UNIVERSIDADE FEDERAL DO PARANÁ

ADRIANA DE ALMEIDA DO NASCIMENTO

Aplicabilidade da segurança da informação nos processos de auditoria de informação

CURITIBA
2013

ADRIANA DE ALMEIDA DO NASCIMENTO

Aplicabilidade da segurança da informação nos processos de auditoria de informação

Monografia apresentada à disciplina de Pesquisa em Informação (SIN 119), como requisito parcial à conclusão do Curso de Gestão da Informação, Setor de Ciências Sociais Aplicadas, Universidade Federal do Paraná.

Orientador: Prof. Dr. José Simão de Paula Pinto

CURITIBA
2013

AGRADECIMENTOS

Agradeço primeiramente a Deus, que pela Sua graça permitiu que realizasse este trabalho, me dando saúde, e perseverança.

A meu esposo Edenilson Roberto do Nascimento, pelo seu amor, companheirismo e paciência, sempre me incentivando, encorajando e me auxiliando nas necessidades.

Ao meu filho Paulo Henrique, que mesmo com sua pouca idade compreendeu que eu precisava ficar horas e horas em frente ao computador trabalhando e sempre tinha uma palavra amorosa para me falar.

Agradeço ao professor Simão que aceitou me orientar nesse trabalho e nos demais realizado sob sua orientação, sempre me passando orientações que foram imprescindíveis para a conclusão desse trabalho.

Aos demais docentes do Curso Gestão da Informação da Universidade Federal do Paraná, que cada um em sua área compartilhou dos seus conhecimentos e assim contribuíram para meu crescimento profissional.

RESUMO

Aborda o tema segurança da informação e processos de auditoria da informação, com o objetivo de mostrar a aplicabilidade dos pilares da segurança da informação nas etapas do processo de auditoria da informação. Realizou-se pesquisa bibliográfica, em artigos e livros existentes em bases de dados nacionais e internacionais que abordaram o assunto a partir do ano 2000. Foi utilizado um modelo de Processos de auditoria já abordado anteriormente e que foi criado a partir de modelos presentes na literatura. Para o tema segurança da informação foi apresentado um processo de maturidade em segurança da informação, pelo qual é possível perceber como se trata a segurança da informação nas organizações. Conclui apresentando a aplicabilidade desses pilares nos processos de auditoria.

Palavras chave: Auditoria da informação. Segurança da informação. Processos de auditoria.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABNT - Associação Brasileira de Normas Técnicas

CMMI -*Capability Maturity Model Integration*

COBIT -*Control Objectives for Information and Related Technology*

DMBOK -*Data Management Body of Knowledge*

IEC -*International Electrotechnical Commission*

ITGI -*Information Technology Governance Institute*

ISACA -*Information Systems Audit and Control Association*

ISO -*International Organization for Standardization*

NBR - Denominação de norma da Associação Brasileira de Normas Técnicas

TI -Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

A auditoria da informação tem como objetivo identificar as necessidades informacionais da organização, assim como determinar os requisitos de negócio da organização e como essas informações podem atender melhor cada necessidade. Para a realização da auditoria da informação é necessário definir as etapas para então ocorrer à execução, que pode ser realizada por uma equipe interna ou externa a organização.

Essas etapas são apresentadas por vários autores na literatura, entre elas envolve planejamento, coleta de dados, análise de dados, avaliação de dados, comunicação e recomendações. O Guia internacional DAMA DMBOK (*Data Management Body of Knowledge)*, apresenta como objetivo final da gestão da segurança de dados, proteger os ativos de informação em alinhamento com as regulamentações de privacidade e confidencialidade e com os requisitos do negócio.

Para a realização de uma auditoria da informação seja por uma equipe interna ou externa à organização, os ativos informacionais ficarão expostos aos envolvidos na realização dos processos auditoria. Desta forma a organização corre o risco de ter suas informações divulgadas/violadas de forma indevida ou então repassadas a terceiros, e assim comprometer não só o andamento e resultado da auditoria como também as decisões futuras que seriam tomadas com o resultado dessa auditoria.

Desta forma, a segurança da Informação (SI), nos processos de auditoria é muito importante, pois envolvem pessoas. Segundo Schneier (2001), a camada humana é uma das mais difíceis de avaliar e gerenciar na segurança da informação, justamente porque envolve o fator humano com características psicológicas, sócios culturais e emocionais diferentes.

Tendo em vista que a maioria dos trabalhos encontrados atualmente na literatura sobre segurança da informação aborda o tema com enfoque na segurança, no aspecto físico e lógico para manter a integridade das informações, como: guardas, usos de crachás, sistemas de portas duplas, controle de acesso biométrico, proteção contra ataques forçados, registros de acessos, autenticação por senhas, bloqueio de múltiplos acessos, backup de segurança, etc. Ferreira (2003).

O presente trabalho objetiva abordar a segurança da informação após as mesmas já terem sido acessadas pelos usuários. Para atingir tal objetivo, foi utilizado o modelo de processo de auditoria proposto por Vieira (2010), que condensa uma série de etapas propostas na literatura. As literaturas abordadas foram sobre auditoria, auditoria da informação, processos de auditorias e modelos processos de existentes na literatura.

Também foi considerada a literatura existente em segurança da informação, mais especificamente nos pilares da SI, pois um dos objetivos é apresentar a aplicação destes pilares nos processos de auditoria.

E conclui com apresentação de um quadro com a aplicação dos pilares da segurança da informação em cada etapa do processo de auditoria da informação.

2 JUSTIFICATIVA

Auditoria da informação é definida por Sharma e Singh (2011), como uma ferramenta que pode ser usada para identificar estrategicamente recursos de informações significantes, tarefas e atividades que geram conhecimento e aquelas que dependem da transferência de conhecimento de uma área para outra no ambiente organizacional. Uma auditoria de informação tem por objetivos analisar a situação atual da informação e ajudar a refletir sobre o melhoramento do seu fluxo dentro da instituição.

Autores como Henczel (2002) e CEDRON-SNI (2006), apresentam técnicas de coletas de dados como: questionários, entrevistas e grupos focais para a realização das etapas da auditoria da informação. E com esse procedimento de coleta de dados para a realização da auditoria, as informações da organização são expostas e muitas vezes os gerentes não se atentam para questões básicas de segurança da informação como confidencialidade, integridade e disponibilidade. E nesse ponto deparamos com o seguinte Problema: **A segurança da Informação é um assunto muito discutido e trabalhado nas organizações, porém a abordagem geralmente se limita a segurança do sistema onde estão inseridas as informações.**

Na década de 90, Hitchings já apresentava a necessidade de um conceito de segurança da informação no qual o aspecto do agente humano tivesse a devida relevância, fosse como usuário das informações ou responsável pelos eventos de segurança.

Percebe-se uma carência de trabalhos publicados em português, sejam livros ou artigos, que tratem de auditoria da informação e da segurança da informação como assuntos complementares. Assim como também observa-se que muitas vezes a segurança se limita a rede e não propriamente a segurança dos conteúdos desconsiderando o fator humano, que é quem de fato acessa as informações em um processo de auditoria da Informação.

