FERNANDO HENRIQUE SOARES ALMEIDA

AVALIAÇÃO DA MATURIDADE DOS PROCESSOS DE SEGURANÇA DA INFORMAÇÃO EM UMA INSTITUIÇÃO DE ENSINO SUPERIOR PÚBLICA FEDERAL

LAVRAS – MG

2014

FERNANDO HENRIQUE SOARES ALMEIDA

AVALIAÇÃO DA MATURIDADE DOS PROCESSOS DE SEGURANÇA DA INFORMAÇÃO EM UMA INSTITUIÇÃO DE ENSINO SUPERIOR PÚBLICA FEDERAL

Monografia apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Sistemas de Informação para obtenção do título de Bacharel.

Orientador
Dr. Joaquim Quinteiro Uchôa

LAVRAS – MG

2014

FERNANDO HENRIQUE SOARES ALMEIDA

AVALIAÇÃO DA MATURIDADE DOS PROCESSOS DE SEGURANÇA DA INFORMAÇÃO EM UMA INSTITUIÇÃO DE ENSINO SUPERIOR PÚBLICA FEDERAL

Monografia de graduação apresentada ao Colegiado do Curso de Bacharelado em Sistemas de Informação, para obtenção do título de Bacharel.

APROVADA em 4 de julho de 2014.

Clayton Ferreira Santos

Rêmulo Maia Alves

Joaquim Quinteiro Uchoa (Orientador)

LAVRAS-MG
2014

Dedico este trabalho aos meus pais Antônio e Isabel que fizeram de tudo para a realização desse sonho e por me apoiar em todas as etapas da minha vida.

AGRADECIMENTOS

Tenho que agradecer primeiramente a Deus, por guiar o meu caminho e ajudar nas escolhas que me fizeram chegar até este momento. Agradeço aos meus pais e irmãos pelo apoio incondicional na realização deste sonho. Aos amigos de curso e companheiros de república pelos momentos incríveis vividos durante a graduação. Agradeço ao meu orientador Joaquim, pelos conselhos e boa vontade em atender as minhas solicitações. Agradeço ao Professor Rêmulo pelo incentivo e apoio nos últimos períodos de graduação e a todo o pessoal do *DGTI* que acreditaram e apoiaram a realização deste projeto.

Sem sacrifícios não há vitórias

(Autor Desconhecido)

RESUMO

Na sociedade da informação, ao mesmo tempo em que a informação é considerada o principal patrimônio de uma organização, ela está também sob constante ameaça, como nunca estivera antes. Cabe a segurança da informação o papel de garantir a integridade, confidencialidade e disponibilidade deste patrimônio. Com isso, a segurança da informação tornou-se um ponto crucial para sobrevivência das instituições. Este trabalho teve como objetivo a realização de um levantamento sobre o nível de maturidade dos processos de segurança da informação em uma instituição do ensino superior da Administração Pública Federal *(APF)*, a partir da percepção dos seus gestores. Foi adotado e atualizado um questionário de avaliação criado por Janssen (2008) e usado por Gabrich (2011) aos novos requisitos da *ISO/IEC* 27001:2013. O questionário foi respondido pelos coordenadores responsáveis pela área de gestão da Diretoria de Gestão de Tecnologia da Informação que apontaram como Informal a maturidade de 78% dos processos avaliados.

Palavras-Chave: Segurança da Informação, ABNT NBR ISO/IEC 27001:2013, Maturidade, Administração Pública Federal

SUMÁRIO

1 Introdução **13**

1.1 Contextualização 15

1.2 Objetivo e escopo 18

1.2.1 Objetivo Geral 18

1.2.2 Objetivos Específicos 18

1.2.3 Escopo 18

1.3 Justificativa 19

1.4 Organização do trabalho 20

2 REFERENCIAL TEÓRICO **22**

2.1 Informação 22

2.1.1 O valor das informações numa organização 22

2.2 Conceitos e Princípios de Segurança da Informação 23

2.3 Gestão da Segurança da Informação 24

2.4 Normas e Padrões de Segurança da Informação 25

2.4.1 ISO/IEC 27001 27

2.4.1.1 Histórico 27

2.4.1.2 ABNT NBR ISO/IEC 27001:2013 28

2.5 Segurança da Informação na Administração Publica Federal (APF) . 31

2.6 Maturidade 33

2.7 Universidade Federal de Lavras (UFLA) 37

2.7.1 Diretoria de Gestão de Tecnologia da Informação (DGTI) 37

3 Metodologia **40**

3.1 Classificação da Pesquisa 40

3.2 Amostra 41

3.3 Etapas da pesquisa 42

3.4 Questionário 42

4 Resultados e Discussão **44**

5 Conclusão **56**

A Apêndice **60**

B Anexo A **68**

LISTA DE FIGURAS

1.1 Estatísticas dos Incidentes Reportados ao CERT.br 15
1.2 Levantamento da segurança da informação pelo Acórdão 1603/2008 . 16
1.3 Situação da segurança da informação conforme Acórdão 2585 17
1.4 Comparativo da situação da segurança da informação 17

2.1 Dados, informação e conhecimento 22
2.2 Mapa das organizações certificadas em ISO 27001 28
2.3 Organograma DGTI 38

4.1 Resultado da Avaliação 54

B.1 Documentação da política de segurança da informação 68
B.2 Responsabilidade organizacional quanto à segurança da informação . 68
B.3 Dispositivos móveis e trabalho remoto 68
B.4 Processos Admissionais 69
B.5 Conscientização, educação e treinamento em segurança da informação 69
B.6 Responsabilidades na demissão ou alteração da contratação 69
B.7 Inventário e alocação de ativos 69
B.8 Diretrizes para classificação da informação 70
B.9 Armazenamento e descarte de mídias removíveis 70
B.10 Política de controle de acesso 70
B.11 Gerenciamento de acesso dos usuários 70
B.12 Uso da informação secreta 71
B.13 Restrição de acesso a informação 71
B.14 Política de uso de criptografia 71
B.15 Controle de acesso físico dos colaboradores 72
B.16 Segurança dos equipamentos que processam ou armazenam informações 72
B.17 Procedimentos operacionais e processamento da informação 72

B.18 Controle contra malware 72
B.19 Backup das informações 73
B.20 Registro das atividades de processamento da informação 73
B.21 Controle das bases de dados dos sistemas aplicativos 73
B.22 Controle das vulnerabilidades técnicas dos sistemas 74
B.23 Planejamento das atividades de auditoria nos sistemas de informação . 74
B.24 Proteção das informações em redes 74
B.25 Transferência da informação 74
B.26 Proteção da informação sobre redes públicas e em aplicativos de serviços 75
B.27 Desenvolvimento e alteração e teste dos sistemas 75
B.28 Proteção dos dados para teste 75
B.29 Acesso dos fornecedores as informações 75
B.30 Gestão de serviços com fornecedores 76
B.31 Comunicação dos eventos e deficiências de segurança da informação . 76
B.32 Gestão da continuidade de negócios 76
B.33 Disponibilidade dos recursos de processamento de informação 76
B.34 Identificação da legislação aplicável 77
B.35 Proteção dos registros com base na legislação aplicável 77
B.36 Conformidade dos sistemas com as políticas de segurança da informação 77

LISTA DE TABELAS

2.1 Principais Decretos e Normas relacionados à segurança da informação na Administração Pública Federal 33

2.2 Níveis de maturidade do modelo proposto por (JANSSEN, 2008) . . 36

4.1 Dimensão de Análise: Política de Segurança da Informação 44

4.2 Dimensão de Análise: Organização da Segurança da Informação . . . 44

4.3 Dimensão de Análise: Segurança em recursos humanos 45

4.4 Dimensão de Análise: Gestão de Ativos 46

4.5 Dimensão de Análise: Controles de acesso 47

4.6 Dimensão de Análise: Criptografia 48

4.7 Dimensão de Análise: Segurança do ambiente 48

4.8 Dimensão de Análise: Segurança nas operações 49

4.9 Dimensão de Análise: Segurança das comunicações 50

4.10 Dimensão de Análise: Aquisição, desenvolvimento e manutenção de sistemas 51

4.11 Dimensão de Análise: Relacionamento com a cadeia de suprimento . 51

4.12 Dimensão de Análise: Gestão de incidentes de segurança da informação 52

4.13 Dimensão de Análise: Aspectos da segurança da informação na gestão da continuidade do negócio 52

4.14 Dimensão de Análise: Conformidade 53

LISTA DE ABREVIATURAS

ABNT	*Associação Brasileira de Normas Técnicas*
APF	*Administração Pública Federal*
BPMM	*Business Process Management Maturity*
CMM	*Capability Maturity Model*
CMMI	*Capability Maturity Model Integration*
COBIT	*Control Objectives for Information and Related Technology*
CSN	*Conselho de Segurança Nacional*
DGTI	*Diretoria de Gestão de Tecnologia da Informação*
DSIC	*Departamento de Segurança da Informação e Comunicação*
ESAL	*Escola Superior de Agricultura de Lavras*
GSI	*Gestão da Segurança da Informação*
GSIPR	*Gabinete de Segurança Institucional da Presidência da República*
IEC	*International Engineering Consortium*
ISACA	*Information Systems Audit and Control Association*
ISO	*International Organization for Standartization*
ITIL	*Information Technology Infraestruture Library*
O-ISM3	*The Open Group Information Security Management Maturity Model*
PCN	*Plano de Continuidade de Negócios*

PDCA	*Plan, Do, Check, Act*
PDTI	*Plano Diretor de Tecnologia da Informação*
PMF	*Process Maturity Framework*
PSI	*Política de Segurança da Informação*
SGI	*Gestão da Segurança da Informação*
SGSI	*Sistemas de Gestão da Segurança da Informação*
SI	*Segurança da Informação*
TCU	*Tribunal de contas da União*
TI	*Tecnologia da Informação*
TIC	*Tecnologia da Informação e Comunicação*
UFLA	*Universidade Federal de Lavras*

1 INTRODUÇÃO

Desde o início da civilização humana, o ser humano tem a necessidade de informação, seja ela escrita, falada, ou visual para poder se comunicar. Russell e Gangemi (1991) argumentam que a segurança da informação é tão antiga quanto a própria informação. A partir do momento em que a informação começou a ser transmitida, armazenada e processada, foi necessário protegê-la.

Inicialmente, esta preocupação pode ser observada no processo de escrita de alguns povos, como o egípcio, no qual somente as castas superiores da sociedade tinham acesso aos manuscritos da época, e menos pessoas ainda ao processo de escrita dos mesmos. Assim a escrita, por meio de hieróglifos, representou uma das várias formas utilizadas pelos egípcios de protegerem e, ao mesmo tempo, perpetuarem o seu conhecimento.

Contudo, em tempos de guerra, a proteção das informações ganhou mais evidência, como foi o caso da Primeira e Segunda Guerra Mundial além da Guerra Fria, onde foram utilizadas diversas técnicas de criptografia, para escreverem mensagens para os outros postos de guerra.

O *Tribunal de contas da União (TCU)*, em sua cartilha Boas Práticas em Segurança da Informação retrata esta evolução da segurança:

> Na época em que as informações eram armazenadas apenas em papel, a segurança era relativamente simples. Bastava trancar os documentos em algum lugar e restringir o acesso físico àquele local. Com as mudanças tecnológicas e o uso de computadores de grande porte, a estrutura de segurança ficou um pouco mais sofisticada, englobando controles lógicos, porém ainda centralizados. Com a chegada dos computadores pessoais e das redes de computadores que conectam o mundo inteiro, os aspectos de segurança atingiram tamanha

> complexidade que há a necessidade de segurança cada vez mais sofisticados. (TCU, 2012).

A *tecnologia da informação (TI)* tornou-se parte integrante da vida moderna. Hoje, a maioria das organizações em todos os setores da indústria, comércio e governo são dependentes de seus sistemas de informações para sobreviver e prosperar.

Na *Administração Pública Federal (APF)* esse cenário não é diferente, interrupções e a suspensão de serviços podem resultar em sérios danos a imagem do governo. Um incidente de segurança pode impactar direta e negativamente as receitas da *APF*, a confiança de seus investidores e da população, acarretando prejuízos a toda sociedade. A adoção de uma gestão de segurança da informação se torna essencial para evitar que ocorram interrupções de qualquer espécie no setor público (XIANG; WANG; ZHANG, 2008).

Neste contexto, foi criado o Decreto nº 3505 de 13 de Junho de 2000, que além de regulamentar a *segurança da informação (SI)* no setor público, oferece diretrizes para o cumprimento da mesma. Além das várias instruções normativas lançadas pelo *Departamento de Segurança da Informação e Comunicação (DSIC)* do *Gabinete de Segurança Institucional da Presidência da República (GSIPR)* nos últimos anos, foram lançadas também novos decretos visando promover e motivar a criação de uma cultura de *SI*.

Segundo Gabrich (2011), apenas a aderência e conformidade a uma dessas normas, por si só, não representa atingir maturidade em um processo de Gestão de Segurança da Informação e Comunicações.

O desafio está em definir objetivos de segurança da informação, alcançá-los, mantê-los e melhorar os controles que os suportam, para assegurar a competitividade, a lucratividade, o atendimento a requisitos legais e a manutenção da imagem da organização junto à sociedade e ao mercado financeiro. Modelos de maturidade podem ajudar a enfrentar este desafio (RIGON; WESTPHALL, 2010).

1.1 Contextualização

A segurança da informação, ganha destaque na mídia mundial em um ano marcado por diversos escândalos de espionagens, envolvendo governos, diversos chefes de estados, setores importantes da indústria.

