemas operacionais são mudados	3	3	9	9	100,00%
Controlar as modificações em pacotes de *softwares*	3	3	9	9	100,00%
Prevenir as oportunidades para vazamento de informações	3	2	9	6	66,66%
Supervisionar e monitorar o desenvolvimento terceirizado de *software*	1	2	3	2	66,66%

Obter informação em tempo hábil sobre vulnerabilidades técnicas dos sistemas de informação em uso, avaliar a exposição da organização a estas vulnerabilidades e tomar as medidas apropriadas para lidar com os riscos associados	3	1	9	3	33,33%
T O T A L			147	125	**85,03%**

Os pontos que se destacam neste processo referem-se ao baixo grau de relevância da atividade relacionada ao desenvolvimento terceirizado de *software*, já que a organização terceiriza pequena parte do desenvolvimento de seus sistemas, e o baixo nível de implementação das atividades relacionadas à política de uso de controles criptográficos e ao gerenciamento de vulnerabilidades técnicas.

4.2.12 Processo de Gestão de Incidentes de Segurança da Informação

Os resultados deste processo são apresentados na Tabela 4.14. A obtenção dos dados referentes às atividades que compõem este processo se deu por meio da consulta a documentos e entrevista com pessoas que integram a organização.

Tabela 4.14 – Gestão de Incidentes de Segurança da Informação.

Atividade	Grau de relevância	Nível de implementação	Valor de referência	Valor apurado	Nível de Aderência
Estabelecer canais apropriados e procedimentos para que os eventos de segurança da informação sejam relatados formalmente	3	1	9	3	33,33%
Estabelecer procedimentos de resposta a incidentes notificados	3	1	9	3	33,33%
Instruir funcionários, fornecedores e terceiros a registrar e notificar qualquer fragilidade em sistemas ou serviços	3	1	9	3	33,33%
Estabelecer responsabilidades e procedimentos de gestão, visando assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação	3	1	9	3	33,33%

Estabelecer mecanismos para permitir que tipos, quantidades e custos dos incidentes de segurança da informação sejam quantificados e monitorados	3	0	9	0	0,00%
Coletar, armazenar e apresentar as evidências, de acordo com a normatização existente para este fim, nos casos de acompanhamento após um incidente de segurança da informação	3	2	9	6	66,66%
T O T A L			54	18	**33,33%**

Pontos relevantes em relação aos resultados obtidos neste processo:

- A organização não possui uma equipe de tratamento e resposta à incidentes de segurança computacional que tenha sido estabelecida formalmente.
- O tratamento e resposta à incidentes de segurança computacional é realizado de maneira reativa pelo pessoal da área de tecnologia da informação da organização, porém, sem seguir qualquer metodologia.
- Inexiste mecanismos que possibilitem a notificação, por parte dos integrantes da organização, de fragilidades e eventos de segurança detectados.
- Inexiste um registro formal de incidentes ocorridos, as ações executadas, nem tampouco uma diretriz regulando a comunicação aos órgãos superiores de tais ocorrências.
- Inexiste mecanismos de quantificação e monitoramento dos incidentes de segurança.

4.2.13 Processo de Gestão de Continuidade do Negócio

Os dados referentes às atividades do processo de gestão de continuidade do negócio foram obtidos por meio da consulta a documentos e arquivos relacionados à segurança da informação e de entrevista com pessoas integrantes dos sistemas da informação da organização. A Tabela 4.15 apresenta os resultados da análise das atividades que compõem este processo.

Tabela 4.15 – Gestão de Continuidade do Negócio.

Atividade	Grau de relevância	Nível de implementação	Valor de referência	Valor apurado	Nível de Aderência
Incluir a segurança da informação no processo de gestão de continuidade do negócio, contemplando os requisitos de segurança da informação necessários	3	2	9	6	66,66%
Entender os riscos a que a organização está exposta, identificando e priorizando os processos críticos do negócio	3	1	9	3	33,33%
Identificar os ativos envolvidos nos processos críticos do negócio	3	3	9	9	100,00%
Entender o impacto que incidentes de segurança da informação provavelmente terão sobre os negócios	3	2	9	6	66,66%
Considerar a contratação de seguro compatível como parte integrante do processo de continuidade do negócio	0	0	0	0	0,00%
Identificar e considerar a implementação de controles preventivos e de mitigação	3	2	9	6	66,66%
Identificar os recursos financeiros, organizacionais, técnicos e ambientais suficientes para identificar os requisitos de segurança da informação	3	2	9	6	66,66%
Garantir a segurança de pessoal e proteção de recursos de processamento das informações e bens da organização	3	3	9	9	100,00%
Detalhar e documentar os planos de continuidade de negócio que contemplem os requisitos de segurança da informação alinhados com a estratégia da continuidade do negócio estabelecida	3	1	9	3	33,33%
Testar e atualizar regularmente os planos e processos implantados	3	1	9	3	33,33%
Garantir que a gestão da continuidade do negócio esteja incorporada aos processos e estrutura da organização	3	1	9	3	33,33%