Problemas já apresentados por Netto e Silveira (2007), afirmam que a gestão da segurança da informação envolve mais do que gerenciar os recursos de tecnologia - hardware e software envolvem pessoas e processos. E também identificado por Johnson (2012), o qual cita que a matriz de risco quando executada, tem uma

tendência de atender a requisitos de operação de TI, porém não consegue abordar outras áreas que influenciam diretamente a segurança da informação, como “recursos humanos, segurança física, treinamentos, conscientização, etc.”.

A *Information Systems Audit and Control Association* - ISACA, anexo 2, apresenta o Código de Ética Profissional para guiar a conduta pessoal e profissional dos membros da associação e/ou detentores de certificação. No item 4, cita que o profissional deve “Manter a privacidade e a confidencialidade de informações obtidas no curso de suas atividades, exceto quanto à divulgação for solicitada por autoridade legal. Tais informações não devem ser usadas em benefício próprio ou disponibilizadas a terceiros”.

Todos os profissionais devem atentar-se para o cumprimento e a observância dos padrões exercidos em todos os aspectos do trabalho de auditoria. O não atendimento da ética pode resultar em uma investigação de conduta a um determinado membro e/ou detentor de certificação gerando as devidas medidas disciplinares. Esse código de ética profissional elaborado pela ISACA é destinado a todos os auditores de tecnologia da informação, conforme cita Imoniana (2005).

A contribuição pretendida com a realização deste trabalho é aplicar os pilares da segurança da informação nos processos de auditorias da informação e reforçar o que o item 4 do código de ética dos profissionais proposto pelo ISACA descreve. Assim como apresentar os temas de segurança da informação e auditoria da informação como assuntos complementares e importantes nas etapas dos processos de auditoria da informação.

3 OBJETIVOS

Esse trabalho possui um objetivo geral e dois objetivos específicos.

3.1 Objetivo geral

Fornecer referencial teórico que reforce a necessidade da segurança da informação nos processos de auditoria.

3.2 Objetivos Específicos

a) Apresentar um modelo com as etapas dos processos auditoria da informação;

b) Discutir o uso dos princípios básicos da segurança da informação, confidencialidade, integridade, disponibilidade e autenticidade nos processos de auditoria.

4 PROCEDIMENTOS METODOLÓGICOS

Este trabalho caracteriza-se em uma pesquisa exploratória, visto que tem por "finalidade esclarecer e oferecer informações sobre o assunto pesquisado, esclarecendo idéias e conceitos" (GIL, 2009, p. 27).

Também trata-se de uma pesquisa bibliográfica, pois está pautada em livros e artigos científicos nacionais e internacionais que abordaram o assunto de interesse deste trabalho. Para Marconi e Lakatos (1990), a pesquisa bibliográfica propicia o exame de um tema sob novo enfoque ou abordagem chegando a novas conclusões.

Para cumprir os objetivos propostos, foram estudadas inicialmente as seguintes literaturas:

ISACA (*Information Systems Audit and Control Association*), associação internacional que suporta e patrocina o desenvolvimento de metodologias e certificações para o desempenho das atividades de auditorias;

COBIT (*Control Objectives for Information and related Technology*), que apresenta uma série de recursos que podem servir como modelo de referência para gestão da TI, incluindo um sumário executivo, um framework, objetivos de controle, mapas de auditoria, ferramentas para a sua implementação e principalmente, um guia com técnicas de gerenciamento.

A ISO/IEC 27002:2005 conhecida nacionalmente como ABNT NBR ISO IEC 27002:2005, que apresentam vários tipos de métodos como controles, políticas, processos e procedimentos, visando minimizar os riscos aos qual a informação está exposta. Sendo essa a ultima versão do padrão ISO, intitulada "Tecnologia da Informação – Técnicas de Segurança – Código de praticas para Gerenciamento da segurança da Informação", que é uma revisão da ISO/IEC 27001, padrão de certificação em Segurança de Informação.

Posteriormente, foram abordados os assuntos específicos referentes a auditorias, auditoria da informação e segurança da informação, a partir daí apresentada a aplicação dos pilares da segurança da informação nos processos auditorias apresentado no quadro 5 (cinco).

5 REVISÃO DE LITERATURA

A revisão de literatura para melhor compreensão foi dividida em três tópicos que corresponde aos assuntos trabalhados no presente trabalho, os quais apresentam os principais autores que abordaram os temas na literatura nacional e internacional.

a) Abordagem dos conceitos de Auditoria e Auditoria da Informação e apresentação de um modelo.

Para apresentar os conceitos, buscou-se material bibliográfico nas bases de dados nacionais e internacionais, da BRAPCI (Base de dados referencial de artigos de periódicos em ciência da informação), Portal de periódicos da Capes, Bases de Teses e Dissertações, ACM (*Association for Computing Machinery)* e EBSCO *Publishing*. Essa busca foi realizada com termos em português e inglês e considerou as publicações posteriores ao ano de 2000.

Os artigos considerados de grande relevância sobre o assunto são:

- *"La auditoría de La información, componente clave da La gestión estratégica de La informacióm", Cristina Soy I Aumatell (2003);*
- A auditoria da informação: Princípios e Diretrizes. *Hanneri e Botha (2003);*

Outro material utilizado para realização desse trabalho, considerado relevante e merecedor de destaque, foi o trabalho de conclusão de curso (TCC) da Gestora da informação, Andrieli Amaral Vieira (2010), "Auditoria de Informação: Fluxos de Informação e coleta de Dados", o qual apresentou os principais modelos de auditoria da informação presentes na literatura e um modelo baseado nas etapas utilizadas por esses autores. Esse modelo foi utilizado no presente trabalho para a aplicação dos pilares da segurança da informação.

b) Abordagem do conceito Segurança da informação

O assunto segurança da informação é amplamente discutido em artigos e livros, porém para a realização desse trabalho foi necessário uma busca de referências que tratassem do tema não apenas aplicados em sistemas ou na proteção física, mais que abordasse o tema pela perspectiva da proteção da Informação quanto ao comportamento dos usuários que a acessam. Para Johnson (2012), as organizações

já compreendem que a segurança saiu dos limites da tecnologia da informação, atingindo todo o ambiente corporativo.

Os artigos sobre este tema foram buscados nas mesmas bases de dados citadas anteriormente e utilizado o mesmo intervalo temporal como critério de busca.

Para esse tema também foi adotado a pesquisa em livros, que possuem uma abordagem mais abrangente. Destacando-se o livro: DAMA - DMBOK (*Data Management Body of Knowledge*), que serve como guia para estabelecer e designar responsabilidades de Gestão de Dados, mais especificamente o capitulo 7 que é o Guia pra a Gestão de Segurança de Dados.