Além disso, a quantidade de crimes pela internet aumenta consideravelmente com o passar do tempo.

O crescimento dos incidentes ocorridos em redes de internet brasileiras, é monitorado pelo CERT.br, Grupo de Resposta a Incidentes de Segurança para a Internet brasileira conforme a Figura 1.1.

Figura 1.1: Estatísticas dos Incidentes Reportados ao CERT.br

Visto a necessidade e criticidade de se proteger os ativos de informação, a *APF* tem direcionado grande atenção para a segurança da informação e comunicação, prova disso, são os Acórdãos feitos pelo *TCU* com o objetivo de elaboração de um mapa da situação da governança de *TI* na Administração Pública Federal (BRASIL, 2008).

Segundo Brasil (2008), o primeiro levantamento deste tipo, Acórdão 1603 de 2008, envolveu 255 órgãos/entidades pesquisados, 47% deles não contam com um planejamento estratégico institucional em vigor, sendo que 59% não possuem

planejamento estratégico de *TI*. A falta destes planejamentos dificulta o estabelecimento de diretrizes para a área de *TI*.

No quesito segurança da informação, a ausência da *Política de Segurança da Informação (PSI)* foi declarada por 64% dos órgãos. Em 88% dos órgãos pesquisados não há um *Plano de Continuidade de Negócios (PCN)* vigente e, entre os que afirmam possuir um *PCN*, somente 30% declararam tê-lo revisado em período inferior a um ano.

Brasil (2008) constatou também, a ausência da análise de riscos na área de *TI*, em 75% dos órgãos/entidades pesquisados. Há também um forte indício de que as ações de segurança não são executadas em sintonia com as necessidades de negócio dessas organizações. A Figura 1.2 retrata a situação da segurança da informação levantada pelo Acórdão.

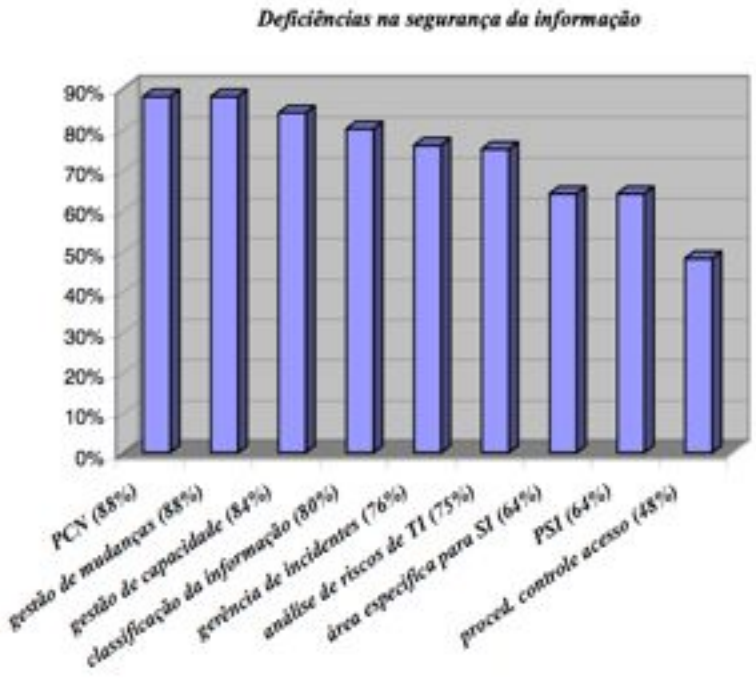

Figura 1.2: Levantamento da segurança da informação pelo Acórdão 1603/2008

Em 2012, com o objetivo de verificar mudanças, Brasil (2012) através do Acórdão 2585 com 301 organizações envolvidas, constatou que: 46% das institui-

ções não estabelecem objetivos de *TI*, 15% delas não contam com um planejamento estratégico ante os 47% em 2008. Em relação ao planejamento estratégico de *TI*, observou-se de melhoria 37%, agora, apenas 22% dos órgãos não apresentam planejamento estratégico de *TI*.

A ausência da *PSI* foi constatada, conforme a Figura 1.3, em 55% dos órgãos e somente 10% das organizações realizam análise de riscos, concluindo que a *gestão da segurança da informação (GSI)* ainda se encontra em nível baixo de maturidade. O resultado da análise de riscos é insumo essencial para outros processos, como a gestão de continuidade do negócio.

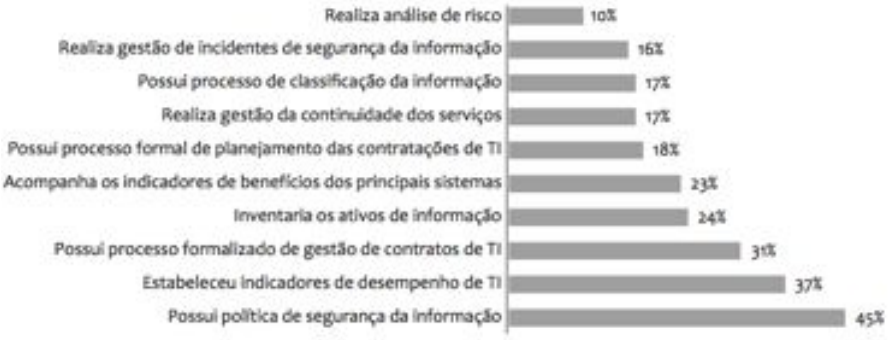

Figura 1.3: Situação da segurança da informação conforme Acórdão 2585

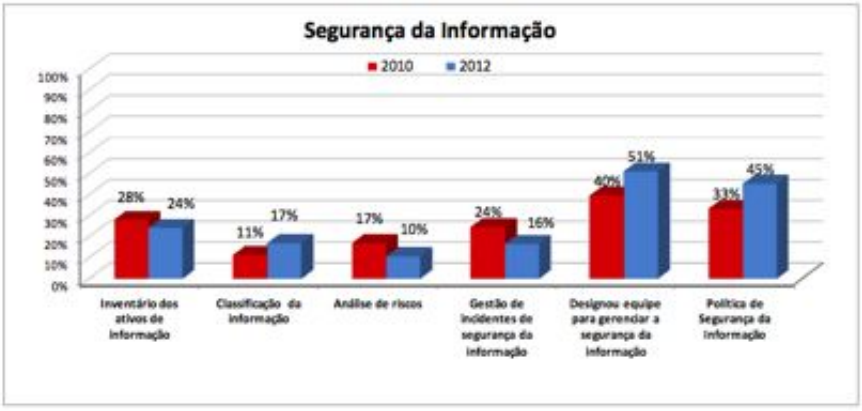

Figura 1.4: Comparativo da situação da segurança da informação

De forma geral, as evoluções da *SI* constatadas entre os Acórdãos e na Figura 1.4, refletem uma maior preocupação dos gestores públicos com os aspectos de segurança. Mas esse cenário ainda é distante do desejado, tendo em vista a criticidade das informações e os benefícios que uma gestão eficiente e madura podem proporcionar a toda população.

1.2 Objetivo e escopo

1.2.1 Objetivo Geral

Avaliar o nível de maturidade dos processos de segurança da informação em uma instituição de ensino da Administração Pública Federal, a partir da visão dos seus gestores.

1.2.2 Objetivos Específicos

- Atualizar e adaptar um instrumento para avaliação da maturidade dos processos de segurança da informação a luz da norma ABNT (2013);
- Identificar o nível de maturidade de uma organização pública do ensino superior;
- Levantar na literatura normas de segurança da informação e segurança da informação na *APF*;
- Levantar na literatura conceitos e modelos de maturidade.

1.2.3 Escopo

O escopo dessa pesquisa, é a Diretoria de Gestão e Tecnologia da Informação da *UFLA*. Por ser um setor estratégico a universidade, reflete as atividades, operações e processos da universidade como um todo.

1.3 Justificativa

A maturidade da segurança da informação foi abordada como contexto deste estudo de caso, visando auxiliar os gestores responsáveis a compreender a real situação do *sistema de gestão da segurança da informação (SGSI)* na *Universidade Federal de Lavras (UFLA)*, mais especificamente na *Diretoria de Gestão de Tecnologia da Informação(DGTI)*.

Neste mundo globalizado, onde as informações atravessam fronteiras com velocidade espantosa, a proteção do conhecimento é de vital importância para a sobrevivência das organizações (NAKAMURA, 2002).

> "Na sociedade da informação, ao mesmo tempo em que as informações são consideradas o principal patrimônio de uma organização, estão também sob constante risco, como nunca estiveram antes. Com isso, a segurança da informação tornou-se um ponto crucial para a sobrevivência das instituições." (TCU, 2008).

A avaliação crítica e metódica dos controles relacionados à segurança da informação torna-se necessária já que tecnologias, processos de negócio e pessoas mudam, alterando constantemente o nível de risco atual e gerando novos riscos à organização (PINHEIRO; SLEIMAN, 2009).

A *UFLA*, desempenha atividades de ensino, pesquisa e extensão, e produção de conhecimento técnico científico para a sociedade. A segurança da informação é de fundamental importância para a continuidade de suas atividades no cumprimento de sua missão de promover e manter a excelência no ensino.

Essa importância também é reconhecida pela *APF* que, de acordo com a Instrução Normativa nº 1 da GSIPR (2008) as informações tratadas no âmbito da Administração Pública Federal, direta e indireta, como ativos valiosos para a eficiente prestação dos serviços públicos. Esta Instrução Normativa também

aprova orientações para a Gestão de Segurança da Informação e Comunicações a serem implementadas por seus órgãos e entidades.

As normas internacionais da família 27000 relacionadas à segurança da informação, são genéricas e aplicáveis a todas organizações, por isso, não definem um método para avaliar a adequação dos controles levando-se em conta o nível de risco associado e o seu custo/benefício.

"A falta de um método para avaliar a adequação dos controles pode levar uma organização a adotar controles fracos, expondo-a ao risco em diversas situações. De modo inverso, pode ocorrer o desperdício de recursos em controles super dimensionados "(RIGON; WESTPHALL, 2010). Mensurando a maturidade dos processos é possível saber quais são as falhas e investir naquilo que é crítico para a organização.

Este estudo traz também, uma importante contribuição para a elaboração de um novo *Plano Diretor de Tecnologia da Informação (PDTI)*, que se encontra desatualizado, pois foi baseado nos novos requisitos da *ISO* 27001.

1.4 Organização do trabalho

O primeiro capítulo apresenta a introdução ao tema, contextualização, justificativa e objetivos do trabalho.

O segundo capítulo contém os fundamentos teóricos utilizados neste trabalho através das subseções nas quais se destacam: os Conceitos e Princípios de Segurança da Informação, Gestão da Segurança da Informação, Normas e Padrões, Segurança da Informação na Administração Pública e modelos de Maturidade.

O terceiro capítulo aborda a metodologia usada (Estudo de Caso) através da Classificação metodológica, amostra selecionada e as etapas da pesquisa e o Questionário utilizado e suas características.

O quarto capítulo apresenta os resultados de cada processo pesquisado e a discussões sobre os mesmos.

O quinto e último capítulo, é a conclusão do trabalho com as considerações finais e propostas para trabalhos futuros.

2 REFERENCIAL TEÓRICO

2.1 Informação

A informação está presente em quase todas as atividades que o ser humano realiza em suas diferentes formas. Porém é um termo difícil de definir já que o seu conceito é vago e intuitivo. Segundo Ferreira *et al.* (1999), informação é o conjunto de dados acerca de alguém ou algo.

Na Figura 2.1 é apresentado a diferença nos significados dos termos "Dados", "Informação"e "Conhecimento".

Dados	Informação	Conhecimento
Simples observações sobre o estado do mundo	Dados dotados de relevância e propósito	Informação valiosa da mente humana
• Facilmente estruturado • Facilmente obtido por máquinas • Frequentemente quantificado • Facilmente transferível	• Requer unidade de análise • Exige consenso em relação ao significado • Exige necessariamente a medição humana	• De difícil estruturação • De difícil captura em máquinas • Frequentemente tácito • De difícil transferência

Figura 2.1: Dados, informação e conhecimento

A partir desses significados, pode-se concluir que a informação é um conjunto de dados quando tratados e interpretados geram conhecimento. Siewert (2006) ainda complementa a definição alegando que a informação é de forma geral, igual para todas as áreas.

2.1.1 O valor das informações numa organização

A informação, hoje, é um elemento fundamental para a existência das organizações. Antes uma organização tinha como seu campo de atuação e principais concorrentes, outras empresas da mesma região. Hoje, ela atua e concorre com empresas do mundo inteiro, e por este motivo, necessita de informações na tomada de decisão para sobreviver e prosperar.

A informação é um ativo que, como qualquer outro, é de suma importância aos negócios de uma organização e necessita ser protegido. A necessidade de um ambiente seguro e acessível aos ativos, torna a segurança da informação uma das ferramentas cruciais que permitem à organização realizar sua missão.

Rocha (2002) explica que para que se garanta um nível de proteção adequado para seus ativos de informação, as organizações e seus gestores necessitam que haja uma visão clara de todas as informações que pretendem salvaguardar e das ameaças que podem estar submetidas, para que haja uma seleção de soluções específicas de segurança.

2.2 Conceitos e Princípios de Segurança da Informação

A segurança é algo específico de cada área, ela pode ser definida como: estado, qualidade ou condição de uma pessoa ou coisa que está livre de perigos, de incertezas, assegurada de danos e riscos eventuais, afastada de todo mal (HOUAISS; VILLAR; FRANCO, 2001).