Atribuir responsabilidade pela coordenação do processo de gestão de continuidade de negócios em um nível adequado dentro da organização	3	1	9	3	33,33%
Identificar os eventos que podem causar interrupções aos processos de negócio, a probabilidade de ocorrência, o impacto de tais interrupções e as consequências para a segurança de informação	3	1	9	3	33,33%
Desenvolver e implementar planos para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos do negócio	3	1	9	3	33,33%
Manter uma estrutura básica dos planos de continuidade do negócio que contemplem os requisitos de segurança da informação	3	1	9	3	33,33%
Testar e atualizar regularmente os planos de continuidade do negócio	3	1	9	3	33,33%
T O T A L			135	69	**51,11%**

Analisando a Tabela 4.15, verifica-se que a atividade relacionada com a contratação de seguros não é aplicável à organização, já que esta prática não é respaldada pela instituição a qual a organização pertence.

A organização não possui políticas e planos documentados que estabeleçam diretrizes no que se refere à continuidade do negócio organizacional nem tampouco implementa ações organizadas de forma metódica, visando a continuidade do negócio.

Inexiste mecanismos que possibilitem a notificação, por parte dos integrantes da organização, de fragilidades e eventos de segurança detectados, sendo que o tratamento e resposta a incidentes de segurança computacional são realizados de maneira reativa não seguindo qualquer plano ou metodologia.

4.2.14 Processo de Conformidade

Os dados referentes às atividades deste processo foram obtidos por meio da consulta a

documentos e arquivos relacionados à conformidade e auditoria de segurança da informação e de entrevista com pessoas que integram a organização. Os resultados da análise do processo de conformidade são apresentados na Tabela 4.16.

Tabela 4.16 – Conformidade.

Atividade	Grau de relevância	Nível de implementação	Valor de referência	Valor apurado	Nível de Aderência
Definir, documentar e manter atualizados, para cada sistema de informação da organização, os requisitos legais, estatutários, regulamentares e contratuais relevantes, bem como o enfoque da organização para atender a esses requisitos	3	2	9	6	66,66%
Definir e documentar controles específicos e as responsabilidades individuais para atender aos requisitos legais, estatutários, regulamentares e contratuais	3	2	9	6	66,66%
Implementar procedimentos apropriados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais no uso de material, em relação aos quais pode haver direitos de propriedade intelectual e sobre o uso de produtos de *software* proprietários	3	2	9	6	66,66%
Divulgar uma política de conformidade com os direitos de propriedade intelectual que defina o uso legal de produtos de *software* e de informação	3	3	9	9	100,00%
Adquirir *software* somente por meio de fontes conhecidas e de reputação	3	3	9	9	100,00%
Manter conscientização das políticas para proteger os direitos de propriedade intelectual e notificar a intenção de tomar ações disciplinares contra pessoas que violarem essas políticas	3	3	9	9	100,00%
Manter de forma adequada os registros de ativos e identificar todos os ativos com requisitos para proteger os direitos de propriedade intelectual	3	2	9	6	66,66%