O DMBOK proporciona uma visão geral sobre gerenciamento de dados, visão padrão da indústria no que concerne a função de gerenciamento de dados, a terminologia e as melhores práticas, sem detalhar os métodos e técnicas específicas. O DMBOK não fornece como a última palavra sobre alguma função específica em gerenciamento de dados ele aponta aos leitores onde obter publicações amplamente reconhecidas, artigos e sites para leitura complementar. O DMBOK introduz pontos de vista alternativos e opiniões aceitas pela indústria, onde abordagens de diferenças de opinião possam existir.

c) Uso da Segurança da Informação em Processos de Auditorias da Informação

Após a pesquisa de literatura dos temas apresentados anteriormente, foram pesquisadas bibliografias que tratam da vulnerabilidade e exposição das Informações durante os processos de auditoria da informação, bem como trabalhos que abordam a aplicabilidade dos pilares da segurança da informação, que é o objetivo principal deste trabalho.

Entre outros Materiais consultados considera-se os mais importantes:

1. *Practical Information Polices: How to Manage Information Flow in Organizations de Elizabeth Orna (1990)*. Livro citado em vários artigos utilizados.
2. A dissertação de mestrado de Luciano Johnson, defendida no ano de 2012, que apresenta uma estrutura de análise de maturidade dos processos de segurança da informação, com base na Norma ABNT NBR ISO/IEC 27002:2005.

5.1 DEFINIÇÃO DE AUDITORIA

Quando o assunto é auditoria, automaticamente há uma associação com a contabilidade, pois é um termo muito mais utilizado por profissionais da área contábil. Entretanto, conforme Botha e Boon (2004), é possível encontrar no mundo comercial diferentes tipos de auditorias, como a Auditoria da Comunicação, Auditoria Financeira, Auditoria Técnica, Auditoria da Informação, etc. Cada auditoria possui suas finalidades próprias e deve atender normas e regras especificas de cada organização.

A auditoria possui como objetivo principal diagnosticar, descobrir e verificar recursos da organização. Também pode ser considerada um mecanismo de controle, assim como apresentar a realidade da organização e confrontar com os padrões que a organização havia pré-estabelecido e então apontar possíveis soluções para eventuais divergências identificadas.

> A função de Auditor deve ser exercida em caráter de entendimento de que o trabalho executado tenha e mereça toda a credibilidade possível, não sendo permissível que paire qualquer sombra de dúvida quanto à integridade, honestidade e aos padrões morais desse profissional. (NORMAS E TÉCNICAS DE AUDITORIA I, 2012, p. 19).

Os processos de auditorias podem ser realizados por profissionais internos a organização ou por uma equipe externa, conforme quadro 1, sendo a primeira visando o cumprimento dos controles internos e a segunda para mostrar se a empresa cumpre as obrigações e normas de forma transparente.

Auditoria interna	Auditoria externa
Realizada por um auditor que fica constantemente na empresa, possui vínculo empregatício e, normalmente, trabalha junto à diretoria executiva.	O auditor externo trabalha de forma independente, sem vínculo empregatício com a empresa.

QUADRO 1 - Diferenças de auditoria interna e externa
Fonte – Técnicas de auditoria I, 2012 – Adaptado.

5.2 AUDITORIA DA INFORMAÇÃO

Para Henczel (2000), a auditoria da informação tem por objetivos analisar a situação atual da informação e ajudar a refletir sobre o melhoramento do seu fluxo dentro da organização. Uma auditoria de informação focaliza os recursos, os usuários e as suas necessidades de informação. O objetivo de uma auditoria da Informação deve ser o de ajudar a organização a contar com a informação correta, no tempo certo, para a pessoa certa e por um custo justo. Aumatell (2003), destaca que a importância de incorporar a prática de auditoria de informações como um padrão na gestão estratégica de ativos e funções informativas e serviços de informação de qualquer organização.

A maioria das organizações, recebem, processam, armazenam e produzem também muitas informações, citado por Dante (1998), de o “ciclo da Informação” e isto não mudará no futuro próximo, ao contrário, tende a crescer cada vez mais com a utilização contínua da Internet e das redes digitais internas e externas .

Uma auditoria de informação traz grandes benefícios, pois diagnostica e identifica os pontos fortes e fracos sobre como a informação flui dentro da organização. Ao mesmo tempo, ela auxilia no foco e na atenção da equipe quanto ao valor e aos benefícios do uso e da partilha da informação, CEDRON SNI (2006).

As etapas do processo de auditoria da informação abordado por Vieira (2010), por meio de comparação das etapas do processo de auditoria da informação presentes na literatura, já estudadas por vários autores, são apresentadas no anexo A. Entre eles Henczel (2000), Bootha e Boon (2003), Crockett e Foster (2004), CEDROM-SNI (2006) Jones (2009).

A partir da comparação das etapas a autora apresentou as diversas etapas da auditoria da informação por meio de um ciclo (figura 1), e considerou os demais processos de auditoria, desta forma não se limitando somente a auditoria da informação, ressaltando a necessidade de se considerar as demais auditorias como um processo continuo, visando sempre à melhoria dos processos em questão.