Em se tratando de segurança da informação, a norma NBR ISO/IEC 27002 (ABNT, 2005) apresenta a seguinte definição: "Segurança da informação é a proteção da informação de vários tipos de ameaças" cujo objetivo é garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

Para a ISO/IEC (2012) a segurança da informação inclui três dimensões principais: disponibilidade, confidencialidade e integridade.

- Disponibilidade: é a garantia de que a informação será acessível e utilizável às pessoas e processos autorizados;
- Confidencialidade: é a garantia de que somente as pessoas autorizadas tenham acesso as informações;

- Integridade: é a fidedignidade da informação. A informação gerada não será alterada sem a devida autorização.

O Decreto nº 3.505 de 13 de Junho de 2000, instituído pelo presidente da República Federativa do Brasil, define segurança da informação como:

> Segurança da Informação: proteção dos sistemas de informação contra negação de serviços a usuários autorizados, assim como contra intrusão e modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento (BRASIL, 2000).

A adição da palavra comunicações ao termo segurança da informação é algo recente na literatura brasileira. Surge em 2000, com o Decreto nº 3.505 e ganha força em 2008, com a Instrução Normativa nº1 do *GSIPR*.

O GSIPR (2008) definiu a Segurança da Informação e Comunicações no âmbito da Administração Pública Federal como "Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações".

A definição de *SIC* adotada pelo *DSIC*, é bem similar às definições de *SI* empregadas pelas normas da *ABNT*, não se observando nenhum conceito ligado especificamente à Segurança das Comunicações (CAMPOS, 2008).

2.3 Gestão da Segurança da Informação

Como já apresentado, a segurança da informação é a proteção da informação e suas propriedades (disponibilidade, confidencialidade e integridade) evitando que as

vulnerabilidades dos ativos possam ser exploradas por ameaças e trazer prejuízos para os negócios.

A proteção dos ativos organizacionais é uma atividade maior do que medidas técnicas de proteção, é necessário um sistema de gestão para tal. Segundo a (ISO/IEC, 2012), o termo gestão envolve atividades para dirigir, controlar e melhorar continuamente a organização.

A *gestão da segurança da informação (GSI)* trata as formas de como criar a cultura de *SI* nas organizações. Envolve a formulação e aplicação de políticas, procedimentos e diretrizes que garantem a proteção dos ativos em casos de um evento de segurança da informação.

2.4 Normas e Padrões de Segurança da Informação

"Normas e padrões tem por objetivo definir regras, princípios e critérios, registrar as melhores práticas e prover uniformidade e qualidade a processos, produtos ou serviços, tendo em vista sua eficiências e eficácia"(BEAL, 2005). Sêmola (2003) também afirma que "uma norma tem o propósito de definir regras padrões e instrumentos de controle que deem uniformidade ao processo, produto ou serviço".

Atualmente os padrões e normas mais difundidos em segurança da informação são:

- As normas para gestão da segurança da informação da família ISO/IEC 27000 adotadas pela *Associação de Normas Técnicas (ABNT)*, dentre as principais estão:
  - ISO/IEC 27000:2012 *Information technology - Security techniques - Information security management systems - Overview and vocabulary*. Descreve a visão geral e o vocabulário utilizado pelas normas da família;

  - ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos;
  - ISO/IEC 27002:2013 Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação;
  - ISO/IEC 27005:2008 Tecnologia da informação - Técnicas de segurança - Gestão de riscos da segurança da informação.

- O framework *Control Objectives for Information and Related Technology (COBIT)*: Criado em 1994 pela ISACF, passou em 2000 em sua 3ª edição a ser publicado pelo *(ITGI)* órgão criado pela *ISACA* . Atualmente encontra-se na 5ª versão com o objetivo de implementar controles para o gerenciamento de *TI* e fornecer um conjunto de melhores práticas. É estruturado em 4 domínios: 1) Planejamento e organização, possui 11 objetivos de controles relacionados como a *Tecnologia da Informação e Comunicação (TIC)* pode contribuir para alcançar os objetivos da organização, 2) Aquisição e planejamento, possui 6 objetivos de controles relacionados a identificação, desenvolvimento e aquisição da infra-estrutura, 3) Entrega e suporte com 13 objetivos de controle ligado ao atendimento dos serviços oferecidos para os clientes, manutenção e as garantias destes serviços, 4) Monitoração com 4 objetivos de controle relacionados a questões de auditoria e acompanhamento de serviços.

- O framework *Information Technology Infraestruture Library (ITIL)*: Desenvolvido no final dos anos 80 pela Central Comupter and Teclecommunications Agency (CCTA), atualmente em sua 3ª edição. O *ITIL* v3 é composto por cinco livros (Estrátegias de Serviço, Desenho de Serviço, Transação de Serviço, Operação de Serviço e Melhoria Contínua de Serviço) que fornecem as melhores práticas para minimizar os custos e aumentar a qualidade dos serviços de TIC. É organizado em 5 módulos principais englobando 25 processos: 1)

A perspectiva de negócios, 2) Gerenciamento de Aplicações, 3) Entrega de serviços, 4) Suporte a Serviços e 5) Gerenciamento de Infra-estrutura.

2.4.1 ISO/IEC 27001

2.4.1.1 Histórico

Em 1989, o *Commercial Computer Security Center*, órgão ligado ao departamento de indústria e comércio do Reino Unido, publicou a primeira versão do PD0003 - Código para Gerenciamento de Segurança da Informação (ROCHA, 2002).

Em 1995, o PD0003 foi revisado passando a ser publicado pela *British Standard* com o nome BS 7799 que visava atender os anseios dos governos e indústrias que buscavam o estabelecimento de melhoras práticas de mercado em segurança da informação. Pouco tempo depois, foi publicada a BS 7799-2 como um guia o para o processo de certificação.

Em 1999, os esforços de revisão e culminaram na evolução da norma que com o acréscimo de novos controles, passou a ser publicada como BS 7799-1:1999. Neste momento a BS 7799 era um padrão seguido por diversos países.

Em dezembro de 2000, a BS 7799-1 foi aceita como padrão internacional *ISO* denominada a partir de então de *ISO* 17799.

Em 2001, no Brasil, a norma foi traduzida e adaptada pela *ABNT* como a norma nacional NBR *ISO/IEC* 17799 - Código de Prática para a Gestão da Segurança da Informação, se tornando mais tarde a *ISO* 27002.

A parte publicada como BS 7799-2:1998 se tornou em 2006 a *ISO* 27001, seguindo o padrão das normas da família *ISO*, onde a norma de requisito vem antes das normas de controles.

Em 2012, de acordo com levantamentos feitos pela Survey (2012), haviam cerca de 20.000 organizações certificadas espalhadas pelo mundo, conforme a Figura 2.2.

Figura 2.2: Mapa das organizações certificadas em ISO 27001

Em Setembro de 2013, a norma passou por sua primeira revisão e ganhou mudanças para alinhar com outras normas de sistema de gestão como a *ISO* 9001 (qualidade) e a *ISO* 22301 (continuidade de negócios).

2.4.1.2 ABNT NBR ISO/IEC 27001:2013

A *International Organization for Standartization (ISO)* é uma organização responsável pela criação de padrões internacionais. Sediada em Genebra, Suíça, fundada em 1974, com o objetivo de criar normas e padrões universalmente aceitos, nas mais diferentes áreas de comércio, indústria, tecnologia e ciência.

Já o *International Engineering Consortium (IEC)* é uma organização sem fins lucrativos patrocinada por universidades e sociedades de engenharia. Hoje a *IEC* mantém sua missão como uma parceira entre a academia a e a indústria, proporcionando uma educação de qualidade continuada, pesquisas, publicações e programas de serviços para a indústria de informação internacional (IEC, 2014).

No Brasil, a *ABNT* é o Foro Nacional responsável pela norma. Atualizada em 08.11.2013, a ABNT (2013) prover requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação.

> Os requisitos definidos nesta norma são genéricos e são pretendidos para serem aplicáveis a todas organizações, independentemente do tipo, tamanho ou natureza (ABNT, 2013).

São especificados 35 objetivos de controle e 144 controles em 11 seções. A organização da norma se encontra da seguinte forma:

0. Introdução: A introdução chama atenção aos requisitos para a implementação de um *SGSI*. Esse sistema deve ser planejado de acordo com as necessidades de cada organização e ser parte de um sistema de administração global. Em particular, nesta nova versão, o modelo *PDCA* foi removido. A razão para isto é a introdução de um capítulo específico de melhoria contínua, e o *PDCA* é apenas uma abordagem para atender essa exigência;

1. Escopo: Para a certificação não é aceitável a exclusão de qualquer controle presente no anexo A;

2. Referência normativa: A única referência normativa é a *ISO/IEC* 27000 - Visão Geral e vocabulário;

3. Termos e definições: Referencia a norma *ISO/IEC* 27000 como guia para os termos e definições;

4. Contexto da organização: Questões internas e externas relevantes (que afetam a capacidade da organização para alcançar resultado pretendidos de seu *SGSI*) com os requisitos das partes interessadas para determinar o escopo do *SGSI*;

5. Liderança: O objetivo desse requisito é demonstrar liderança e comprometimento da alta direção com o *SGSI*, estabelecendo a política de segurança da informação, assegurando recursos e fornecendo meios para sua manutenção. Por fim, a seção coloca exigências sobre atribuição de responsabilidades de segurança da informação e das autoridades competentes, com destaque para

duas funções específicas: a conformidade com a norma e a elaboração de relatórios sobre o desempenho;

6. Planejamento: Essa seção, preocupa em identificar, analisar e planejar um processo de tratamento e avaliação de riscos. Em alinhamento com os princípios e as orientações dadas na *ISO* 31000, esta seção remove a identificação de ativos, ameaças e vulnerabilidades como um pré-requisito para a identificação de riscos. Também, refere-se a critérios de aceitação de riscos, como um dos processos para avaliação de riscos e o tratamento dos mesmos;

7. Apoio: Esta seção começa com uma exigência de que as organizações devem determinar e prover os recursos necessários para estabelecer, implementar, manter e melhorar continuamente o *SGSI*. A seção continua com requisitos de competência, consciência e comunicação, que são semelhantes a sua homóloga *ISO/IEC* 27001:2005. Ao final, apresenta os requisitos para a informação documentada, termo novo que substitui Controle de Documentos e Controle de Registro na norma de 2005.

8. Operação: Esta seção trata da execução dos planos e processos para alcançar os objetivos propostos na seção Planejamento. A necessidade de avaliações de riscos em intervalos planejados ou quando mudanças significativas são propostas.

9. Avaliação do desempenho: A primeira parte desta seção, trata a necessidade de avaliação da eficácia do *SGSI*. Como recomendação geral, determinar quais e como os métodos serão utilizados para análise e medição. A segunda parte, Auditoria interna é semelhante a norma de 2005, na condução de auditorias internas em intervalos planejados e o estabelecimento de um plano de auditoria. Na última parte, a norma coloca exigências sobre os temas a serem considerados durante a revisão e documentação a ser realizada em intervalos planejados;

10. Melhoria: Esta seção estabelece algumas novas exigências para as ações corretivas das não conformidades, apresentando diretrizes para controle e correções dos seus impactos. A exigência de melhoria contínua foi estendida para adequação do *SGSI*, bem como a sua eficácia, mas não especifica como uma organização conseguirá isso.

Depois de sete anos desde sua primeira publicação, a norma necessitava de atualizações para acompanhar as evolução tecnológicas e alinhar-se com as normas de sistemas de gestão lançadas posteriormente.

Hoje uma organização certificada, além de atestar que o seu *SGSI* é certificado em relação as melhores práticas de *SI*, significa também, que seu sistema de gestão está alinhado com outras normas de gestão.

2.5 Segurança da Informação na Administração Publica Federal (APF)

A Administração Pública Federal tem se organizado de forma legal para obter maior controle da informação pública, como levantado no Capítulo 1, incidentes de segurança podem resultar em sérios danos a imagem do governo. Prova disso, foi em 13 de Junho de 2000, por iniciativa do *Conselho de Segurança Nacional (CSN)*, foi publicado o Decreto nº 3505, que instituiu a Política de Segurança nós órgãos públicos.

> Art. 1 Fica instituída a Política de Segurança da informação nos órgãos e nas entidades da Administração Pública Federal, que tem como pressupostos básicos:
>
> V - criação, desenvolvimento e manutenção de mentalidade de segurança da informação;

> VII - conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas sobre o risco da sua vulnerabilidade.
>
> [...]
>
> Art. 3 São objetivos da Política da Informação:
>
> I - dotar os órgãos e as entidades da Administração Pública Federal de instrumento jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, o não repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis;
>
> III - promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação (BRASIL, 2000).

> Os problemas de vazamento de informações, ou quebra de sigilo em organizações públicas são recorrentes. Entretanto, há tempos o Governo Federal brasileiro vem implementando procedimentos para gestão da segurança da informação com vistas a minimizar tais problemas. Grande parte destas ações está registrada em normas, decretos e Leis (ARAUJO, 2012).

Após a publicação do Decreto nº 3505, outras normas e instruções normativas foram lançadas no intuito de assegurar a segurança da informação nos órgãos da *APF* listadas por Vieira (2013) e apresentado na Tabela 2.1.

O Governo tenta através dos instrumentos normativos se precaver e proteger todos os órgãos/entidades contra falhas em seus sistemas de gestão e uso indevido dos ativos, que estão sob sua responsabilidade.