Manter provas e evidências da propriedade de licenças	3	3	9	9	100,00%
Implementar controles para assegurar que o número máximo de usuários permitidos não excede o número de licenças adquiridas	3	3	9	9	100,00%
Conduzir verificações para que somente produtos de *software* autorizados e licenciados sejam instalados	3	2	9	6	66,66%
Estabelecer uma política para a manutenção das condições adequadas de licenças	3	1	9	3	33,33%
Estabelecer uma política para disposição ou transferência de *software* para outros	0	0	0	0	0,00%
Utilizar ferramentas de auditoria apropriadas	3	0	9	0	0,00%
Cumprir termos e condições para *software* e informação obtidos a partir de redes públicas	3	3	9	9	100,00%
Proteger os registros importantes da organização contra perda, destruição e falsificação, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio	3	2	9	6	66,66%
Emitir diretrizes gerais para retenção, armazenamento, tratamento e disposição de registros e informações	3	2	9	6	66,66%
Elaborar uma programação para retenção, identificando os registros essenciais e o período que cada um deve ser mantido	3	2	9	6	66,66%
Manter um inventário das fontes de informações-chave	3	2	9	6	66,66%
Implementar controles apropriados para proteger registros e informações contra perda, destruição e falsificação	3	2	9	6	66,66%
Assegurar a privacidade e proteção de dados conforme exigido nas legislações relevantes, regulamentações e nas cláusulas contratuais	3	3	9	9	100,00%
Prevenir o mau uso dos recursos de processamento da informação	3	3	9	9	100,00%

Conscientizar os usuários do escopo preciso de suas permissões de acesso e da monitoração realizada para detectar o uso não autorizado	3	3	9	9	100,00%
Utilizar controles de criptografia em conformidade com todas as leis, acordos e regulamentações relevantes	3	3	9	9	100,00%
Garantir que todos os procedimentos de segurança da informação estão sendo executados corretamente para atender à conformidade com as normas e políticas de segurança da informação	3	2	9	6	66,66%
Registrar e manter os resultados das análises críticas e das ações corretivas realizadas	3	1	9	3	33,33%
Verificar periodicamente os sistemas de informação em sua conformidade técnica com as normas de segurança da informação implementadas	3	1	9	3	33,33%
Planejar e acordar os requisitos e atividades de auditoria envolvendo verificação nos sistemas operacionais, visando minimizar os riscos de interrupção dos processos do negócio	3	1	9	3	33,33%
Proteger o acesso às ferramentas de auditoria de sistema de informação	3	0	9	0	00,00%
Planejar e implementar um programa de auditorias, visando verificar os objetivos de controle, controles, processos e procedimentos do sistema de gestão da segurança da informação	3	0	9	0	00,00%
Definir e documentar as responsabilidades e os requisitos para planejamento e para execução de auditorias e para relatar os resultados e a manutenção dos registros	3	0	9	0	00,00%
T O T A L			261	168	**64,37%**

Pela análise dos dados levantados sobre este processo foi possível perceber as seguintes evidências:

- As atividades relacionadas à política de transferência de *softwares* para outros não possuem relevância para a organização, pois tais transferências não são realizadas pela organização.
- A organização não possui uma política que estabeleça diretrizes para verificação da conformidade de segurança em seus sistemas de informação. As orientações existentes foram publicadas por órgãos aos quais a organização está subordinada e tratam da questão da auditoria de segurança dos sistemas de informação no âmbito institucional.
- Não são implementados mecanismos que visem à verificação da conformidade da segurança da informação, seguindo uma metodologia definida pela própria organização e com padrões a serem alcançados.
- Não foram encontrados registros de auditorias que tenham sido realizadas na organização, bem como qualquer planejamento sobre auditorias a serem realizadas.
- Não são implementados controles visando à conformidade técnica de segurança da informação.
- Não são implementadas auditorias nos diversos sistemas de informação.
- Inexiste um registro formal de não-conformidades dos diversos sistemas de informação nem tampouco uma diretriz regulando a comunicação de tais não-conformidades.

4.2.15 Processo de Análise Crítica do Sistema de Gestão da Segurança da Informação

Os dados referentes às atividades que compõem o processo de análise crítica do SGSI foram obtidos por meio da consulta a documentos e arquivos relacionados à segurança da informação e de entrevista com pessoas que integram a organização. A Tabela 4.17 apresenta os resultados da análise deste processo.

Tabela 4.17 – Análise Crítica do Sistema de Gestão da Segurança da Informação.