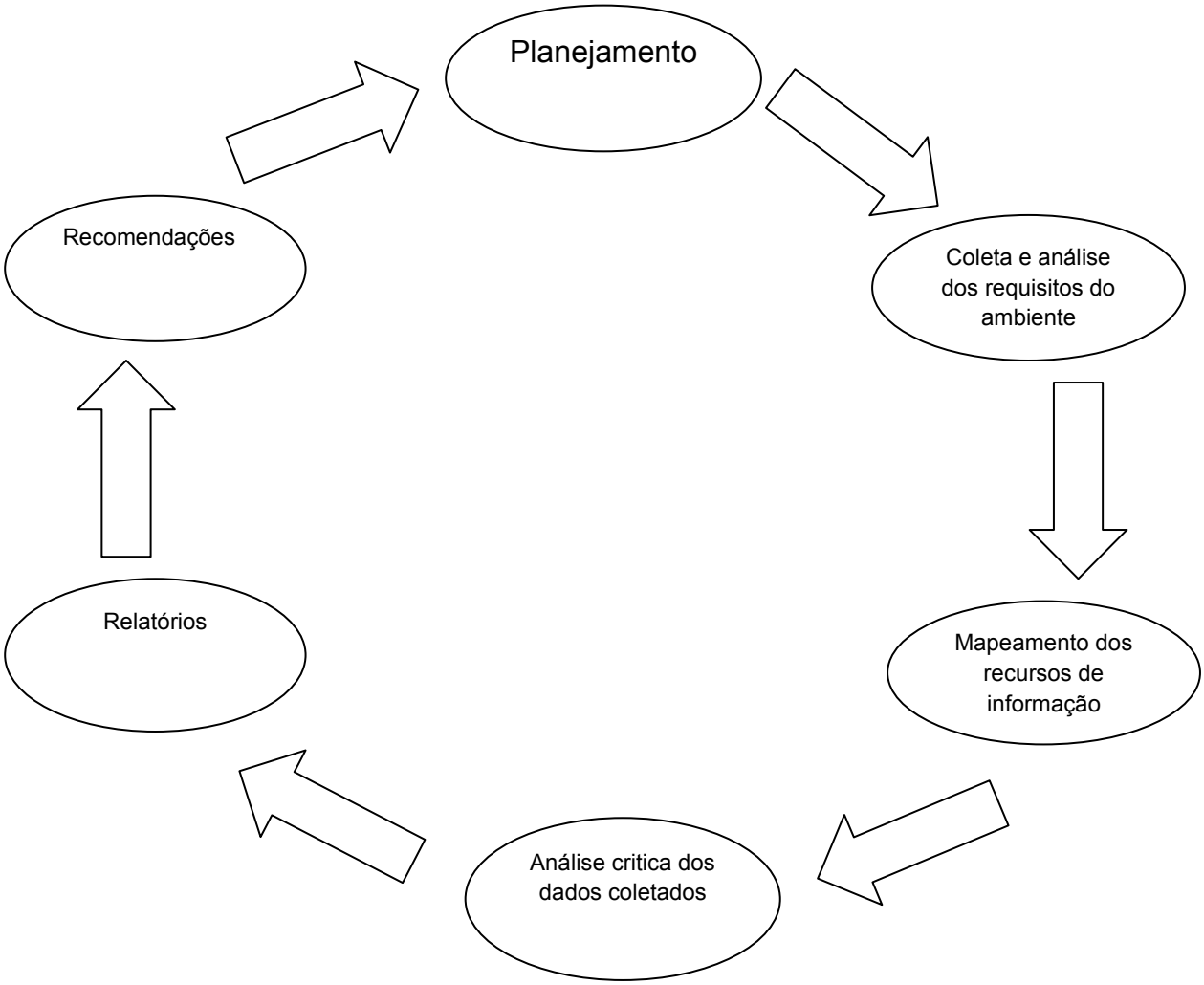

Figura 1 - Ciclo etapas de auditoria
Fonte: Vieira, 2010

O ciclo inicia com a etapa de “planejamento”, tem como finalidade apresentar um plano de como a auditoria deverá ser executada, desde aspectos relacionados à compreensão e revisão de práticas destinadas aos fluxos de informação, aspectos de custos e tempo para execução, definição do método para a ação, todos visando minimizar os erros e problemas durante a execução da auditoria da Informação.

A segunda etapa é a “Coleta e análise das necessidades do ambiente”, a qual deve fornecer todas as informações pelas quais será possível conhecer a organização ou o setor que deseja atuar, Vieira (2010), considera essa etapa crucial para o andamento das demais, pois ela aponta os possíveis problemas existentes na organização.

A próxima etapa apresentada é o “Mapeamento dos recursos de informação”, essa etapa objetiva fornecer um inventário dos recursos de informação, onde é

possível verificar sua utilização de acordo com as necessidades identificadas, assim como os padrões adotados pela organização.

A etapa “Análise crítica dos dados coletados”, tem como intenção final avaliar os requisitos coletados, comparando com os recursos informacionais já existentes e a partir daí apresentar soluções que se façam necessários para preencher as lacunas existentes.

Na penúltima etapa “Relatório”, deve ser apresentado todas as não conformidades encontradas, assim como a soluções passiveis de execução para empresa em questão. Também é nesta etapa que se decide a forma de ser entregue e/ou apresentar a auditoria e quem terá acesso a mesma.

Por fim a etapa “Recomendações”, apresentado no ciclo das etapas de auditoria por Vieira (2010), pelo fato de ser estudado por Henczel e CEDROM- SNI (2006). Essa etapa sugere possíveis medidas para a resolução dos problemas apontados na etapa relatório, e pretende sugerir um roteiro de sugestões e modificações, para ser apresentado e aceito pelo proprietário da informação, essas recomendações devem ser elaborados pensando nos “problemas” apresentados.

5.3 SEGURANÇA DA INFORMAÇÃO

Segurança da informação segundo Beal (2005), é o processo de proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade. Sêmola (2003), define segurança da informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.

A ABNT NBR ISO/IEC 27002:2005, em sua seção introdutória, define segurança da informação como “a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”. Assim, podemos definir segurança da informação como a área do conhecimento que visa à proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade e autenticidade, a fim de garantir a continuidade do negócio e minimizar os riscos, Figura 2.

Atualmente o conceito de segurança da informação está padronizado pela norma ISO/IEC 27002:2005, influenciada pelo padrão inglês (*British Standard*) BS 7799. A série de normas ISO/IEC 27000, foram reservadas para tratar de padrões de segurança da informação, incluindo a complementação ao trabalho original do padrão inglês. A ISO/IEC 27002:2005 continua sendo considerada formalmente como 17799:2005 para fins históricos.

PILARES DA SEGURANÇA DA INFORMAÇÃO

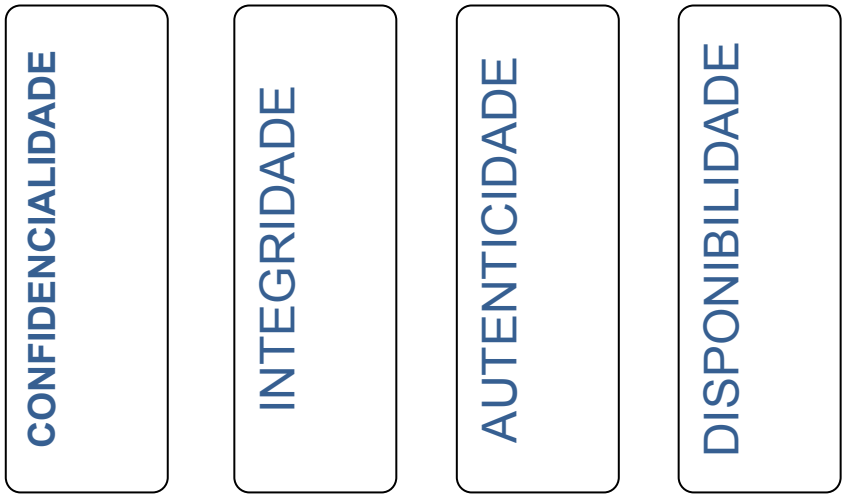

Figura 2 – Pilares da Segurança da Informação
Fonte: ABNT NBR ISO/IEC 27001:2006

5.3.1 Confidencialidade

Para Beal (2005), a confidencialidade é a garantia de que o acesso à informação é restrito aos seus usuários legítimos, ou seja, quando uma informação representa uma vantagem de mercado, um diferencial competitivo, diz-se que a informação possui um valor de restrição, a ser mantido por meio de preservação de sua confidencialidade. No âmbito da administração pública federal, o decreto nº 4.553/2002 classifica os documentos públicos em 4 categorias sendo um deles de confidencias, que são aqueles que, no interesse do Poder Executivo e das partes, devem ser de conhecimento restrito, e cuja revelação não autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do estado.