Tabela 2.1: Principais Decretos e Normas relacionados à segurança da informação na Administração Pública Federal

Regulamento	Assunto
Decreto 3996, 31 de Outubro de 2001	Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal
Decreto 4.553, 27 de Dezembro 2002	Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências
Decreto 5772, 08 de Maio de 2006	Institui na estrutura regimental do Gabinete de Segurança Institucional da Presidência da República o Departamento de Segurança da Informação e Comunicações com diversas atribuições na área de segurança da informação e comunicações.
Instrução Normativa Nº 1, Junho de 2008	Disciplina a Gestão de Segurança da informação e Comunicações na Administração Pública Federal, direta e indireta.
Instrução Normativa Nº 4, 2010	Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal.
Norma Complementar 01/IN01/DISC/GSIPR	Atividade de normatização
Norma Complementar 02/IN01/DISC/GSIPR	Metodologia de Gestão de Segurança da Informação
Norma Complementar 03/IN01/DISC/GSIPR	Diretrizes para elaboração de Política de segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal
Norma Complementar 04/IN01/DISC/GSIPR	Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos Órgãos e entidades da Administração Pública Federal.
Norma Complementar 06/IN01/DISC/GSIPR	Gestão da Continuidade de Negócios em Segurança da Informação e Comunicações.
Instrução Normativa Nº 2, 5 de Fevereiro de 2013	Dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal.
Instrução Normativa Nº 3, 6 de Março de 2013	Disciplina a Gestão de Segurança da informação e Comunicações na Administração Pública Federal, direta e indireta.

2.6 Maturidade

Como já apresentado, as normas internacionais relacionadas à segurança da informação, como a ABNT (2013), apresenta uma série de controles para a gestão da segurança da informação, mas não define um método para avaliar a adequação dos controles. Umas das formas de avaliação do progresso dos processos em uma organização é através de modelos de maturidade.

Os modelos de maturidade baseiam-se na compreensão da evolução de organizações, processos, pessoas e etc, ao longo do tempo. Estes modelos fornecem aos gestores preciosos instrumentos que permitem a identificação do nível atual e

o planejamento de ações para atingir uma maturidade superior. Segundo Klimko (2001), os modelos apresentam as seguintes propriedades:

- Desenvolvimento de um única entidade com um número limitado de níveis de maturidade (normalmente de 4 a 6);
- Caracterização de cada nível e exigências para atingir os níveis;
- Ordenação de forma sequencial dos níveis, do inicial até o nível final que representa a perfeição;
- A evolução de uma entidade consiste em avançar de um nível para outro, sem a exclusão de níveis.

O conceito de níveis de maturidade surgiu do gerenciamento de qualidade. Em Quality is Free (CROSBY, 1979) são descritos cinco níveis de qualidade: Incerteza, Despertar, Esclarecimento, Sabedoria e Certeza. A partir de então surgiram diversos modelos com propósitos e finalidades diferentes.

Em 1986, surgiu o *Capability Maturity Model (CMM)*, introduzindo o conceito de maturidade contínua, que considera objetivos específicos a serem alcançados. O objetivo desse modelo, foi medir a maturidade na área de desenvolvimento de *software*, descrevendo as etapas para a produção de produtos com qualidade assegurada. É composto por cinco níveis de maturidade que Janssen (2008) descreve como:

1. Inicial: o processo de software é caracterizado como *ad hoc* e ocasionalmente pode ser considerado caótico. Poucos processos são definidos e o sucesso depende do esforço individual dos recursos;
2. Repetível: os processos básicos de gestão de projeto são estabelecidos para acompanhar custo, cronograma e funcionalidade;

3. Definido: o processo de desenvolvimento de *software* para as atividades de gestão e engenharia é documentado, padronizado e integrado em um processo de *software* padrão para a organização.

4. Gerenciado: o processo e os produtos de *software* são quantitativamente compreendidos e controlados;

5. Em otimização: melhoria contínua do processo é propiciada pelo *feedback* do processo e pelas ideias e tecnologias inovadoras.

O modelo de maturidade de processos é um referencial para avaliar a capacidade de processos na realização de seus objetivos, para localizar oportunidades de melhoria de produtividade, para reduzir custos e para planejar e monitorar ações de melhoria dos processos empresariais (JANSSEN, 2008). Mas o modelo só fará sentido se for continuamente avaliado ao longo do tempo, medindo além da qualidade sua evolução e resultados obtidos.

Em se tratando de gerenciamento da tecnologia da informação pode-se destacar os seguintes modelos:

- *Business Process Management Maturity (BPMM)*;
- Bootstrap - metodologia voltada para a avaliação e melhoria do processo de desenvolvimento de software;
- *Capability Maturity Model Integration (CMMI)* - composto de vários modelos desenvolvidos a partir do *CMM*;
- *COBIT* - conjunto das melhores práticas, que auxiliam na otimização de investimentos em *TI*. O modelo de maturidade é composto por seis níveis: não existente, inicial, repetitivo, definido, gerenciado e otimizado;
- *Process Maturity Framework (PMF)* é um modelo de maturidade desenhado especificamente para o *ITIL*. O *PMF* possui cinco níveis de maturidade: Inicial, Repetitivo, Definido, Gerenciado e Otimizado;

- *The Open Group Information Security Management Maturity Model (O-ISM3)* - modelo de maturidade para o gerenciamento da segurança da informação em cinco níveis: indefinido, definido, gerenciado, controlado e otimizado. O *O-ISM3* é baseado em boas práticas de vários padrões como *CMMI*, *ITIL*, *ISO* 9000 e *ISO* 27001.

Em comum, o objetivo desses modelos está na transições dos níveis obedecendo os requisitos de cada nível cujo o principal objetivo é a melhoria contínua.

Para realização desse estudo de caso, que avaliou a maturidade dos processos de segurança da informação no *DGTI*, foi utilizado um modelo de avaliação da maturidade adaptado por Gabrich (2011). Esse instrumento deriva do trabalho apresentado por Janssen (2008) contruído na compilação de vários modelos de maturidade. Os critérios de avaliação são compostos por cinco níveis de maturidade descritos na Tabela 2.2.

Tabela 2.2: Níveis de maturidade do modelo proposto por (JANSSEN, 2008)

Níveis	
N1- Inexistente	Não existe nenhum processo relativo ao item.
N2 - Informal	Existe um processo relativo ao item, porém não existe a formalização do processo, mas os envolvidos demonstram conhecer o processo.
N3 - Organizado	Existe a formalização do processo e este é conhecido e disponibilizado a todos os envolvidos no processo.
N4 - Gerenciado	Existe um processo formal e conhecido por todos os envolvidos. Além disso, o processo é controlado por indicadores de avaliação.
N5 - Otimizado	Existe um processo formal com indicadores de acompanhamento. Além disso, o processo é submetido periodicamente à reavaliação para melhoria contínua.

2.7 Universidade Federal de Lavras (UFLA)

A *UFLA* foi criada em 1908, com o nome Escola Agrícola por protestantes que vieram ao Brasil. Em 1938, dois anos após ser reconhecida pelo Governo Federal, passou a ser denominada *Escola Superior de Agricultura de Lavras (ESAL)* .

Somente em 1994, foi transformada em Universidade, hoje, conta com 26 cursos de graduação presenciais e a distância, 32 cursos de mestrados e 21 doutorados. Possui cerca de 16581 estudantes com cerca de 13 mil pessoas frequentando o campus diariamente.

> Possui a missão de manter e promover a excelência no ensino, na pesquisa e na extensão, formando cidadãos e profissionais qualificados, produzindo conhecimento científico e tecnológico de alta qualidade e disseminando a cultura acadêmica, o conhecimento científico e tecnológico na sociedade (PDI, 2010).

2.7.1 Diretoria de Gestão de Tecnologia da Informação (DGTI)

A *DGTI* tem como missão de fornecimento serviços e produtos de *software* ou *hardware* com qualidade e efetividade, suportando as atividades de ensino, pesquisa e extensão da *UFLA*, no âmbito de Tecnologia da Informação e Comunicações. Para isso ela conta com 84 funcionários (funcionários concursados, contratados, estagiários de outras instituições e bolsistas).

Sua visão, é ser excelência na prestação de serviços de *TI* e aumentar o nível de maturidade de governança de *TI* da *UFLA*, alinhando a Tecnologia da Informação aos objetivos de negócio (ensino, pesquisa e extensão) das unidades organizacionais (Pró-reitoras, diretorias, setores administrativos e departamentos didáticos científicos).

A Figura 2.3 apresenta a divisão interna do *DGTI*.

Figura 2.3: Organograma DGTI

Segundo PDI (2010), os principais serviços prestados pelo *DGTI* são:

- *Web hosting* (Hospedagem de *website*) e domínio virtual em diversas modalidades;
- Projetos e instalação de redes convergentes de dados, voz e vídeo por meio de cabeamento estruturado ou rede sem fio;
- Serviços de telefonia e VOIP;
- Instalação e manutenção de sistemas de controle de acesso (catracas eletrônicas, fechos eletrônicos e controles biométricos);
- Serviços de vídeo vigilância e vídeo conferência.
- Instalação de antivírus institucional;

- Suporte, manutenção e administração do servidor de bancos de dados institucional;
- Suporte aos laboratórios institucionais administrados pela DADP.

3 METODOLOGIA

3.1 Classificação da Pesquisa

O pilar desse estudo, foi a utilização da norma *ABNT NBR ISO/IEC* 27001, com o objetivo de medir e aprofundar os conhecimentos sobre o nível de maturidade em uma organização pública de ensino superior.

Sendo assim, do ponto de vista de seus objetivos, a pesquisa é classificada como exploratória. "Um trabalho é de natureza exploratória quando envolver levantamento bibliográfico, entrevistas com pessoas que tiveram (ou tem) experiências práticas com o problema pesquisado e análise de exemplos que estimulem a compreensão. Possui ainda a finalidade básica de desenvolver, esclarecer e modificar conceitos e ideias para a formulação de abordagens posteriores"(GIL, 2010).

Em relação a metodologia, esta pesquisa é classificada como estudo de caso. Segundo Fernandes (2010) essa metodologia visa conferir simplicidade, uniformidade e promoção de pesquisas de qualidade. Para Yin e Grassi (2010) o estudo de caso é mais apropriado quando:

- questões do tipo “como” ou “por que” são propostas;
- quando o investigador tem pouco controle sobre os eventos e
- quando o enfoque está sobre um fenômeno contemporâneo no contexto da vida real.

Estas são características desta pesquisa, uma vez que foi avaliado na percepção dos gestores, o nível de maturidade dos processos em uma organização pública de ensino superior.

Este estudo, também é classificado como estudo de caso único, porque seu foco foi em um setor de uma instituição de ensino superior.

3.2 Amostra

Em vista da dificuldade e complexidade de realização desse estudo de caso em toda universidade, o *DGTI* foi escolhido como amostra, pois além de ser um setor estratégico, representa o comportamento da *UFLA* como um todo.

> [...] definir toda a população e a população amostral. Entende-se por população não o número de habitantes de um local [...] mas como um conjunto de elementos [...] que possuem características que serão objeto de estudo. População amostral ou amostra é uma parte do universo (população) escolhida segundo algum critério de representatividade (VERGARA, 2005).

O estudo de caso foi realizado junto a sete coordenadores do *DGTI* responsáveis pelas respectivas coordenadorias conforme a Figura 2.3.

- Diretoria executiva,
- Secretaria Administrativa,
- Coordenação de segurança da informação,
- Coordenação de infra-estrutura de redes e telecomunicação,
- Coordenação de suporte e manutenção, Coordenação de administração de redes e sistemas,
- Coordenação de sistemas de informação.

Pela posição e cargo, os sete funcionários tem uma visão ampla do funcionamento de suas coordenadorias, pontos fortes, fraquezas e deficiências.

3.3 Etapas da pesquisa

A pesquisa foi realizada em quatro etapas.

Na primeira etapa deste trabalho, foram definidos os objetivos almejados pela pesquisa. Em seguida, uma pesquisa bibliográfica feita a partir da *ISO/IEC* 27001:2013, normas e regimentos internos e outras normas e padrões que abrangem a segurança da informação e a segurança da informação na Administração Pública Federal. Também como foco da pesquisa bibliográfica, foi levantado sobre a origem da maturidade e seus conceitos para aplicação na segurança da informação.

Na segunda etapa, foi definido o *DGTI* como escopo do trabalho. Os sete coordenadores foram entrevistados. As entrevistas tiveram o propósito de conhecer o funcionamento, os processos e o cumprimento das normas e política em cada coordenação.

Na terceira etapa foram feitas atualizações no questionário adotado pela Gabrich (2011) para atender a norma *ISO/IEC* 27001:2013.

Última etapa, realização de testes e aplicação do questionário. Os testes foram feitos para verificação de erros e possíveis melhorias pelo próprio autor do trabalho, um professor na área de *SI* e dois alunos de graduação voluntários. Somente depois de feitas as correções e melhorias o questionário foi disponibilizado aos coordenadores.

3.4 Questionário

O questionário utilizado para avaliação da maturidade dos processos de segurança da informação neste estudo, é uma atualização dos trabalhos de Gabrich (2011) e Janssen (2008). Ele foi baseado na recém atualizada norma ABNT (2013).

Conforme Janssen (2008), essa norma foi considerada como base estrutural do instrumento de avaliação utilizado, por possuir dimensões de avaliação que são estruturadas em diferentes perspectivas sobre o tema segurança da informação.

Como já apresentado, a ABNT (2013) contempla 35 objetivos de controle e 144 controles em 11 seções. O atual estudo manteve as 11 dimensões do trabalho anterior, mas reduziu de 40 para 36 itens de avaliação para atender a nova versão da norma. Outras alterações, como criação de novas Categorias de Análises, novos Critérios, alterações dos controles dos níveis e um rearranjo na ordem das Categorias de Análise também foram necessárias para garantir a conformidade com a norma.