Atividade	Grau de relevância	Nível de implementação	Valor de referência	Valor apurado	Nível de Aderência
Avaliar a política de segurança da informação	3	1	9	3	33,33%
Avaliar os objetivos de segurança da informação	3	1	9	3	33,33%
Avaliar a adequabilidade e eficácia dos controles de segurança da informação implementados	3	1	9	3	33,33%
Avaliar a necessidade de mudanças no SGSI	3	1	9	3	33,33%
Avaliar a oportunidade para melhorias do SGSI	3	1	9	3	33,33%
Documentar e manter os registros dos resultados da análise crítica	3	0	9	0	00,00%
T O T A L			54	15	**27,78%**

Analisando os resultados apresentados na Tabela 4.17 é possível perceber que todas as atividades que compõem o processo de análise crítica do SGSI da organização apresentam um baixo grau de implementação.

As ações referentes a este processo são realizadas sem qualquer metodologia e planejamento devidamente formalizado e documentado.

4.3 Análise da Situação Encontrada

A Tabela 4.18 apresenta os níveis de aderência de cada processo que compõe o sistema de gestão da segurança da informação (SGSI) observado, em relação ao que está previsto nas normas que serviram de base para confecção do modelo. A Figura 4.1 ilustra a situação geral do sistema, possibilitando uma melhor visualização.

O nível de aderência do SGSI analisado foi de 60,93%. Esse valor demonstra o grau de conformidade da gestão da segurança da informação organizacional em relação ao que está previsto nas normas utilizadas como referência para confecção do modelo utilizado.

Tabela 4.18 – Níveis de Aderência dos Processos do SGSI.

PROCESSO	NÍVEL DE ADERÊNCIA
Implementação, Manutenção e Melhoria do Sistema de Gestão da Segurança da Informação (SGSI)	54,32%
Organização da Segurança da Informação	65,79%
Política de Segurança da Informação	69,00%
Gestão de Riscos de Segurança da Informação	19,54%
Assessoria Jurídica	66,66%
Gestão de Ativos de Informação	55,55%
Segurança em Recursos Humanos	69,23%
Segurança Física e do Ambiente	86,49%
Gerenciamento de Operações e Comunicações	77,55%
Controle de Acessos	88,13%
Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação	85,03%
Gestão de Incidentes de Segurança da Informação	33,33%
Gestão da Continuidade do Negócio	51,11%
Conformidade	64,37%
Análise Crítica do Sistema de Gestão da Segurança da Informação (SGSI)	27,78%