Segundo Ferreira (2003), a informação dever ser protegida, independente da mídia que a mesma esteja contida, como por exemplo, documentos impressos ou mídia digital. Que além de cuidar da informação como uma todo também deve-se

preocupar com a proteção de partes de informação que podem ser utilizadas para interferir sobre o todo.

Beal (2005), apresenta um exemplo de classificação da informação quanto aos requisitos de confidencialidade mostrado no quadro 2.

Tipo	**Características**
Confidencial	A divulgação para pessoas não autorizadas pode causar danos graves à organização
Reservada	Informação que no interesse da organização devam ser de conhecimento restrito e cuja revelação não autorizada pode frustrar o alcance de objetivos e metas
Pública	Informações de acesso livre

QUADRO 2 - Classificação da confidencialidade da informação.
Fonte: Beal, 2005 - Adaptado.

5.3.2 Integridade

Garantia da criação legítima e da consistência da informação ao longo do seu ciclo de vida: em especial, prevenção contra criação, alteração ou destruição não autorizada de dados e informações. A integridade consiste em proteger a informação contra modificação sem a permissão explícita do proprietário. “Proprietário da informação é o executivo de negócio ou gerente de uma determinada área responsável pelos ativos da informação da organização.” (Ferreira, 2003, pg. 25). Dados e informações perdem sua integridade em tentativas de fraudes, quanto maior for o impacto para a organização da perda de integridade de uma informação, maior o investimento a ser feito em controles para prevenir, detectar e corrigir a produção errada ou a alteração indevida de informações. (Beal, 2005, pg. 67).

A integridade pode ser definida como de: alta exigência de integridade, que é a criação com erro ou alteração indevida e assim comprometer as operações e

objetivos da organização, acarretando em descumprimentos de leis, prazos e normas, levando a mesma ter prejuízos; de média exigência de integridade, onde a criação com erro ou alteração indevida das informações não compromete as operações nem traz impactos muitos grandes, apenas pode causar algum tipo de prejuízo; e de baixa exigência de integridade é a criação com erro ou indevida, que é facilmente detectada e os riscos que oferece são praticamente desprezíveis.

5.3.3 Autenticidade

Para Ferreira (2003), o serviço de autenticação em um sistema deve assegurar ao usuário que recebe a informação, que a mensagem é realmente procedente da origem informada em seu conteúdo. A verificação da autenticidade faz-se necessário após todo processo de identificação, seja do sistema para o usuário, do usuário para o sistema ou do sistema para outro sistema.

O objetivo da autenticidade é englobado pelo de integridade, quando se assume que este visa garantir não só que as informações permaneçam completas e precisas, mais também que a informação capturada do ambiente externo tenha sua fidedignidade verificada e que a criada internamente seja produzida apenas por pessoas autorizadas e atribuída unicamente ao seu autor legítimo.

A implementação para o processo de autenticidade geralmente é implementado a partir de mecanismos de senhas e assinaturas digitais.

Beal (2005), cita que a segmentação dos ativos por característica como: tipo de usuário, tipo de aplicação, ambiente de uso etc., permite a criação de estratégias diferenciadas de armazenamentos, controle de acesso, controles e recuperação de serviços, assim aplica os controles adequados conforme o nível de proteção requerido por cada segmentação.

5.3.4 Disponibilidade

Garantia de que a informação e os ativos associados estejam disponíveis para os usuários legítimos de forma oportuna. Beal (2005), apresenta como objetivo da disponibilidade, o controle de acesso que permite identificar os usuários legítimos da informação para então liberar o acesso solicitado. Quando analisado a

disponibilidade é considera-se questões como: “quanto custa para produzir”, “quanto custa para recuperar” e quais consequências gera para a organização se a informação não está mais disponível. Conclui-se que a falta de informações pode afetar a organização e o que deve ser considerado é quanto tempo levaria para superar esse impacto. Desta forma a classificação das informações e a ordem de prioridade de recuperação em caso de indisponibilidade são muito importantes e a organização deve atribuir a cada categoria as informações conforme o grau de importância do ativo para a organização. Essa ordem de importância é expressa por Beal (2005), começando pelas mais importantes categoria 1 e menos importantes categoria 6, conforme quadro 3.

Ordem	Tempo de recuperação
Categoria 1	Devem ser recuperadas dentro de ‘x’ minutos
Categoria 2	Devem ser recuperado dentro de ‘y’ horas
Categoria 3	Devem ser recuperadas dentro de ‘z’ dias
Categoria 4	Devem ser recuperadas dentro de ‘n’ semanas
Categoria 5	A importância do tempo de recuperação varia de acordo com o período (tempo) e para que o sistema seja utilizado.
Categoria 6	Aplicações não críticas.

QUADRO 3 – Categorias e tempo para Disponibilidade.
Fonte: Beal (2005).

Considera-se que pode abranger as categorias 1 e 2 informações que exigem recuperação em um curto espaço de tempo, as quais mesmo indisponíveis em um curto período podem causar prejuízos inaceitáveis. Nas categorias 2, 3 e 4 cabe informações com exigência de recuperação em médio espaço de tempo, sendo que as indisponibilidades temporárias não afetam o desempenho dos processos críticos, porém que ao longo período de tempo pode causar atrasos ou decisões erradas. Categoria 5 o tempo de recuperação depende do tipo de informações, é aceitável a indisponibilidade variada. E a categoria 6 não possui exigência de tempo para recuperação, pois a perda ou indisponibilidade por períodos longos não traz consequências negativas consideráveis, seja pela pouca relevância da informação ou pela facilidade de recuperação da mesma.

6 APLICAÇÃO DOS PRINCIPIOS BÁSICOS DA SEGURANÇA DA INFORMAÇÃO NOS PROCESSOS DE AUDITORIA

A gestão de dados é o planejamento, desenvolvimento e execução de políticas e procedimentos de segurança para proporcionar a devida autenticação, autorização e acesso nos ativos de dados e informações (Seções da ISO IEC 27002). Seu objetivo é proteger os ativos de Informação em alinhamento com as regulamentações de privacidade e confidencialidade e requisitos do negócio. Em uma organização existem muitas fontes de informações que não ficam à disposição da gerência para tomadas de decisões, fazendo-se necessário a aplicação dos processos de auditorias da Informação, e para ORNA (1990) entre essas fontes estão:

- Registros de clientes;
- Informação sobre fornecedores;
- Informações sobre orçamentos operacionais;
- Resultados financeiros;
- Relatórios de operações externas;
- Informação dos concorrentes: como eles estão fazendo financeiramente, o que eles estão produzindo;
- A informação que a própria empresa produz, para o mundo exterior, e para o público interno;
- Informações sobre seu mercado, seu público-alvo ou de seus clientes;
- Informações sobre áreas de importância, por exemplo: a produção ou indústria de serviço que pertence o sistema de educação, ciência e tecnologia; processos, materiais, instalações ou equipamentos;
- Informações sobre o ambiente em que opera: a economia, regulamentos comunitários governamentais, legislação, etc.