Cada item de avaliação foi baseado em um objetivo de controle, exceto o controle A.18.1 (Conformidade com requisitos legais e contratuais). Neste foi mantida a divisão em dois itens "para cobrir itens de avaliação de maturidade que o pesquisador considerava significativos para o contexto"(GABRICH, 2011).

O questionário contém 36 itens de múltipla escolha com opção de Justificativa ou detalhamento da forma de controle. Em cada item, há cinco alternativas, distribuídas do nível mínimo (Inexistente) ao nível máximo (Otimizado) de maturidade avaliado. A Tabela 2.2, apresentou os níveis de maturidade propostos por Janssen (2008) e adotado pela Gabrich (2011).

As perguntas fechadas, por sua vez, são indicadas para investigar temas mais pesquisados e conhecidos pelos sujeitos, principalmente quando os respondentes não são muitos e dispõe de pouco tempo. A justificativa é essencial para averiguar a existência do controle, a situação da forma de controle e o conhecimento das formas de controles pelos entrevistados.

Para que a aplicação do questionário fosse confortável aos respondentes, e por preferência dos mesmos, foi adotada a ferramenta SurveyMonkey [1] que possibilitou a criação de questionário *online* e a divulgação por email.

O questionário desenvolvido para a pesquisa, encontra-se no Apêndice A.

[1] https://pt.surveymonkey.com

4 RESULTADOS E DISCUSSÃO

O estudo de caso teve a preocupação em detectar o nível de maturidade dos processos de segurança da informação junto a uma organização da *APF* do ensino superior. Com base nas respostas dos coordenadores, foi possível mensurar o grau de maturidade de cada processo de acordo com a *ISO/IEC* 27001.

Quando se tratou de avaliar a maturidade dos processos de segurança da informação, é de suma importância a apresentação da prova material para confirmação do nível detectado. Em alguns processos, o autor deste trabalho não encontrou a prova material necessária para confirmar o nível aferido pelos coordenadores, apresentando em alguns casos, níveis de maturidade diferente dos medidos. Foram considerados Indefinidos, os processos que tiveram 2 ou mais níveis com mesmo percentual de votos.

O resultado completo do questionário se encontra no Anexo A.

Tabela 4.1: Dimensão de Análise: Política de Segurança da Informação

Categoria de Análise	Nível	Percentual
Orientação da Direção para segurança da informação	Organizado	100%

Na visão dos gestores, todos consideraram o nível de maturidade da política de segurança da informação como Organizado, conforme a Tabela 4.1. A política, foi documentada e formalizada no ano de 2011 e desde então não passou por nenhuma atualização. Como a norma prega a melhoria contínua, não basta apenas ter a política de segurança da informação seria necessário revisá-la para se adequar a nova conjuntura da universidade.

Tabela 4.2: Dimensão de Análise: Organização da Segurança da Informação

Categoria de Análise	Nível	Percentual
Organização interna	Organizado	100%
Dispositivos móveis e trabalho remoto	Informal	57,14%

A classificação da Organização interna foi um dos itens mais bem avaliados. Foi dado como Organizado por 100% dos coordenadores, devido as responsabilidades organizacionais quanto a *SI* estarem documentadas e formalizadas na política de segurança da informação. O Capítulo IV da UFLA (2011b), prevê responsabilidades aos usuários dos ativos de informação, as chefias, a gerência de segurança da informação e comunicação do *DGTI* e aos prestadores de serviços.

A categoria Dispositivos móveis e trabalho remoto, foi considerada Informal por 57,14% dos votos. Não existiam procedimentos formais para este processo, este tinha o controle informal do *Firewall*, que controlava e limitava o acesso externo ao sistema.

Tabela 4.3: Dimensão de Análise: Segurança em recursos humanos

Categoria de Análise	Nível	Percentual
Antes da contratação	Informal	57,14%
Durante a contratação	Organizado	83,33%
Encerramento e mudança da contratação	Informal	85,71%

A Categoria de análise Antes da contratação da Tabela 4.3 teve seu nível de maturidade avaliado como Informal. Na admissão, existia um processo informal de divulgação e apresentação da *PSI* e responsabilidades aos funcionários e partes externas. Além da informalidade, nem todos os funcionários (concursados, contratados, estagiários e bolsistas) passaram por esta etapa de apresentação.

Durante a contratação, houveram treinamentos oferecidos pelas coordenadorias de Segurança da Informação e Administração de Redes e Sistemas as demais coordenadorias e as partes interessadas, com o intuito de conscientizar e nivelar os conhecimentos em *SI*. Apesar de ser mensurado como Organizado por 83,33% dos votos, vide Tabela 4.3, este processo também apresentou indícios de informalidade. Não existe uma periodicidade desses treinamentos, e não havia uma documentação formalizada com o conteúdo desses treinamentos.

O Encerramento e mudança da contratação foi considerado Informal por 85,71% dos entrevistados. O cancelamento e mudança dos privilégios de acessos aos sistemas, eram realizados informalmente pelos coordenadores. Não existiam procedimentos documentados para estas atividades.

Tabela 4.4: Dimensão de Análise: Gestão de Ativos

Categoria de Análise	Nível	Percentual
Responsabilidades pelos ativos	Informal	50,00%
Classificação da informação	Indefinido	-
Tratamento de mídia	Informal	66,67%

O processo Responsabilidades pelos ativos foi dado como Informal pelos gestores. De acordo com o Capítulo III da UFLA (2011b), é de responsabilidade da *DGTI* a classificação e reavaliação de todos os ativos da *UFLA*. Este controle do ativos até o momento da pesquisa era inexistente. Existia um agente patrimonial responsável pelo controle dos bens patrimoniados de toda a universidade abrangendo a *DGTI*, mas esse agente não dispunha de instrumentos necessários para fiscalização, controle e atualizações do patrimônio. Interno ao *DGTI*, foi encontrado algumas formas de controle informais dos ativos de cada coordenadoria, por não estarem interligadas e formalizadas, não refletiam a quantidade real dos ativos informacionais.

A categoria de análise Classificação da informação, teve grande discrepância nos níveis de maturidade medidos. Ela foi classificada como Indefinida, conforme a Tabela 4.4, pois houve empate entre os níveis Inexistente, Informal e Organizado. Apesar das informações da *APF* serem disponíveis a qualquer cidadão brasileiro, o autor deste trabalho não encontrou nenhuma evidência da classificação quanto ao grau de sensibilidade dos ativos, como definido no item IX do Art. 3º da UFLA (2011b).

A maturidade do processo de Tratamento de mídia, foi considerada Informal por 66,67% do entrevistados. Informalmente, existia uma preocupação com a

forma de descarte das informações. Apesar dessa preocupação, o autor considerou a maturidade Inexistente, pois não existiam equipamentos ou documentação específica da universidade sobre a forma correta de descarte das informações.

Tabela 4.5: Dimensão de Análise: Controles de acesso

Categoria de Análise	Nível	Percentual
Requisitos de negócio para controle de acesso	Informal	71,43%
Gerenciamento de acesso do usuário	Indefinido	-
Responsabilidades dos usuários	Informal	57,14%
Controle de acesso ao sistema e à aplicação	Indefinido	-

Os requisitos para controle de acesso foram classificados como Informal, como apresentado na Tabela 4.5. Eram implementados procedimentos de controle *ad hoc* para cada sistema e não existia formalização dos controles de acesso a serem adotados por todos os sistemas.

Gerenciamento de acesso aos usuários na Tabela 4.5 foi classificado como Indefinido pois houve empate entre os níveis Informal e Organizado. O autor considerou este processo como Informal, pois o gerenciamento era feito pelo desligamento automático dos alunos que se formam, de funcionários terceirizados e dos servidores públicos (Técnicos e Professores).

A maturidade do processo de Responsabilidade do usuário foi considerada Informal pelos gestores. O assunto de senhas seguras era um dos assuntos abordados nos cursos de conscientização e capacitação. Não existiam normas ou procedimentos formalizados que orientavam os usuários a adotarem senhas fortes, trocá-las periodicamente e não compartilharem suas senhas com os demais. Não existia um único *Sign On*, os usuários tiveram que criar uma senha para cada sistema o que aumentava o número de informações a serem armazenadas. Futuramente essa grande quantidade de informação, sem força de proteção, poderá se tornar uma ameaça para a universidade.

A categoria de análise Controle de acesso ao sistema e aplicação foi classificada na Tabela 4.5 como Indefinida, pois os níveis encontrados foram Informal

e Organizado. O autor deste trabalho, considerou o nível desta categoria como Informal, apesar da existência de certificados SSL para a autenticação nos sistemas, estes não eram regulamentados pela unidade certificadora GlobalSigin. Não existia nenhuma documentação formal sobre a uso e acesso aos serviços com a utilização destes certificados.

Tabela 4.6: Dimensão de Análise: Criptografia

Crategoria de Análise	Nível	Percentual
Criptografia	Informal	85,71%

A categoria de análise Criptografia da Tabela 4.6, foi considerada com a maturidade Informal na visão dos gestores. Apesar do uso da criptografia para proteção de dados sensíveis, não existiam documentações formalizadas ou uma política sobre o uso de controles criptográficos para a proteção da informação.

Tabela 4.7: Dimensão de Análise: Segurança do ambiente

Crategoria de Análise	Nível	Percentual
Áreas seguras	Informal	100%
Equipamentos	Informal	83,33%

O nível de maturidade da categoria de análise Áreas seguras da Tabela 4.7 foi dado como Informal pelos coordenadores. O autor deste estudo o considerou Inexistente, pois não existiam regras formais para o controle de acesso físico. Além da ausência de regras formais, não haviam barreiras físicas para impedir o acesso físico ao local, bem como a ausência de controles de entrada e saída de visitantes e a não exigência de funcionários, visitantes e partes externas de alguma forma de identificação.

Assim como Áreas seguras, a outra categoria da Tabela 4.7, Equipamentos também foi dada como Informal. Nesta categoria, foram encontrados procedimentos informais como manutenção dos equipamentos e a proteção dos equipamentos contra falha elétrica para manter os serviços essenciais a universidade. O autor

constatou também, que a política de mesa e tela limpa não era seguida em algumas coordenadorias.

Tabela 4.8: Dimensão de Análise: Segurança nas operações

Categoria de Análise	Nível	Percentual
Responsabilidades dos procedimentos de operação	Informal	71,43%
Proteção contra malware	Informal	83,33%
Cópias de segurança	Informal	85,71%
Registro e monitoramento	Informal	83,33%
Controle do software operacional	Informal	50,00%
Gestão de vulnerabilidades técnicas	Informal	85,71%
Consideração quanto à auditoria de sistemas de informação	Informal	71,43%

Na Dimensão de Análise Segurança nas operações da Tabela 4.8, todas as categorias de análise apresentaram nível de maturidade Informal. Existiam controles para detecção, prevenção e recuperação contra *malware*, e controles de restrição ao acesso de *websites* suspeitos ou de palavras chave na *blacklist* do *firewall*. Apesar do controle por *software*, não existia uma política formal proibindo o uso de *software* não autorizados e planos de continuidade do negócio para recuperação em casos de ataques por *malwares*.

Não havia uma política de *backup* formalizada, apesar que eram feitos *backups* regulares e a *DGTI* apresentar ampla estrutura para esta atividade em vários pontos da universidade. Os registros (logs) eram realizados e controlados a todos os usuários conectados a rede interna. Os registros eram feitos de acordo com cada sistema, portanto não havia uma padronização dos mesmos. Outro aspecto importante, foi o tempo de vida dos logs, como não existiam servidores exclusivos para esta atividade o tempo que permaneciam guardados no sistema era curto.

Em relação ao Controle de *software* operacional, não existia procedimentos formalizados a para controle da instalação de *software* em sistemas operacionais, havia apenas uma preocupação com a autenticidade dos *software* instalados.

Para a Gestão de vulnerabilidades técnicas o nível de maturidade encontrado pelo autor foi Inexistente, diferente do apontado pelos gestores. Um inven-

tário dos ativos é um pré-requisito para gerir as vulnerabilidades juntamente com as atividades da gestão de incidentes que comunica as vulnerabilidades para as correções apropriadas e ambas as atividades são inexistentes no *DGTI*.

Tabela 4.9: Dimensão de Análise: Segurança das comunicações

Categoria de Análise	Nível	Percentual
Gerenciamento da segurança em redes	Informal	100%
Transferência da informação	Informal	83,33%

Na dimensão de Análise da Tabela 4.9, todas as categorias tiveram a maturidade dada como Informal. As responsabilidades e procedimentos sobre o gerenciamento de equipamentos foram documentadas e formalizadas na Seção VII do UFLA (2012). Esta categoria foi dada como Informal, pois as tecnologias aplicadas para segurança de redes como encriptação, autenticação e controle de conexões não eram formalizadas. A encriptação quando feita, era realizada por *software* não padronizados, e não existia uma formalização para o uso da criptografia, algoritmos adotados e a chave de encriptação. A autenticação se dava somente para a rede *wireless*, na qual não havia uma segregação para redes diferentes de acordo com o setor e cargo ocupado.

A informalidade da categoria Transferência da informação se justificou, pela inexistência de diretrizes para retenção e descarte da correspondência, pela ausência de controles e restrições formais, associados à retransmissão dos recursos de comunicação como, por exemplo, a retransmissão de mensagens eletrônicas para serviços de *e-mail* externos a universidade. E também, pela falta de uma política formal para uso de serviços públicos externos, como sistemas de mensagens instantâneas, redes sociais e compartilhamento de arquivos.