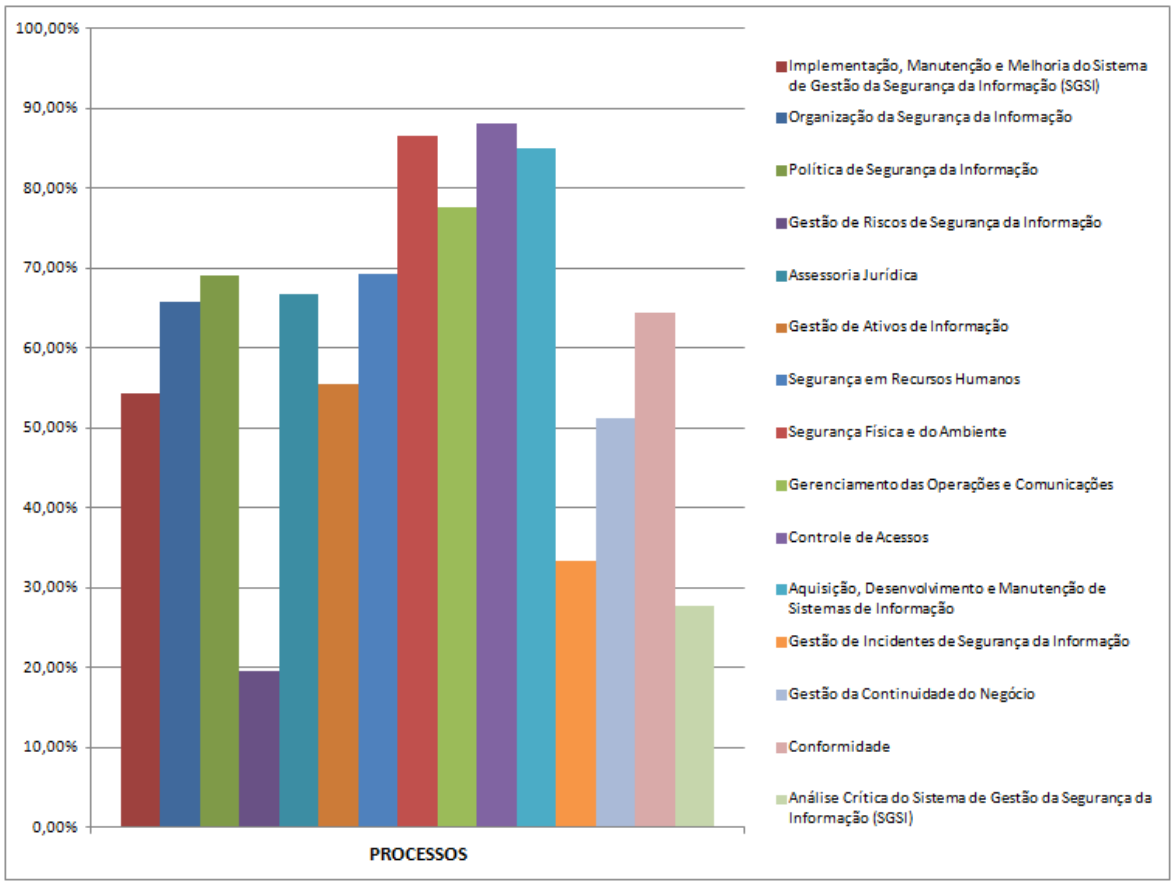

Figura 4.1 – Níveis de aderência dos processos do SGSI.

O nível de aderência do sistema (*NAs*), foi obtido por meio da seguinte equação:

$$NAs = \frac{\sum NAp}{15} \tag{4.5}$$

onde *NAp* representa o nível de aderência de cada processo (Equação 4.4) e a constante 15 refere-se ao número de processos do sistema.

Analisando os níveis de aderência de cada processo, percebe-se que os processos de gestão de riscos de segurança da informação (com 19,54%), análise crítica do sistema de gestão da segurança da informação (com 27,78%) e gestão de incidentes de segurança (com 33,33%) destacam-se negativamente por possuírem valores abaixo da média geral do sistema.

Capítulo 5

Conclusões

Este trabalho apresentou um modelo de sistema de gestão da segurança da informação em que os principais processos que compõem tal sistema foram mapeados e as respectivas atividades a serem desenvolvidas foram descritas. O modelo segue as diretrizes contidas nas normas ABNT NBR ISO/IEC 27001, 27002 e 27005, de forma que seja possível a obtenção de uma visão geral dos pontos relacionados à segurança da informação em uma organização.

A modelagem dos processos que constituem o sistema, que permite uma melhor compreensão dos relacionamentos existentes entre eles, aliada à descrição de seus objetivos, do que recebem como entradas, das atividades que devem ser realizadas e o que oferecem como saídas, constitui um elemento facilitador no gerenciamento da segurança da informação em qualquer organização.

O modelo proposto pode ser usado como um guia para implementação de um sistema de gestão da segurança da informação ou para a verificação de conformidade de um sistema já existente. Ele não visa, de forma alguma, substituir as normas que serviram de base para a sua confecção, mas, sim, realizar uma consolidação das diretrizes que são estabelecidas em tais normas, facilitando seu entendimento e aplicação.

Um exemplo de aplicação do modelo, na verificação da situação da segurança da informação em uma organização, foi mostrado no capítulo 4. Os resultados mostram o nível de

aderência do sistema de gestão da segurança desta organização às diretrizes previstas na normatização. Analisando os resultados da verificação é possível identificar os pontos fortes e fracos em cada processo que constitui o sistema, quando comparados com a situação julgada ideal, de acordo com as características do negócio da organização. Os pontos fortes são constituídos pelo alto nível de implementação por parte da organização das atividades consideradas relevantes para a segurança da informação organizacional. Já os pontos fracos são aqueles em que as atividades previstas no modelo, apesar de serem relevantes para a segurança da informação, apresentam um baixo grau de implementação.

O resultado da aplicação do modelo mostra que o processo de Gestão de Riscos de Segurança da Informação apresenta um nível de aderência baixo (19,54%). Essa constatação é altamente preocupante, pois a Gestão de Riscos de Segurança da Informação constitui um dos pilares do sistema de gestão da segurança da informação.

Outro fator preocupante é o baixo nível de aderência, 27,78%, no processo de Análise Crítica do Sistema de Gestão da Segurança da Informação, o que mostra a falta de comprometimento da organização com a metodologia e planejamento de sua segurança.