E é justamente por existir muitas fontes de informações que a organização deve atentar-se para a sua segurança, pois há uma exposição maior quando é realizado um processo de auditoria da informação.

Para o Guia DAMA-DMBOK (2012), gestão de qualidades de dados é sinônimo de qualidade da informação e considera que a falta de qualidade nos dados resulta em informação imprecisa e um desempenho fraco de negócio. Desta

forma faz-se necessário ter qualidade para prover uma solução econômica e melhorar a qualidade e integridade dos dados.

Para a efetiva realização da segurança da informação na organização, são utilizados vários métodos como controles, políticas, processos e procedimentos, geralmente definidos por uma política de segurança da Informação Baars *et al*.,(2009).

Atualmente as organizações entendem que segurança não está mais apenas nos limites da tecnologia, mais atinge todo o ambiente corporativo, principalmente o fator humano. E as organizações muitas vezes por insegurança em expor as informações existentes, dificultam a realização das auditorias, conforme aponta Orna no livro "*Practical Information Polices*" (1990), muitas empresas desnecessariamente dificultam seu trabalho, não deixando que informações externas sejam mostradas internamente e vice versa.

Johnson (2012), em sua pesquisa apresenta as iniciativas de segurança da informação presente nas organizações e o nível de maturidade dos mesmos, baseado no modelo de maturidade genérico proposto pelo Capability Maturity Model Integration (CMMI) e as atividades definidas para cada processo.

Os processos de segurança da informação foram apresentados em cinco categorias inspirados no Cobit (ITGI, 2008), Planejamento, Organização e Alinhamento (POA), Segurança Organizacional (ORG), Segurança Física (FIS), Segurança Técnica (TEC) e Gestão de Segurança (GES).

Para cada modelo de maturidade de processo, o autor desenvolveu um questionário de avaliação. Cada questionário continha questões que foram divididas em cinco níveis, representando os níveis de maturidade do processo.

Cada questão com quatro alternativas de respostas, que representam os níveis em que as atividades de segurança do processo são aplicadas na organização. Seguiu a norma ABNT NBR ISO/IEC 27002:2005 que tem como característica ser aplicada em todas as áreas da organização. Essa características que inspirou Johnson (2012), na definição das 4 (quatros) alternativas de respostas do questionário, sendo elas: a) Somente em algumas situações; b) em toda a tecnologia da informação da organização; c) em vários departamentos da organização, inclusive TI; e d) em toda a organização.

No presente trabalho será abordado apenas uma categoria, o ORGS, que trata da segurança da informação visando atender os requisitos internos a organização.

O processo ORGS (Segurança Organizacional), é referente aos processos que visam à segurança da informação sob a ótica da organização como empresa. Esses processos objetivam organizar as ações de segurança da informação, relacionando os requisitos internos da organização com as práticas de segurança da informação. Nesse processo foi avaliado o nível de maturidade de cada processo de segurança da informação, foi dividido em 8 subcategorias, conforme mostra o quadro 4, que apresenta também a média de maturidade de cada processo.

A média foi calculada somando os valores individuais do processo para cada respondente e dividido pela quantidade de respondentes, no caso da respectiva pesquisa foram 10 (dez) empresas.

Foram utilizados os dados desta pesquisa para apoiar os resultados do presente trabalho, visto que estes resultados apoiam a preocupação com a segurança da Informação e ao mesmo tempo se relacionam com a área de TI.

E pelo estudo é possível verificar que a responsabilidade referente à segurança da informação ainda é um assunto que recaí sobre a TI da organização.

ORG – Segurança Organizacional	Média de Maturidade
Responsabilidades pelos ativos	**1,2**
• Inventario dos ativos • Proprietário dos ativos • Uso aceitável dos ativos	
Classificação da Informação	**1,5**
• Recomendações para classificação • Rótulos e tratamento da Informação	
Segurança em recursos humanos	**1,6**
• Papéis e Responsabilidades • Seleção • Termos e condição de contratação • Responsabilidades da direção • Conscientização, educação e treinamento em Segurança da Informação • Processo Disciplinar • Encerramento das atividades • Devolução dos ativos • Retirada de direito de acesso	
Procedimentos e Responsabilidades Operacionais	**1,8**
• Documentação dos procedimentos de Operação • Gestão de mudanças • Segregação de Funções • Separação dos recursos de desenvolvimento, teste e de produção	
Troca de Informação;	**1,6**
• Políticas e procedimentos para troca de Informações • Acordos para troca de Informações • Mídias em trânsito • Mensagens eletrônicas • Sistemas de Informação do Negócio	
Requisitos de Negócios para controle de acesso;	**2,1**
• Política de Controle de Acesso	
Responsabilidades dos Usuários;	**2,6**
• Uso de senhas • Equipamentos de usuários Monitorados • Política de mesa limpa e tela limpa	
Requisitos de Segurança de Sistemas de Informação	**1,8**
• Análise e especificação dos requisitos de Segurança	

QUADRO 4 - Processos e média maturidade
Fonte: Johnson, 2012 – Adaptado.

No quadro 5, são apresentados as etapas dos processos de auditoria e a aplicação dos princípios básicos de segurança da informação, segundo os padrões internacionais ABNT(2005).

Considera-se que se faz necessário a aplicação de todos os pilares de segurança da informação em todas as etapas de auditoria, entretanto alguns são mais “aplicáveis”, ou seja, são extremamente indispensáveis para manter a informação segura. Dessa forma as aplicações ficaram das seguintes formas:

Na etapa de Planejamento, os pilares: Integridade, confidencialidade e autenticidade são consideradas os mais aplicáveis, pois nessa etapa já se tem um mínimo de conhecimento sobre os ativos existentes na organização. "Ativo é qualquer coisa que tenha valor para a organização." (ABNT NBR ISO/IEC 27001:2006, pg. 08).

Na segunda etapa “Coleta e análise das necessidades do ambiente” são aplicados: Integridade, confidencialidade e autenticidade. Sendo que nessa etapa todas as informações da organização serão acessadas pelos envolvidos das auditorias. Para Espírito Santo (2010), a definição de uma política de confidencialidade ou código de ética entre trabalhadores e organização deve ser realizada em conjunto com os recursos humanos.

Na etapa “Mapeamento dos recursos de informação”, também se considera os requisitos integridade, confidencialidade e autenticidade, sendo que nessa etapa será realizado a identificação e classificação dos ativos, fazendo-se necessário os citados para a segurança das Informações.

Já na etapa de “Análise crítica dos dados coletados” aplica-se os princípios de confidencialidade e autenticidade, devido a necessidade de analisar o plano existente, os recursos, o custo beneficio e identificar o problema existente, para então apresentar uma possível solução.

Nas etapas de Relatórios e Recomendações aplicam-se todos os pilares de segurança da informação abordados, pois nessas etapas será apresentada a compilação do trabalho e sugestões para os problemas identificados.

Todas as informações presentes nestas etapas devem possuir os atributos dos pilares de segurança da informação para que se considere uma auditoria da informação, que utilizou apenas informações existentes na organização e obteve os resultados sem interferências externas.