Na visão dos gestores, o nível de maturidade da Categoria de Análise: Requisitos de segurança de sistemas de informação da Tabela 4.10, foi apontado como Informal. Os controles desta categoria baseiam-se nos controles de Crip-

Tabela 4.10: Dimensão de Análise: Aquisição, desenvolvimento e manutenção de sistemas

Categoria de Análise	Nível	Percentual
Requisitos de segurança de sistemas de informação	Informal	83,33%
Segurança em processos de desenvolvimento e suporte	Informal	71,43%
Dados para teste	Informal	71,43%

tografia (Tabela 4.6) e Controle de acesso ao sistema e à aplicação (Tabela 4.5), ambos informais como constatado anteriormente.

Foi feito um mapeamento dos processos internos da Coordenação de Sistemas de Informação para o desenvolvimento de *software*, assim como o teste dos dados. Apesar da existência desse mapeamento, este encontra-se informalizado fato que justifica os níveis apontados pelos gestores nas outras categorias de análise.

Tabela 4.11: Dimensão de Análise: Relacionamento com a cadeia de suprimento

Categoria de Análise	Nível	Percentual
Segurança da informação na cadeia de suprimento	Informal	66.67%
Gerenciamento da entrega do serviço do fornecedor	Organizado	57,14%

O critério Segurança da informação na cadeia de suprimento da Tabela 4.11 foi classificado como Informal pelos gestores. A sua informalidade foi constatada pela ausência de um processo padronizado para gerenciar as relações com o fornecedor. Essa relação consistia na definição informal dos tipos de acesso à informação e o controle dos mesmos, que diferentes tipos de fornecedores teriam permissão. Foi constato também, ausência de treinamentos para conscientização dos fornecedores, às regras e procedimentos adotados pela *PSI*.

O outro critério desta dimensão, Gerenciamento da entrega do serviço do fornecedor teve sua maturidade dada como Organizado pelos gestores. A universidade através dos setores competentes, realiza auditorias e fiscaliza a entrega dos serviços executados pelos fornecedores, com base nos contratos formalizados entre ambas as partes.

Tabela 4.12: Dimensão de Análise: Gestão de incidentes de segurança da informação

Categoria de Análise	Nível	Percentual
Gestão de incidentes de segurança da informação e melhorias	Informal	71,43%

A Gestão de incidentes de segurança da informação e melhorias teve o seu nível de maturidade dado como Informal como mostrado na Tabela 4.12. O autor também o considera Informal apesar de alguns indícios de Organização.

Os funcionários foram instruídos pelo Art. 9 º da UFLA (2011b), a reportar e registrar fragilidades e eventos de segurança, mas não existiam procedimentos documentados de como seria a notificação. Os incidentes tratados com sucesso, não eram registrados formalmente. A quem cometia violações de *SI*, as sanções adotadas estavam documentadas no Capítulo V da UFLA (2011b), mas não existia um processo disciplinar formal para tratar funcionários e usuários que descumpriam as normas.

Contatos eram mantidos com autoridades públicas, grupos externos e fóruns de *SI* com o intuito de facilitar a resolução dos problemas encontrados.

Tabela 4.13: Dimensão de Análise: Aspectos da segurança da informação na gestão da continuidade do negócio

Categoria de Análise	Nível	Percentual
Continuidade da segurança da informação	Informal	83,33%
Redundâncias	Informal	83,33%

A Categoria de análise da Tabela 4.13 Continuidade da segurança da informação teve a maturidade medida como Informal pelos gestores. Porém, o autor deste trabalho a considerou Inexistente. Apesar de ser atribuída formalmente a coordenadoria de Segurança da Informação elaborar e manter atualizado o Plano de Continuidade de Negócio, este por sua vez, não fora elaborado. O *PCN* deveria ser baseado na análise de risco da universidade que também é inexistente. A ausência de um Plano de Continuidade de Negócio também foi constatada no UFLA (2011a).

Tabela 4.14: Dimensão de Análise: Conformidade

Categoria de Análise	Nível	Percentual
Conformidade com requisitos legais e contratuais	Indefinido	-
Conformidade com requisitos legais e contratuais	Informal	83,33%
Análise crítica da segurança da informação	Informal	83,33%

A Categoria de análise Conformidade com requisitos legais possui dois critérios avaliados Proteção dos registros com base na legislação aplicável e Conformidade com as políticas de segurança da informação. Para o primeiro critério, a maturidade foi considerada Indefinida havendo empate nos níveis Informal e Organizado. O autor deste trabalho considerou a maturidade como Organizado, pois existem leis e normas específicas a segurança da informação a *APF* como as levantadas na Tabela 2.1. Já a maturidade do segundo critério, foi considerada Informal pelos gestores. Não existiam procedimentos formais para a classificação dos registros de acordo com a estrutura da universidade. Existiam sistemas de armazenamentos para os registros como servidores e arquivos, mas nem todos os arquivos dispunham de armazenamento correto para evitar sua deterioração.

A última Categoria de análise da Tabela 4.14, Análise crítica da segurança da informação, também teve seu nível de maturidade definido como Informal. Não existiam procedimentos formais para averiguar se os requisitos, procedimentos e normas de segurança da informação estabelecidos na política e em outras regulamentações estavam sendo atendidos.

Como resultado geral, a avaliação da maturidade apresentou um resultado preocupante, 78% dos processos avaliados apresentaram o nível de maturidade Informal, contra 11% Organizado e 11% Indefinido conforme a Figura 4.1.

Alguns fatores contribuíram de forma significativa para este baixo resultado como: a falta da documentação dos processos, a inexistência da análise e avaliação dos riscos, desatualização do *PDTI* e da *PSI*, além da ausência do plano

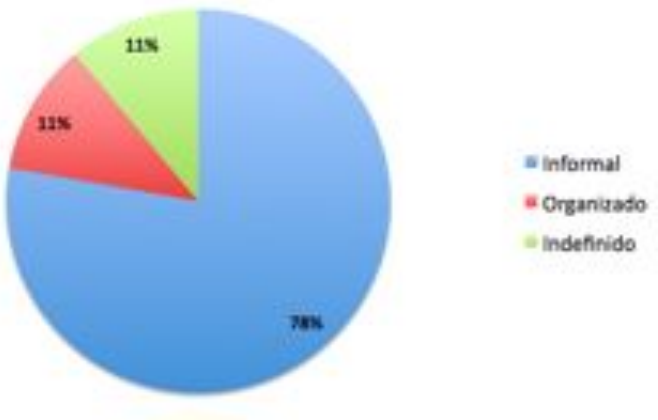

Figura 4.1: Resultado da Avaliação

de continuidade de negócios e o déficit de funcionários em algumas coordenadorias.

A documentação dos processos é a transformação do conhecimento tácito em gestão do conhecimento, onde o conhecimento é formalizado e acessível a todos. Uma vez formalizados, os processos serão mais ágeis, eficazes e terão os riscos residuais de cada operação calculados, eliminando retrabalhos e gastos desnecessários.

A análise e avaliação dos riscos é necessária para a identificação e conhecimento dos riscos aos quais a *UFLA* e o *DGTI* estão expostos possibilitando a adoção de práticas e controles mais eficientes. A inexistência dessa análise, representa um risco de ausência ou de ações de segurança ineficazes e descoordenadas. O resultado dessa análise é insumo a outros processos e atividades.

A desatualização dos documentos que sustentam a *SI* deve-se a dissolução do Comitê de Segurança da Informação e Comunicação da universidade. A descontinuidade dos trabalhos deste comitê, sugerem um baixo envolvimento da alta administração com a *GSI* e a falta de planejamento para ações a médio prazo.

Com apenas um gestor de *SI* responsável por toda universidade, muitas das ações e procedimentos de segurança esbarram no gargalo do déficit de funcionários e se tornam rotinas apenas para a resolução de problemas.

A constatação como Informal, a maturidade dos processos avaliados por este estudo, também reforça a discussão da situação da *SI* na administração pública em um momento que ela foi colocada a prova por constantes escândalos e vazamento de informações.

5 CONCLUSÃO

A informação é um dos ativos mais importantes do mundo moderno. O avanço das tecnologias e comunicações transformou o ciclo de vida da informação e a forma de protegê-la. A proteção desses ativos da informação, não pode ser vista como uma iniciativa isolada de *TI*, ou como um conjunto de ações pontuais executadas em momentos de crise. Ela deve ser parte de um sistema de gestão apoiado em pessoas, processos, tecnologias, patrocinado pela alta administração e que atenda às demandas de segurança da organização.

As organizações da *APF* passam por um momento onde precisam demonstrar mais eficiência e transparência. Nesse novo cenário, elas não podem mais usar estratégias e medidas de segurança da informação improvisadas.

Apesar de existirem um conjunto de leis e regulamentações de segurança, como os Decretos e as Normas do *GSIPR*, que deveriam assegurar um nível adequado de segurança da informação aos órgãos, os resultados desse estudo de caso apontaram para uma baixa maturidade dos processos da instituição avaliada.

Ainda há um extenso caminho a ser percorrido para a melhoria do nível da maturidade na instituição avaliada. Existem diversas iniciativas com o objetivo de melhorar a qualidade dos processos, mas parece faltar decisões estratégicas que apoiem e sustentem essas ações de forma integrada.

O objetivo deste trabalho foi avaliar a maturidade dos processos de segurança da informação na instituição de ensino superior da *APF*. O objetivo foi alcançado, através de um instrumento de avaliação baseado nos requisitos da norma *ABNT NBR ISO/IEC* 27001. O instrumento atualizado, cumpriu seu objetivo de avaliar a maturidade de cada processo.

Como trabalhos futuro, existe ainda a necessidade de uma pesquisa em um número maior de instituições públicas do ensino superior, buscando confirmar ou identificar novos fatores que possam explicar o baixo nível de maturidade encontrado.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT. *ABNT NBR ISO/IEC 27002 Tecnologia da informação - Técnicas de segurança - Código de pratica para a gestão da segurança da informação*. Rio de Janeiro, 2005.

ABNT. *ABNT NBR ISO/IEC 27001 Tecnologia da informação - Técnicas de segurança - Requisitos*. Rio de Janeiro, 2013.

ARAUJO, W. J. de. Leis, decretos e normas sobre gestão da segurança da informação nos órgãos da administração pública federal. *Informação & Sociedade: Estudos*, v. 22, 2012.

BEAL, A. *Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações*. [S.l.]: Atlas, 2005.

BRASIL. Decreto no 3.505, de 13 de junho de 2000. *Diário Oficial da União*, Brasília, Junho 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em: 05 jan 2014.

BRASIL. *Acórdão 1603/2008-Plenário*. Brasília, 2008. Disponível em: <http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_informacao/pesquisas_governanca/D75C7DF1F44EB21CE040010A890070EC>. Acesso em: 1 jan 2014.

BRASIL. *Acórdão 2585/2012-Plenário*. Brasília, 2012. Disponível em: <http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_informacao/pesquisas_governanca/D500BE942EEF7793E040010A89001367>. Acesso em: 2 jan 2014.

CAMPOS, L. S. L. D. Q. *UMA PROPOSTA DE CONCEITO PARA 'COMUNICAÇÕES' NO TERMO SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES*. Dissertação (Mestrado) — UNIVERSIDADE DE BRASÍLIA, 2008. Disponível em: <http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/liliana_suzete.pdf>. Acesso em: 6 Maio 2014.

CROSBY, P. B. *Quality is free: The art of making quality certain*. [S.l.]: McGraw-Hill New York, 1979.

FERNANDES, J. H. C. *Metodologia de Pesquisas de Estudo de Caso no Programa de Formação de Especialistas para Desenvolvimento da Estratégia e Metodologia Brasileira de Gestão de Segurança da Informação e Comunicações*. Brasília, 2010.

FERREIRA, A. B. d. H. *et al.* Novo dicionário aurélio-século xxi. *Rio de Janeiro: Nova Fronteira*, v. 1, 1999.

GABRICH, C. C. C. *Avaliação da Maturidade dos Processos de Segurança da Informação do Banco Gama: a percpeção dos gestores*. Dissertação (Mestrado) — Universidade de Brasília, Brasília, 2011.

GIL, A. C. Métodos e técnicas de pesquisa social; methods and techniques of social research. Atlas, 2010.

GSIPR, D. D. S. D. I. E. C. D. *Instrução Normativa GSI/PR no 1*. Brasília, 2008. Disponível em: <http://www.governoeletronico.gov.br/anexos/instrucao-normativa-no-01-2009-gsi>. Acesso em: 9 Jan 2014.

HOUAISS, A.; VILLAR, M. de S.; FRANCO, F. M. de M. *Minidicionário Houaiss da língua portuguesa*. [S.l.]: Objetiva Rio de Janeiro, 2001.

IEC. 2014. Disponível em: <http://www.iec.org>. Acesso em: 24 Janeiro 2014.

ISO/IEC. *ISO/IEC 27000*: Information technology — security techniques — information security management systems — overview and vocabulary. Second edition. [S.l.]: ISO/IEC, 2012.

JANSSEN, L. A. *Instrumento de avaliação de maturidade em processos de segurança da informação: estudo de caso em instituições hospitalares*. Dissertação (Mestrado) — PUCRS, 2008. Disponível em: <http://repositorio.pucrs.br/dspace/bitstream/10923/1240/1/000400421-Texto%2bCompleto-0.pdf>. Acesso em: 7 Janeiro 2014.

KLIMKO, G. Knowledge management and maturity models: Building common understanding. In: BLED, SLOVENIA. *Proceedings of the 2nd European Conference on Knowledge Management*. [S.l.], 2001. p. 269–278.

NAKAMURA, E. T. Geus, paulo l. de. *Segurança de Redes em Ambiente Cooperativos*, 2002.

PDI: Plano de desenvolvimento institucional 2011/2015. Lavras: UFLA, 2010.