Nota-se também a baixa preocupação da organização com a Gestão de Incidentes de Segurança da Informação, 33,33%, caracterizada pela falta de uma equipe dedicada a esses eventos, falta de metodologia, inexistência de registros formais de incidentes e meios de quantificação.

De modo geral, pode ser concluído a partir da Tabela 4.18 e do gráfico da Figura 4.1 que, devido a integração do modelo proposto, a organização apresenta falhas marcantes em 3 processos da gestão da segurança da informação que pode comprometer todo o sistema.

Assim, a aplicação do modelo proposto na organização escolhida mostrou a sua utilidade e praticidade em determinar, de forma preliminar, os pontos mais deficientes do sistema de gestão da segurança da informação.

A aplicação do modelo abordada no capítulo 4 utilizou como forma de cálculo do nível de aderência do sistema de gestão da segurança da informação (60,93%) a média aritmética dos níveis de aderência de cada processo. Ao ser adotada essa forma de cálculo, partimos do princípio de que todos os processos que constituem o sistema possuem o mesmo grau de relevância para a segurança da informação da organização. Porém uma outra maneira de realizar o cômputo geral

do nível de aderência do SGSI de uma organização seria o cálculo da média ponderada dos diversos processos, de acordo com a importância que cada processo representa para a segurança da informação daquela organização especificamente.

Portanto a forma como é determinado o nível de segurança ideal, bem como calculado o nível de aderência do sistema, é flexível e pode ser adaptado às características de cada organização, por meio da mudança na ponderação.

A segurança da informação abrange todas as áreas de uma organização. A harmoniosa integração das áreas de segurança, tecnológica e jurídica, é fator fundamental para a gestão da segurança da informação organizacional.

Como pode ser observado nos diagramas das Figuras 3.1 e 3.2, o estabelecimento e implementação de uma política de segurança da informação, o processo de gestão de riscos de segurança da informação e a infraestrutura de tecnologia da informação, podem ser considerados os pilares fundamentais de um sistema de gestão da segurança da informação. Sendo assim, o aprimoramento desses três elementos contribui de maneira significativa para a implementação dos demais componentes do sistema, fazendo com que a organização gerencie a segurança da informação de forma mais eficiente e eficaz.

As características e peculiaridades inerentes a cada organização torna difícil a obtenção de parâmetros de referência, que possibilitem a comparação do nível de proteção da informação de uma dada organização.

5.1 Trabalhos Futuros

Como trabalhos futuros, é sugerido que o modelo proposto, composto pelo arcabouço de tópicos utilizados, seja replicado em outras organizações com características semelhantes, possibilitando, dessa forma, a verificação de tendências nos resultados alcançados, bem como o aprimoramento desse modelo, por meio da inserção de outros elementos/enfoques julgados relevantes e exclusão daqueles considerados sem aplicação no contexto da organização pesquisada. Um trabalho mais amplo estenderia a aplicação do modelo na verificação dos sistemas de gestão da segurança da informação em um número de organizações que integram áreas distintas, tanto do setor público como privado, tais como comércio, educação, saúde, etc. Dessa forma, seria possível traçar um perfil de como é tratada a segurança da informação nas

mais diversas áreas e setores em distintos grupos de organizações.

Outro trabalho julgado relevante, seria a realização de um modelo de desenvolvimento de *software*, com mapeamento dos processos e descrição das atividades destinadas a tornar um *software* seguro em relação às ameaças atualmente existentes. Embora o trabalho proposto esteja voltado para uma área mais específica da segurança da informação, ele apresenta alguma similaridade com o modelo de sistema de gestão da segurança da informação aqui proposto, no que se refere ao mapeamento de processos e descrição das atividades a serem desenvolvidas.

Referências

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27002: *Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação*, 2005.

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27001: *Tecnologia da Informação – Técnicas de Segurança – Sistema de Gestão de Segurança da Informação – Requisitos*, 2006.

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27005: *Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação*, 2008.

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27011. *Tecnologia da informação — Técnicas de segurança — Diretrizes para gestão da segurança da informação para organizações de telecomunicações baseadas na ABNT NBR ISO/IEC 27002*, 2009.

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27004. *Tecnologia da informação — Técnicas de segurança — Gestão da segurança da informação — Medição*, 2010.

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27003. *Tecnologia da informação — Técnicas de segurança — Diretrizes para implantação de um sistema de gestão da segurança da informação*, 2011.