Para aplicar os pilares da segurança da informação nos processos de auditoria faz-se necessário estabelecer diretrizes, mecanismos de segurança, políticas e procedimentos específicos que atendam as etapas do processo de

auditoria, desta forma, dando condições para a efetiva aplicação dos conceitos que devem ser seguidos pelos participantes envolvidos.

Segundo Espírito Santo (2010), uma solução completa abrange a rede interna e deve ser composta de: “Uma Política de Segurança Corporativa com definição clara das diretrizes, normas, padrões e procedimentos que devem ser seguidos por todos os usuários envolvidos na auditoria da informação”.

Há também a necessidade de analisar cada organização e definir se a auditoria da informação deve ser realizada por uma equipe interna ou externa, e então adaptar a política de modo que atenda a problemas de segurança internos, e atenda a cultura seguida por cada organização. Para Espírito Santo (2010), o modelo atual para segurança de redes tem assumido que o inimigo está do lado de fora da empresa enquanto que dentro, todos são confiáveis, porém, sabe-se que a maior parte dos problemas ocorre em função de ameaças internas.

Etapas processos Auditorias	**Pilares Segurança da Informação**			
	Integridade	Disponibilidade	Confidencialidade	Autenticidade
Planejamento	X		X	X
Coleta e análise das necessidades do ambiente	X		X	X
Mapeamento dos recursos de informação	X		X	X
Análise crítica dos dados coletados			X	X
Relatório	X	X	X	X
Recomendações	X	X	X	X

QUADRO 5 - Aplicabilidade Pilares SI em processos Auditorias da Informação
Fonte: Autora

A escolha da aplicação dos princípios básicos, confidencialidade, integridade, autenticidade e disponibilidade conforme mostra no quadro 5, é embasado em Ferreira (2003), que define que esses pilares são essenciais para preservar a competitividade, o faturamento, a lucratividade, o atendimento aos requisitos legais e a imagem da organização.

Os controles de segurança de dados em sistemas de informações são referentes à proteção da informação, evitando atos de destruição intencionais, ou mesmo não intencionais e outros referentes à manipulação, divulgação de informações sigilosas, e esses atos segundo Imoniana (2005), não devem ser desprezados, pois podem causar efeitos devastadores na organização.

O requisito integridade não foi considerado em análise critica dos dados, pois nessa etapa será apenas analisado o plano existente, comparando com as necessidades, análises dos recursos existentes, identificação do problema existente e análise do custo beneficio Vieira (2010). Assim como se considera que o princípio de disponibilidade não se aplica nas etapas de planejamento, Coleta e analise das necessidades do ambiente, mapeamento dos recursos de informação e análise crítica dos dados coletados, pois baseados nas características apresentadas por Vieira (2010), nessas etapas as informações serão realizadas apenas as análises das informações já existentes e as mesmas estão à disposição da organização.

7 CONSIDERAÇÕES FINAIS

Com este trabalho buscou-se apresentar a necessidade de aplicação dos pilares de Segurança da Informação (Integridade, confidencialidade, disponibilidade e autenticidade), nos processos de auditorias da Informação. Considerando que as informações são totalmente expostas nos processos de auditoria e mesmo que os profissionais respeitem o código de ética proposto pelo ISACA as mesmas ficam mais vulneráveis a serem violadas ou então disponibilizadas inadequadamente, comprometendo os ativos existentes na organização.

Para a realização do presente trabalho foi dividido em objetivo geral e objetivos específicos, objetivos estes que para serem alcançados foi necessário abordar os temas, Auditoria da Informação e Segurança da Informação separadamente para então apresentar a aplicabilidade dos pilares da segurança da informação nos processos de auditorias. Foi utilizado um modelo de processos auditoria da informação apresentado em trabalho anterior, modelo esse que foi criado a partir de outros modelos existentes na literatura.

Na área de segurança da informação foi apresentado o estudo de Johnson (2012), que contribuiu para o entendimento da maturidade dos processos de segurança da informação nas organizações e as normas ABNT.

A partir do estudo de literaturas dos temas, foi possível apresentar no quadro 5, a aplicabilidade dos pilares da segurança da informação nos processos de auditoria da informação e descrever a necessidade de cada pilar nas etapas do processo.

Deve-se destacar que os processos de auditoria não foram mostrados em quadros separados, visto que é um tema já abordado anteriormente e está disponível para consulta. Assim como os demais processos de maturidade estudados por Johnson também não foram detalhados, visto que não havia contribuição significativa para o resultado do presente trabalho e também está disponível para consulta.

Conclui-se que a auditoria da informação faz-se cada vez mais presente nas organizações, contribuindo para manter transações com clientes, fornecedores e colaboradores; o monitoramento dos ativos da empresa e suas finanças; a avaliação de concorrentes, sobre o uso assertivos dos ativos da empresa para seu desenvolvimento e crescimento no mercado atuante.

Porém, a segurança da informação faz-se necessária não apenas na área de tecnologia da organização, mais em cada processo realizado e em cada departamento, evitando que as informações acessadas acabem sendo violadas ou disponibilizadas indevidamente.

E nos processos de auditoria da informação a aplicação dos pilares da segurança da informação é possível através de políticas da segurança da informação, que tem a finalidade de fornecer orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

A contribuição desse trabalho é apresentação de um referencial teórico com o tema segurança da informação e auditoria da informação se complementando. São temas presentes na literatura internacional, porém carentes na nacional, principalmente em relação à auditoria da informação.

Salientamos que referencias do tema segurança da informação aplicados em processos de auditorias da informação não foram encontrados nas bases pesquisadas.

Sugere-se para um trabalho futuro a aplicação desses pilares apresentados em um processo de auditoria da informação em uma organização. Pois certamente é um ramo de atividade do gestor da informação, que estará presente nas atividades dos profissionais e ambos os temas auditorias da informação e segurança da informação são assuntos que estão cada vez mais presentes e fazem-se necessários nas organizações.

REFERENCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2005** Tecnologia da informação – código de prática para gestão da Segurança da Informação. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001**: Tecnologia da informação – Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos. Rio de Janeiro, 2006.

AUMATELL, S. I. Cristina. La auditoría de la información, componente clave de la gestión estratégica de la información. En: **El profesional de la información**, 2003, jul.-agosto, v.12,n.4 pp.261-268.

BAARS, H.; HINTZBERGEN, K.; HINTZBERGEN, J.; SMULDERS, A. **The Basis of information Security – A Pratical Handbook**. Newton Translations, the Netherlands, 2009.

BEAL, Adriana. **Segurança da Informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações – São Paulo: Atlas, 2005.

BOTHA, H.; BOON, J. A. The information audit: principles and guidelines. **Libri,** Pretoria, v. 53, p. 23-38, 2003.

CEDROM –SNI. **The strategic information audit: a powerful tool to prevent chaos**. 2006. 21 slides, color. Disponível em: <http://www.cedrom-sni.qc.ca/default.asp?menu=Accueil>. Acesso em: 07 dez. 2012.