PINHEIRO, P. P.; SLEIMAN, C. M. *Tudo o que você precisa saber sobre direito digital no dia a dia*. [S.l.]: Saraiva, 2009.

RIGON, E. A.; WESTPHALL, C. M. *Modelo de Avaliação da Maturidade da Segurança da Informação*. [S.l.]: UFSC, 2010.

ROCHA. *Acusação de roubo de base de dados agita web brasileira*. Rio de Janeiro: Módulo Security Magazine, 2002.

RUSSELL, D.; GANGEMI, G. *Computer security basics*. [S.l.]: O'Reilly Media, Inc., 1991.

SÊMOLA, M. *Gestão da segurança da informação: uma visão executiva*. [S.l.]: Campus, 2003.

SIEWERT, V. C. A constante evolução da segurança da informação. 2006. Disponível em: <http://www.artigocientifico.com.br/uploads/artc_1202929819_49.pdf>. Acesso em: 9 Jan 2014.

SURVEY, I. *ISO*. 2012. 2012. Disponível em: <http://www.iso27001security.com/html/27001.html>. Acesso em: 30 Maio 2014.

TCU, T. de Contas da U. *Boas práticas em segurança da informação*. Brasília, 2008. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2059160.PDF>. Acesso em: 9 Jan 2014.

TCU, T. de Contas da U. *Boas práticas em segurança da informação*. 4. ed. Brasília, 2012. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2511466.PDF>. Acesso em: 30 dez 2013.

UFLA. *PDTI Plano Diretor de Tecnologia da Informação*. UFLA, 2011. Disponível em: <http://www.dgti.ufla.br/site/wp-content/uploads/2011/10/PDTI.pdf>. Acesso em: 7 Janeiro 2014.

UFLA. *RESOLUÇÃO CUNI No 054, DE 5 DE JULHO DE 2011*. 2011. 2011. Disponível em: <www.ufla.br/documentos/arquivos/1_CUNI%20054.pdf>. Acesso em: 7 Janeiro 2014.

UFLA. *RESOLUÇÃO CUNI Nº 030, DE 15 DE MAIO DE 2012*. 2012. Disponível em: <http://www.ufla.br/documentos/arquivos/030_15052012.pdf>. Acesso em: 7 Janeiro 2014.

VERGARA, S. C. *Projetos e relatórios de pesquisa em administração*. [S.l.]: Atlas, 2005.

VIEIRA, T. M. *QUADRO DA LEGISLAÇÃO RELACIONADA À SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES*. 2013. Disponível em: <http://dsic.planalto.gov.br/documentos/quadro_legislacao.htm>. Acesso em: 25 Abril 2014.

XIANG, W.; WANG, Y.; ZHANG, Z. The research on business continuity planning of e-government based on information security risk management. In: *Networking, Sensing and Control, 2008. ICNSC 2008. IEEE International Conference on*. [S.l.: s.n.], 2008. p. 446–450.

YIN, R. K.; GRASSI, D. Estudo de caso. Bookman Porto Alegre, 2010.

A APÊNDICE

Dimensão de análise da ISO/IEC 27001:2013	Categoria de Analise	Nr.	Critério	Inexistente	Informal	Organizado	Gerenciado	Otimizado	Especificação da forma de controle
Políticas de segurança da informação	Orientação da Direção para segurança da informação	1	**Documentação da política de segurança da informação**	Não existe nenhuma política de segurança da informação ( )	Existe uma política de segurança da informação informal ( )	Existe uma política de segurança da informação formalizada ( )	Existe uma política de segurança da informação formalizada e revisada, com indicadores de acompanhamento de sua implementação ( )	Com base nos indicadores são implementadas melhorias contínuas na política de segurança da informação ( )	
Organização da segurança da informação	Organização interna	2	**Responsabilidade organizacional quanto à segurança da informação**	Não existe definição de responsabilidades pela segurança da informação dentro da organização ( )	Existe, informalmente, uma atribuição de responsabilidades pela segurança da informação ( )	As responsabilidades pela segurança da informação são atribuídas formalmente dentro da organização ( )	Existe um processo formal para a atribuição das responsabilidades pela segurança da informação dentro da organização, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias continuas no processo de atribuição de responsabilidades pela segurança da informação dentro da organização ( )	
	Dispositivos móveis e trabalho remoto	3	**Dispositivos móveis e trabalho remoto**	Não existem procedimentos de segurança definidos para dispositivos móveis e trabalho remoto ( )	Existem procedimentos informais de segurança para dispositivos móveis e trabalho remoto ( )	Existem procedimentos de segurança documentados para dispositivos móveis e trabalho remoto ( )	Existe um processo formal de controle da segurança para dispositivos móveis e trabalho remoto, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas nos procedimentos de segurança para dispositivos móveis e trabalho remoto ( )	

Dimensão de análise da ISO/IEC 27001:2013	Categoria de Análise	Nr.	Critério	Inexistente	Informal	Organizado	Gerenciado	Otimizado	Especificação da forma de controle
Segurança em recursos humanos	Antes da contratação	4	**Processos admissionais**	Não existe, na admissão de funcionários ou partes externas, um` processo de esclarecimento das responssabilidades com a segurança da informação na organização ( )	Existe, na admissão de funcionários ou partes externas, um processo informal de esclarecimento quanto a responsabilidades pela segurança da informação na organização ( )	Existe, na admissão de funcionários ou partes externas, um processo formal de esclarecimento quanto as responsabilidades pela segurança da informação na organização ( )	Existe, na admissão de funcionários ou partes externas, um processo formal de esclarecimento quanto as responsabilidades pela segurança da informação na organização, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas nos processos de admissão, no que se refere ao esclarecimento quanto as responsabilidades pela segurança da informação na organização ( )	
	Durante a contratação	5	**Conscientização, educação e treinamento em segurança da informação**	Não existe um processo de conscientização, educação ou treinamento em segurança da informação na organização ( )	Existe informalmente um processo de conscientização, educação ou treinamento em segurança da informação na organização ( )	Existe um processo formal de conscientização, educação ou treinamento em segurança da informação na organização ( )	Existe um processo formal de conscientização, educação ou treinamento em segurança da informação na organização, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas no processo de conscientização, educação e treinamento em segurança da informação na organização ( )	
	Encerramento e mudança da contratação	6	**Responsabilidades na demissão ou alteração da contratação**	Não existe uma definição de responsabilidades e obrigações no processo de demissão ou mudança da contratação quanto a segurança da informação ( )	Existe uma definição informal de responsabilidades e obrigações no processo de demissão ou mudança da contratação quanto a segurança da informação ( )	Existe uma definição documentada de responsabilidades e obrigações no processo de demissão ou mudança da contratação quanto a segurança da informação ( )	Existe um processo formal de definição de responsabilidades e obrigações no processo de demissão ou mudança da contratação quanto a segurança da informação, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas na definição de responsabilidades e obrigações no processo de demissão ou alteração da contratação quanto a segurança da informação ( )	
Gestão de ativos	Responsabilidades pelos ativos	7	**Inventário e alocação de ativos**	Não existe controle de inventário e alocação dos ativos ( )	Existe um controle informal de inventário e alocação dos ativos ( )	Existe um controle documentado de inventário e alocação dos ativos ( )	Existe um controle documentado de inventário e alocação dos ativos, revisado periodicamente, com indicadores de acompanhamento ( )	Com base nos indicadores são implementadas melhorias contínuas no processo de inventário e alocação dos ativos ( )	

	Classificação da informação	8	**Diretrizes para classificação da informação**	Não existem diretrizes organizacionais para a classificação da informação ( )	Existem diretrizes informais para classificação da informação dentro da organização ( )	Existem diretrizes formalizadas para classificação da informação dentro da organização ( )	Existem diretrizes formalizadas para classificação da informação dentro da organização, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas nas diretrizes organizacionais para classificação da informação ( )	
	Tratamento de mídia	9	**Armazenamento e descarte de mídiasremovíveis**	Não existem procedimentos definidos para armazenamento e descarte das mídias removíveis ( )	Existem procedimentos informais para armazenamento e descarte das mídias removíveis ( )	Existem procedimentos documentados para armazenamento e descarte das mídias removíveis ( )	Existe um processo formal para armazenamento e descarte das mídias removíveis, com indicadores de acompanhamento ( )	Com base em indicadores, são implementadas melhorias contínuas nos processos de armazenamento e descarte das mídias removíveis ( )	

Dimensão de Análise ISO/IEC 27001:2013	Categoria de Análise	Nr.	Critério	Inexistente	Informal	Organizado	Gerenciado	Otimizado	Especificação da forma de controle
Controles de acesso	Requisitos de negócio para controle de acesso	10	**Política de controle de acesso**	Não existe uma política/norma de controle de acesso aos sistemas ( )	Existe uma política/norma informal de controle de acesso aos sistemas ( )	Existe uma política/norma documentada de controle de acesso aos sistemas ( )	Existe uma política/norma documentada de controle de acesso aos sistemas, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas na política/norma de controle de acesso aos sistemas ( )	
	Gerenciamento de acesso do usuários	11	**Gerenciamento de acesso dos usuários**	Não existem procedimentos para registro/cancelamento do usuário bem como conceder/retirar os direitos de acesso aos sistemas ( )	Existem procedimentos informais para registro/cancelamento do usuário bem como conceder/retirar os direitos de acesso acesso dos usuários aos sistemas ( )	Existem procedimentos documentados para registro/cancelamento do usuário bem como conceder/retirar os direitos de acesso aos sistemas ( )	Existe um processo formal para registro/cancelamento do usuário bem como conceder/retirar os direitos de acesso aos sistemas, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas no processo de gerenciamento de acesso dos usuários aos sistemas ( )	
	Responsabilidades dos usuários	12	**Uso da informação secreta**	Não existe um procedimento ou norma para proteção das informações para autenticação nos sistemas ( )	Existem procedimentos ou normas informais para proteção das informações para autenticação nos sistemas ( )	Existem procedimentos ou normas documentados para proteção das informações para autenticação nos sistemas ( )	Existem procedimentos ou normas formais para proteção das informações para autenticação nos sistemas com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias de procedimentos ou normas para proteção das informações para autenticação nos sistemas ( )	
	Controle de acesso ao sistemas e à aplicação	13	**Restrição de acesso à informação**	Não existem procedimentos (log-on, senhas fortes e etc) para restringir o acesso à informação contida nos sistemas e nas aplicações ( )	Existem procedimentos (log-on, senhas fortes e etc) informais para restringir o acesso à informação contida nos sistemas e nas aplicações ( )	Existem procedimentos (log-on, senhas fortes e etc) documentados para restringir o acesso à infomação contida nos sistemas e nas aplicações ( )	Existe um processo formal para restringir o acesso à informação contida nos sistemas e nas aplicações, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas no processo de proteção das informações contidas nos sistemas e nas aplicações ( )	
Criptografia	Criptografia	14	**Política de uso de criptografia**	Não existe uma política/norma sobre o uso de criptografia ( )	Existe uma política/norma informal sobre o uso de criptografia ( )	Existe uma política/norma documentada sobre o uso de criptografia ( )	Existe uma política/norma documentada sobre uso de criptografia, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas na política/norma sobre o uso de criptografia ( )	

Dimensão de Análise ISO/IEC 27001:2013	Categoria de Análise	Nr.	Critério	Inexistente	Informal	Organizado	Gerenciado	Otimizado	Especificação da forma de controle
Segurança física e do ambiente	Áreas seguras	15	**Controle de acesso físico dos colaboradores**	Não existem regras para o controle de acesso físico dos colaboradores ( )	Existem regras informais para o controle de acesso físico dos colaboradores ( )	Existem regras documentadas para o controle de acesso físico dos colaboradores ( )	Existem regras documentadas para o controle de acesso físico dos colaboradores, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas no controle de acesso físico dos colaboradores ( )	
	Equipamentos	16	**Segurança dos equipamentos que processam ou armazenam informações**	Não existem procedimentos para a proteção dos equipamentos que processam ou armazenam informações ( )	Existem procedimentos informais para a proteção dos equipamentos que processam ou armazenam informações ( )	Existem procedimentos documentados para a proteção dos equipamentos que processam ou armazenam informações ( )	Existe um processo formal para a proteção dos equipamentos que processam ou armazenam informações, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas relacionadas à proteção dos equipamentos que processam ou armazenam informações ( )	
Segurança nas operações	Responsabilidades dos procedimentos de operação	15	**Procedimentos operacionais e processamento da informação**	Não existem procedimentos operacionais e controles nos processos de negócio ( )	Existem, informalmente, procedimentos operacionais e controles nos processos de negócio ( )	Existem procedimentos operacionais e controles nos processos de negócio documentados e disponibilizados ( )	Existem procedimentos operacionais e controles nos processos de negócio documentados e disponibilizados, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas nos procedimentos operacionais e controles nos processos de negócio ( )	
	Proteção contra malware	18	**Controle contra malware**	Não existem procedimentos para a proteção dos *software* contra malware ( )	Existem procedimentos informais para a proteção dos *software* contra malware ( )	Existem procedimentos documentados para a proteção dos *software* contra malware ( )	Existe um processo formal para a proteção dos *software* contra malware, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas no processo de proteção dos *software* contra malware ( )	
	Cópias de segurança	19	**Backup das informações**	Não existem procedimentos definidos para geração e manutenção das cópias de segurança ( )	Existem procedimentos informais para geração e manutenção das cópias de segurança ( )	Existem procedimentos documentados para geração e manutenção das cópias de segurança ( )	Existe um processo formal para geração e manutenção das cópias de segurança, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas nos processos de geração e manutenção das cópias de segurança ( )	
	Registro e monitoramento	20	**Registro das atividades de processamento da informação**	Não existem procedimentos de registros das atividades realizadas nos sistemas ( )	Existem procedimentos informais de resgistros das atividades realizadas nos sistemas ( )	Existem procedimentos documentados de registros das atividades realizadas nos sistemas ( )	Existe um processo formal de registros das atividades realizadas nos sistemas, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas no processo de registros das atividades realizadas nos sistemas ( )	