BATISTA, C. F. A. *Métricas de Segurança de Software*. 102 p. Dissertação (Mestre) - Curso de Mestrado em Informática, Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro. Rio de Janeiro, 2007. Disponível em: http://www2.dbd.puc-rio.br. Acesso em: julho de 2012.

BAUER, C. A. *Política de Segurança da Informação para Redes Corporativas*. Novo Hamburgo, 2006. Disponível em: <http://tconline.feevale.br/tc/files/621.pdf>. Acesso em: março de 2011.

BEAL, A. *Introdução à Gestão de Tecnologia da Informação*. 2001. Disponível em: <http://www.atarp.com.br/tiplanning/ti.pdf>. Acesso em: julho de 2012.BENZ, K. H. *Alinhamento Estratégico entre as Políticas de Segurança da Informação e as Estratégias e Práticas Adotadas na TI*: Estudos de Caso em Instituições Financeiras. Porto Alegre, 2008. Disponível em: <http://www.lume.ufrgs.br/bitstream/handle/10183/12905/000636569.pdf?sequence=1>. Acesso em: julho de 2012.

BORDIM, J. L. *Gestão da Segurança da Informação e Comunicações* : Controles de Segurança da Informação. Brasília. 2008. Disponível em: <http://rbrito.googlecode.com/svn/diversos/UNB/GSIC320-Controles_SI/Texto_-_Controles_de_seg_da_informacao.pdf>. Acesso em: dezembro de 2010.

BRASIL. Exército Brasileiro. Gabinete do Comandante do Exército. *Instruções Gerais de Segurança da Informação para o Exército Brasileiro*. Brasília, DF, 2001.

BRASIL. Exército Brasileiro. Departamento de Ciência e Tecnologia. Instruções Reguladoras de Auditoria de Segurança de Sistemas de Informação do Exército Brasileiro – IRASEG (IR 13-09). Brasília, DF, 2007.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. *Instrução Normativa GSI/PR nº 1*. Brasília, DF, 2008. Disponível em: <http://dsic.planalto.gov.br/documentos/in_01_gsidsic.pdf>. Acesso em: julho de 2012.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. *Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC* . Brasília, DF, 2009a. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf>. Acesso em: julho de 2012.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. *Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR*. Brasília, DF, 2009b. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_05_etir.pdf>. Acesso em: julho de 2012.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. *Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações*. Brasília, DF, 2009c. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_6_gcn.pdf>. Acesso em: julho de 2012.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. *Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações* . Brasília, DF, 2010. Disponível em: < http://dsic.planalto.gov.br/documentos/nc_7_controle_acesso.pdf>. Acesso em: julho de 2012.

CICCO, F. *A Nova Norma Internacional ISO 27005 de Gestão de Riscos de Segurança da Informação*. 2008. Disponível em: <http://www.qsp.org.br/artigo_27005.shtml>. Acesso em: julho de 2012.

DURANS, L. *Abstrações Acerca de Qualquer Coisa – Questões Comentadas: Serpro 2008 – COBIT*. São Luís. 2010. Disponível em: <http://leodurans.blogspot.com/2010/09/questoes-comentadas-serpro-2008-cobit.html>Acesso em: junho de 2011.

FAGUNDES, E. *COBIT Um kit de ferramentas para a excelência na gestão de TI*. 2011. Disponível em <http://www.efagundes.com/artigos/Arquivos_pdf/Cobit.PDF>. Acesso em: junho de 2012.

FERNANDES, J. H. C. *Controle de Acessos*. GSIC211 (Notas de Aula). Curso de Especialização em Gestão da Segurança da Informação e Comunicações: 2009/2011. Departamento de Ciências da Computação da Universidade de Brasília. 2010. 32 p.

GONDIM, J. J. C. *Gerenciamento das Operações e Comunicações*: GSIC602 (Notas de Aula). Curso de Especialização em Gestão da Segurança da Informação e Comunicações: 2009/2011. Departamento de Ciências da Computação da Universidade de Brasília. 2010a. 23 p.

GONDIM, J. J. C. *Tratamento de Incidentes de Segurança*: GSIC651 (Notas de Aula). Curso de Especialização em Gestão da Segurança da Informação e Comunicações: 2009/2011. Departamento de Ciências da Computação da Universidade de Brasília. 2010b. 23 p.