CROCKETT, M,; FOSTER,J. Using ISO 15489 as an audit tool. **The information Management Journal**, p. 46-53, 2004.

DANTE, G. P. **Gestión de Información em las organizaciones**: princípios, conceptos y aplicaciones. Santiago. 1998.

ESPIRITO SANTO, A. F. S. **Segurança da Informação**. Disponível em: < http://www.ice.edu.br/TNX/encontrocomputacao/artigos-internos/aluno_adrielle_fernanda_seguranca_da_informacao.pdf>. Acesso em 21/01/2013.

FERREIRA, Fernando N. F. **Segurança da informação**. Rio de Janeiro: Ciência Moderna, 2003. p.161.

FERREIRA, Fernando N. F. ARAUJO, M.T. **Política de segurança da informação**: Guia prático para Elaboração e Implementação. 2.ed. Rio de Janeiro: Ciência Moderna, 2006. p.177.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2009.

HENCZEL, S. The information audit as a first step towards effective knowledge management: an opportunity for special librarians. **INSPEL**, Potsdam, v. 34, n.3/4, p.210 -226, 2000.

HITCHINGS, J. Deficiencies of the traditional approach to information security and the requirements for a new methodology. **Computers & Security**, v. 14, n. 5, p. 377–383, Maio 1995.

IMONIANA, J. O. **Auditoria de Sistemas de Informação**. São Paulo: Atlas, 2005. p.197.

ITGI – Information Technology Governance Institute. **COBIT 4.1**. Rolling Meadows, 2008.

JOHNSON, L. **Proposta de uma estrutura de análise de maturidade dos processos de Segurança da informação com base na norma ABNT NBR ISO/IEC 27002:2005**. 55 f. Dissertação (Mestrado em Gestão e Tecnologia da Informação) – Setor Ciências Sociais Aplicados, Universidade Federal do Paraná, Curitiba, 2012.

JONES, S.; ROSS, S.; RUUSALEPP, R. **Data Audit Framework Methodology: draft for discussion**. Version 1.8. Glasgow, May 2009. Disponível em: <http://www.data-audit.eu/DAF_Methodology.pdf.>Acesso em; 07 jan, 2013.

MARCONI, M.,A.; LAKATOS,E. M. **Técnicas de pesquisa**: **planejamento e execução de pesquisas, amostragens e técnicas de pesquisa, elaboração, análise e interpretação de dados**. São Paulo: Atlas, 2007.

MOSLEY, M.(Org.); BRACKETT, M.(Org.); EARLEY, S.(Org.). **Guia da DAMA para o corpo de conhecimento em gestão de dados DAMA-DMBOK**. Primeira Edição. Technics Publications. U.S.A. 2012.

NETTO, A. da S.; SILVEIRA, M. A. P. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. **Revista de Gestão da Tecnologia e Sistemas de Informação**. Vol. 4, No. 3, 2007, p. 375-397.

Controle Interno e Auditoria Governamental: Controladoria-Geral do Estado – CGE. Curso Básico de Controle Interno e Auditoria Governamental. Minas Gerais, 2012.

ORNA, E. **Practical Information Polices – How to manage information flow in organizations**. Gower. 1990.

SCHNEIER, Bruce. **Segurança.com: segredos e mentiras sobre a proteção na vida digital** – Rio de Janeiro: Campus, 2001.

SÊMOLA, Marcos. Gestão **da Segurança da Informação: uma visão executiva** – Rio de Janeiro: Campus, 2003.

SHARMA C. K.; SINGH, A. K. An evaluative study of information audit and knowledge management audit. **Brazilian Journal of Information Science**, Marília, v.5, n.1, p.53-59, Jan./Jun. 2011. Disponível em:<http://www.brapci.ufpr.br/documento.php?dd0=0000011692&dd1=446a4>. Acesso em: 09 de jun. 2012.

VIEIRA, A. A. **Auditoria de Informação:** Fluxos de Informação e coleta de dados. 49 f. Trabalho de graduação (Bacharel em Gestão da Informação) – Setor Ciências Sociais Aplicadas, Universidade Federal do Paraná, Curitiba, 2010.

ANEXOS

Anexo A: Quadro comparativo das etapas do processo de Auditoria de Informação

Henczel (2003)	**Botha e Boon (2003)**	**Crockett e Foster (2004)**	**CEDROM SNI (2006)**	**Jones (2009)**	**Vieira (2010) (Resultado)**
Planejamento	Planejamento	Definição do escopo do projeto	Revisão da estrutura organizacional	Planejar a auditoria	**Planejamento**
			Revisão dos processos de Gestão da Informação		
		Preparação			
Coleta de dados	Avaliação das necessidades de Informação	Coleta de dados	Identificação das necessidades estratégicas		**Coleta e análise dos requisitos do ambiente**
	Inventário de Informações			Identificar e classificar os ativos de dados	**Mapear recursos de Informação**
	Determinação de custo e valor da Informação				
Análise dos dados	Análise				
Avaliação dos dados			Análise das lacunas do planejamento das metas anteriores	Avaliar a gestão dos ativos de dados	**Análise crítica dos dados coletados**
Comunicação das recomendações	Relatório	Relatório escrito	Apresentar relatório e recomendações à organização	Relatar resultados e recomendar mudanças	**Relatório**
Implementação das recomendações			Implementação das Recomendações		**Recomendações**
Continuidade do processo					

Fonte: VIEIRA, 2010.

Anexo B - Código de ética profissional (ISACA)

A Information Systems Audit and Control Association, Inc. (ISACA) apresenta esse Código de Ética Profissional para guiar a conduta pessoal e profissional dos membros da associação e/ou detentores de certificação.

Membros e detentores de certificações da ISACA devem:

Item 1 Apoiar a implementação de, e encorajar a aderência aos modelos, procedimentos e controles para os sistemas de informação.

Item 2 Desempenhar suas atividades com objetividade, dedicação e profissionalismo, de acordo com modelos profissionais e as melhores práticas.

Item 3 Servir aos interesses dos acionistas de forma honesta e legal, mantendo altos padrões de conduta e caráter e não se relacionando em atos desonrosos à profissão.

Item 4 Manter a privacidade e a confidencialidade de informações obtidas no curso de suas atividades, exceto quanto à divulgação for solicitada por autoridade legal. Tais informações não devem ser usadas em benefício próprio ou disponibilizadas a terceiros.

Item 5 Manter competência em seu respectivo campo de atuação e concordar em atuar apenas com as atividades onde tenha razoável expectativa de conclusão com competência profissional.

Item 6 Informar às partes competentes dos resultados obtidos no trabalho, revelando todos os fatos significativos.

Item 7 Apoiar a educação profissional dos acionistas no aumento de sua compreensão dos controles e segurança dos sistemas de informação.

O não atendimento a esse Código de Ética Profissional pode resultar em uma investigação de conduta a um determinado membro e/ou detentor de certificação gerando as devidas medidas disciplinares.