Dimensão de Análise ISO/IEC 27001:2013	Categoria de Análise	Nr.	Critério	Inexistente	Informal	Organizado	Gerenciado	Otimizado	Especificação da forma de controle
Segurança nas operações	Controle do software operacional	21	**Controle das bases de dados dos sistemas aplicativos**	Não existem procedimentos para controlar a instalação de software em sistemas operacionais ( )	Existem procedimentos informais para controlar a instalação de software em sistemas operacionais ( )	Existem procedimentos documentados para controlar a instalação de software em sistemas operacionais ( )	Existe um processo formal de controle de instalação de software em sistemas operacionais com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas no processo de controle da instalação de software em sistemas operacionais ( )	
	Gestão de vulnerabilidades técnicas	22	**Controle das vulnerabilidades técnicas dos sistemas**	Não existem procedimentos para controle de vulnerabilidades técnicas dos sistemas ( )	Existem procedimentos informais para controle de vulnerabilidades técnicas dos sistemas ( )	Existem procedimentos documentados para controle de vulnerabilidades técnicas dos sistemas ( )	Existe um processo formal para controle de vulnerabilidades técnicas dos sistemas, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas no processo de controle de vulnerabilidades técnicas dos sistemas ( )	
	Consideração quanto à auditoria de sistemas de informação	23	**Planejamento das atividades de auditoria nos sistemas de informação**	Não existe planejamento referente às atividades de auditoria nos sistemas de informação ( )	Existe, informalmente, um planejamento referente às atividades de auditoria nos sistemas de informação ( )	Existe um planejamento formal das atividades de auditoria nos sistemas de informação ( )	Existe um processo formal de planejamento das atividades de auditoria nos sistemas de informação, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas no processo de auditoria nos sistemas de informação ( )	
Segurança das comunicações	Gerenciamento da segurança em redes	24	**Proteção das informações em redes**	Não existem procedimentos definidos para a proteção das informações em redes ( )	Existem procedimentos informais para a proteção das informações em redes ( )	Existem procedimentos documentados para a proteção das informações em redes ( )	Existe um processo formal para a proteção das informações em redes, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas no processo de proteção das informações em redes ( )	
	Transferência da informação	25	**Transferência da informação**	Não existem processos para proteção das mensagens eletrônicas dentro e fora da organização ( )	Existem processos informais para proteção das mensagens eletrônicas dentro e fora da organização ( )	Existem processos documentados para proteção das mensagens eletrônicas dentro e fora da organização ( )	Existem processos formais documentados para proteção das mensagens eletrônicas dentro e fora da organização , com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas nos processos para proteção das mensagens eletrônicas dentro e fora da organização ( )	

Dimensão de Análise ISO/IEC 27001:2013	Categoria de Análise	Nr.	Critério	Inexistente	Informal	Organizado	Gerenciado	Otimizado	Especificação da forma de controle
Aquisição, desenvolvimento e manutenção de sistemas	Requisitos de segurança de sistemas de informação	26	**Proteção da informação sobre redes públicas e em aplicativos de serviços**	Não existem procedimentos para proteção das informações sobre redes públicas ( )	Existem procedimentos informais para proteção das informações sobre redes públicas ( )	Existem procedimentos documentados para proteção das informações sobre redes públicas ( )	Existe um processo formal para análise e inclusão de requisistos de segurança nas informações sobre redes públicas ( )	Com base nos indicadores, são implementadas melhorias contínuas no processo de análise e inclusão de requisistos de segurança nas informações sobre redes públicas ( )	
	Segurança em processos de desenvolvimento e de suporte	27	**Desenvolvimento e alteração e teste dos sistemas**	Não existe controle de desenvolvimento e alteração e teste dos sistemas ( )	Existe uma verificação informal de segurança nos processos de desenvolvimento e alteração e teste dos sistemas ( )	Existem procedimentos documentados de controle da segurança nos processos de desenvolvimento e alteração e testes dos sistemas ( )	Existe um processo formal de controle da segurança no desenvolvimento e na alteração e teste dos sistemas, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas no processo de controle da segurança no desenvolvimento e na alteração e teste dos sistemas ( )	
	Dados para teste	28	**Proteção dos dados para teste**	Não existem procedimentos para a seleção e proteção de dados para teste ( )	Existe uma verificação informal de segurança nos processos seleção e proteção de dados para teste ( )	Existem processos documentados para a seleção e proteção de dados para teste ( )	Existe um processso formal para a seleção e proteção de dados para teste, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas no processo para a selação e proteção de dados para teste ( )	
Relacionamento com a cadeia de suprimento	Segurança da informação na cadeia de suprimento	29	**Acesso dos fornecedores as informações**	Não existem requisitos de segurança para o acesso de fornecedores às informações organizacionais ( )	Existem requisitos informais de segurança para o acesso de fornecedores às informações organizacionais ( )	Existem requisitos de segurança documentados para o acesso de fornecedores às informações organizacionais ( )	Exitem requisitos de segurança documentados para o acesso de fornecedores às informações organizacionais, revisados periodicamente e acompanhados por indicadores ( )	Com base nos indicadores, são implementadas melhorias contínuas nos requisitos de segurança para o acesso dos fornecedores às informações organizacionais ( )	
	Gerenciamento da entrega do serviço do fornecedor	30	**Gestão de serviços com fornecedores**	Não existe um processo para a gestão dos serviços executados pelos fornecedores ( )	Existe, informalmente, um processo para a gestão dos serviços executados pelos fornecedores ( )	Existe um processo formal para a gestão dos serviços executados pelos fornecedores ( )	Existe um processo formal de gestão de serviços executados pelos fornecedores com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas na gestão de serviços executadados pelos fornecedores ( )	

Dimensão de Análise ISO/IEC 27001:2013	Categoria de Análise	Nr.	Critério	Inexistente	Informal	Organizado	Gerenciado	Otimizado	Especificação da forma de controle
Gestão de incidentes de segurança da informação	Gestão de incidentes de segurança da informação e melhorias	31	**Comunicação dos eventos e deficiências de segurança da informação**	Não existem procedimentos para a comunicação dos eventos e deficiências de segurança da informação ( )	Existem procedimentos informais comunicação dos eventos e deficiências de segurança da informação ( )	Existem procedimentos documentados para a comunicação dos eventos e deficiências de segurança da informação ( )	Existe um processo formal para a comunicação dos eventos e deficiências de segurança da informação com indicadores de acompanhamento ( )	Com base nos indicadores são implementadas melhorias contínuas no processo de gestão de incidentes de segurança da informação ( )	
Aspectos da sedasdasgurança da informação na gestão da contidsadasnuidade do negócio	Continuidade da segurança da informação	32	**Gestão da continuidade de negócios**	Não existem requisitos de segurança da informação no processo de gestão da continuidade de negócios ( )	Existem, informalmente, requisitos de segurança da informação contemplados no processo de gestão da continuidade de negócios ( )	Existem requisitos de segurança da informação contemplados no processo de gestão da continuidade de negócios ( )	Existem requisitos de segurança da informação formalmente contemplados no processo de gestão da continuidade dos negócios, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas no processo de gestão da continuidade de negócios no que se refere à segurança da informação ( )	
	Redundâncias	33	**Disponibilidade dos recursos de processamento de informação**	Não existem processos para redundâncias de sistemas ( )	Existem, informalmente, processos para redundância de sistemas ( )	Existem processos documentados para a redundância de sistemas ( )	Existe um processo formal para redundância de sistemas com indicadores de acompanhamento ( )	Com base nos indicadores são implementadas melhorias contínuas no processo de redundância de sistemas ( )	
Conformidade	Conformidade com requisitos legais e contratuais	34	**Identificação da legislaçãoaplicável**	Não existem procedimentos para identificação da legislação de segurança da informação aplicável à empresa ( )	Existem procedimentos informais para identificação da legislação de segurança da informação aplicável à empresa ( )	Existem procedimentos documentados para identificação da legislação de segurança da informação aplicável à empresa ( )	Existe um processo formal de identificação da legislação de segurança da informação, com indicadores de acompanhamento ( )	Com base nos indicadores são implementadas melhorias contínuas no processo de identificação da legislação de segurança da informação aplicável à empresa ( )	
		35	**Proteção dos registros com base na legislaçãoaplicável**	Não existem procedimentos para a proteção dos registros organizacionais, com base na legislação aplicável ( )	Existem procedimentos informais para a proteção dos registros organizacionais com base na legislação aplicável ( )	Existem procedimentos documentados para a proteção dos registros organizacionais com base na legislação aplicável ( )	Existe um processo formal para proteção dos registros organizacionais, de acordo com a legislação aplicável, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas no processo de proteção dos registros organizacionais ( )	
	Análise crítica da segurança da informação	36	**Conformidade dos sistemas com as políticas de segurança da informação**	Não existem procedimentos para verificação da conformidade dos sistemas com as políticas de segurança da informação ( )	Existem procedimentos informais para verificação da conformidade dos sistemas com as políticas de segurança da informação ( )	Existem procedimentos documentados para verificação da conformidade dos sistemas com as políticas de segurança da informação ( )	Existe um processo formal de verificação da conformidade dos sistemas com as políticas de segurança da informação, com indicadores de acompanhamento ( )	Com base nos indicadores, são implementadas melhorias contínuas no processo de verificação da conformidade dos sistemas com as políticas de segurança da informação ( )	

B ANEXO A

Os gráficos a seguir, ilustram os resultados encontrados de cada objetivo de controle:

Figura B.1: Documentação da política de segurança da informação

Figura B.2: Responsabilidade organizacional quanto à segurança da informação

Figura B.3: Dispositivos móveis e trabalho remoto

Figura B.4: Processos Admissionais

Figura B.5: Conscientização, educação e treinamento em segurança da informação

Figura B.6: Responsabilidades na demissão ou alteração da contratação

Figura B.7: Inventário e alocação de ativos

Figura B.8: Diretrizes para classificação da informação

Figura B.9: Armazenamento e descarte de mídias removíveis

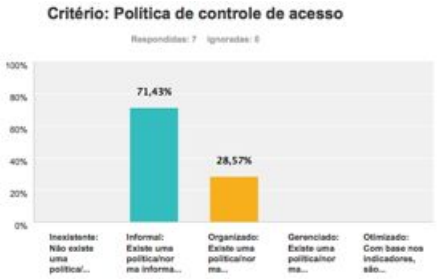

Figura B.10: Política de controle de acesso

Figura B.11: Gerenciamento de acesso dos usuários

Figura B.12: Uso da informação secreta

Figura B.13: Restrição de acesso a informação

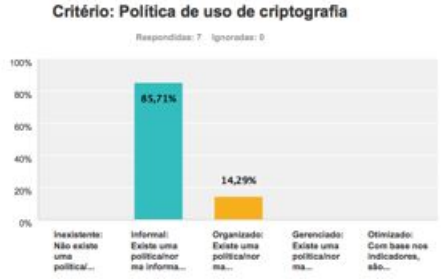

Figura B.14: Política de uso de criptografia

Figura B.15: Controle de acesso físico dos colaboradores

Figura B.16: Segurança dos equipamentos que processam ou armazenam informações

Figura B.17: Procedimentos operacionais e processamento da informação

Figura B.18: Controle contra malware

Figura B.19: Backup das informações

Figura B.20: Registro das atividades de processamento da informação

Figura B.21: Controle das bases de dados dos sistemas aplicativos

Figura B.22: Controle das vulnerabilidades técnicas dos sistemas

Figura B.23: Planejamento das atividades de auditoria nos sistemas de informação

Figura B.24: Proteção das informações em redes

Figura B.25: Transferência da informação

Figura B.26: Proteção da informação sobre redes públicas e em aplicativos de serviços

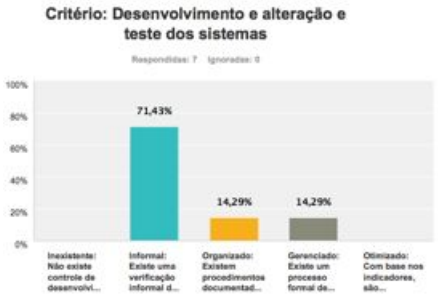

Figura B.27: Desenvolvimento e alteração e teste dos sistemas

Figura B.28: Proteção dos dados para teste

Figura B.29: Acesso dos fornecedores as informações

Figura B.30: Gestão de serviços com fornecedores

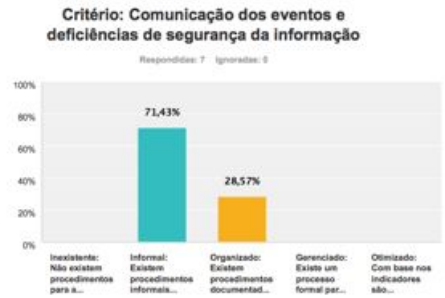

Figura B.31: Comunicação dos eventos e deficiências de segurança da informação

Figura B.32: Gestão da continuidade de negócios

Figura B.33: Disponibilidade dos recursos de processamento de informação

Figura B.34: Identificação da legislação aplicável

Figura B.35: Proteção dos registros com base na legislação aplicável

Figura B.36: Conformidade dos sistemas com as políticas de segurança da informação