GUINDANI, A. *Gestão da Continuidade dos Negócios*. Disponível em: <http://www.upis.br/revistavirtual/pos_graduacao/revista_integracao_pos_final.pdf#page=54>. Acesso em: julho de 2012.

HOLANDA, M. T.; FERNANDES, J. H. C. *Segurança no desenvolvimento de aplicações*. versão 1 GSIC701 (Notas de Aula). Curso de Especialização em Gestão da Segurança da Informação e Comunicações: 2009/2011. Departamento de Ciências da Computação da Universidade de Brasília. 2011. 43 p.

ITGI - IT GOVERNANCE INSTITUTE. *COBIT 4.1*. USA, 2007. Disponível em: <http://www.itgi.org/>. Acesso em: julho de 2012.

MACHADO, U. A. L. *DIREITO E RESPOSTA – De Dostoiévski a Mitnick: um olhar jurídico sobre a conduta humana em matéria de GSI*. Brasília, 2008. Disponível em: <http://www.devir.adv.br/GESIC/DIREITO_NA_SOCIEDADE_DA_INFORMAÇÃO_files/DELITO%20E%20RESPOSTA%20%20.pdf>. Acesso em: janeiro de 2011.

MACHADO, U. A. L. *Protocolo de Estudo de Caso:* Direito no Espaço Virtual Um Estudo do Direito que se Pratica na Sociedade da Informação à Luz do GESIC. GSIC102 (Notas de Aula). Curso de Especialização em Gestão da Segurança da Informação e Comunicações: 2009/2011. Departamento de Ciências da Computação da Universidade de Brasília. 2010. 19 p.

NETO, A. S. *Gestão da Segurança da Informação*: Fatores que influenciam sua adoção em pequenas e médias empresas. 2007. Disponível em: <http://www.uscs.edu.br/posstricto/administracao/dissertacoes/2007/abner_da_silva_neto/dissertacao_AbnerNetto.pdf>. Acesso em: janeiro de 2011.

NETO, J. S. *Política e Cultura de Segurança*. GSIC331 (Notas de Aula). Curso de Especialização em Gestão da Segurança da Informação e Comunicações: 2009/2011. Departamento de Ciências da Computação da Universidade de Brasília. 2010. 33 p.

OHTOSHI, P. H. *Análise Comparativa de Metodologias de Gestão e de Análise de Riscos sob a Ótica da Norma NBR-ISO/IEC 27005*. Brasília, 2008. Monografia de Conclusão de Curso (Especialização) – Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília. Disponível em: <http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/paulo_hideo.pdf>. Acesso em: julho de 2012.

PROMON Business & Technology Review. *Segurança da Informação*: Um Diferencial Determinante na Competitividade das Corporações, 2005. Disponível em: <http://www.promon.com.br/portugues/noticias/download/Seguranca_4Web.pdf>. Acesso em: julho de 2012.

ROCHA, P. C. C. *Segurança da Informação – Uma Questão Não Apenas Tecnológica*. Brasília, 2008. Disponível em: <http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/paulo_cesar.pdf>. Acesso em: julho de 2012.

ROCHA, R. *Certificação ISO e Você*. 2010. Disponível em: <http://gestao.adv.br/blog_gestaoadvbr/index.php/category/pdca/>. Acesso em: julho de 2012.

RODRIGUES, F. *Segurança uma Questão de Prevenção*. Madrid, 2004. Disponível em: <http://svn.assembla.com/svn/odinIDS/Egio/artigos/PraticasSeguranca/planoSeguranca.pdf>. Acesso em: julho de 2012.

SILVA, R. F. *Política de Segurança da Informação*. [2010?]. Disponível em: <http://www.faustiniconsulting.com/artigo05.htm>. Acesso em: agosto de 2011.

SILVA, T. B. P. *Protocolos de Comunicação Homem-Máquina*. GSIC601 (Notas de Aula). Curso de Especialização em Gestão da Segurança da Informação e Comunicações: 2009/2011. Departamento de Ciências da Computação da Universidade de Brasília. 2010. 28 p.

VENEZIANO, W. H. *Organizações e Sistemas de Informação*. GSIC051 (Notas de Aula). Curso de Especialização em Gestão da Segurança da Informação e Comunicações: 2009/2011. Departamento de Ciências da Computação da Universidade de Brasília. 2010. 13 p