

Universidade Federal de Pernambuco

Centro de Informática

Graduação em Ciência da Computação

**Auditoria de Sistemas: a Importância da Segurança da Informação para as Demonstrações Financeiras**

Marina Alecrim de Carvalho Novaes

**Trabalho de Graduação**

Recife, 13 de dezembro de 2011

Universidade Federal de Pernambuco

Centro de Informática

**Auditoria de Sistemas: a Importância da Segurança da Informação para as Demonstrações Financeiras**

Marina Alecrim de Carvalho Novaes

*Monografia apresentada ao Centro de Informática da Universidade Federal de Pernambuco, como requisito parcial para obtenção do Grau de Bacharel em Ciência da Computação.*

*Orientador: Hermano Perrelli de Moura*

Recife, 13 de dezembro de 2011

*"Julgue o seu sucesso pelas coisas que você teve que renunciar pra conseguir."*

**Dalai Lama**

Dedico a meus pais José e Valéria, a quem devo a minha formação moral. Meu reconhecimento e eterna gratidão pela paciência, compreensão e apoio constante na minha jornada.

**Agradecimentos**

A Mariana, que sempre me encorajou a concluir o trabalho monográfico**.**

Aos meus pais que são pessoas que acreditam muito no meu potencial e me sinto muito feliz em poder orgulhá-los com mais essa conquista.

Aos professores e monitores desta instituição que sempre se dedicaram a formar profissionais diferenciais para o mercado de trabalho e, sem dúvida, fazem isso com muita competência.

Aos meus amigos de turma que me fizeram companhia durante estes quatro anos e meio de faculdade com quem compartilhei minhas viradas de noite, debates sobre diversos temas, contribuindo bastante para minha formação acadêmica. Gostaria de pontuar, inclusive alguns nomes, Thaís, Juliana, André, Tiaguinho, Sara e Tarcísio, vocês possuíam qualidades que me faziam querer seguir em frente, mesmo nos momentos mais complicados deste curso.

Aos meus colegas de trabalho, que possuem o conhecimento técnico e me ajudaram a realizar este trabalho de graduação. Pude contar com a enorme experiência e competência de vocês e isso é um grande incentivo para mim, pois essa admiração que sinto só me faz querer me espelhar.

A meu namorado, Domingos Mendes, pela paciência e compreensão que teve que ter pelas várias vezes que não pude estar ao seu lado.

**Resumo**

O presente estudo aborda um tema bastante sensível para qualquer empresa: a Segurança da Informação. Os sistemas de informação que fazem parte dela suportam dados críticos e, por conta disso, são considerados ferramentas de grande importância na gestão estratégica de conhecimento das organizações. Estes sistemas são os grandes responsáveis pela maior agilidade nos processos e disponibilidade das informações.

Neste trabalho é proposta a auditoria de sistemas das empresas com foco em segurança da informação, salientando a necessidade das organizações oferecerem informações seguras aos tomadores de decisão. Essa confiabilidade nas informações, dados, registros e sistemas podem ser maximizadas através da utilização de mecanismos de segurança da informação.

Porém, segurança implica em custos de manutenção, uma vez que sistemas que não levam em consideração segurança são mais simples e fáceis de manter. O problema é que a falta de confiabilidade ou perda de informações pode custar muito mais caro. Desta forma, através de modelos como CobiT, bibliotecas de melhores práticas como o ITIL, implementação de normas como as ISO 27001 e ISO 27002 são ótimas alternativas para as empresas estarem em conformidade com as melhores práticas de segurança da informação do mercado.

No processo de auditoria de sistemas de informação é avaliado se estas boas práticas estão sendo obedecidas nas organizações. Caso não estejam, é dever da auditoria realizar recomendações para mitigar os riscos que a organização pode estar correndo. Sendo assim, em alguns casos, a decorrência de um trabalho de auditoria facilita as organizações perceberem a importância do investimento na área de segurança da informação em prol de um maior conforto nas informações suportadas pelos sistemas.

Palavras-chave: Segurança da Informação, Auditoria de Sistemas.

Abstract

The current study addresses a very sensitive theme to any company: The Information´s security. Critical data are supported by companies´ information system , and because of this, they are considered great importance tools on companies´ strategic management . These systems are the most responsible for the bigger agility on processes and information´s availability.

Along this work, it is proposed the auditing for companies´ systems focusing on information´s security, highlighting the need for the of the organizations offer security information to decision markers. This reability of the information, data, records and systems can be maximized through the use of information security mechanisms.

However, security implies maintenance costs, since systems that do not take into account security are simpler and easier to maintain. The problem is that the lack of reliability or loss of information can cost a lot more expensive. Thus, through models such as CobiT, libraries of best practices like ITIL, implementation of standards such as ISO 27001 and ISO 27002 are great alternatives for companies to comply with best practice information security market.

In Information Systems Audit process is assessed if these practices are being followed in organizations. If not, it is the duty of the audit make recommendations to mitigate the risks that organization may be running. Thus, in some cases, the result of the audit helps organization realize the importance of investments in the area of information security for the sake of greater comfort supports by the information systems.

Keywords: Information Security, Systems Audit.

Sumário

[1. Introdução 1](#_Toc311582591)

[2. Auditoria Contábil 3](#_Toc311582592)

[2.1. História da Auditoria 3](#_Toc311582593)

[2.2. Definição 3](#_Toc311582594)

[2.3. Características e Habilidades Requeridas de um Auditor 4](#_Toc311582595)

[2.4. Objetivo da Auditoria Contábil 6](#_Toc311582596)

[2.5. Materialidade em Auditoria 7](#_Toc311582597)

[3. Auditoria de Sistemas de Informação 8](#_Toc311582598)

[3.1. Objetivo 8](#_Toc311582599)

[3.2. Segurança da Informação 8](#_Toc311582600)

[3.2.1. O valor da Informação 8](#_Toc311582601)

[3.2.2. Princípios da Segurança da Informação 9](#_Toc311582602)

[3.2.3. A Importância da Segurança da Informação 10](#_Toc311582603)

[4. CobiT 12](#_Toc311582604)

[4.1. O Modelo 12](#_Toc311582605)

[4.2. Visão Geral 14](#_Toc311582606)

[4.3. Princípios Básicos 15](#_Toc311582607)

[4.3.1. Planejar e Organizar (PO – Plan and Organize) 16](#_Toc311582608)

[4.3.2. Adquirir e Implementar (AI – Acquire and Implement) 16](#_Toc311582609)

[4.3.3. Entregar e Suportar (Deliver and Support) 16](#_Toc311582610)

[4.3.4. Monitorar e Avaliar (Monitoring and Evaluate) 17](#_Toc311582611)

[4.4. Garantir a Segurança dos Sistemas 18](#_Toc311582619)

[5. Outros Referenciais Metodológicos 23](#_Toc311582620)

[5.1. ITIL 23](#_Toc311582621)

[5.2. PMBOK 23](#_Toc311582622)

[5.3. ISO 27001 e ISO 27002 24](#_Toc311582623)

[5.3.1. ISO 27001 – Information Security Management Systems Requirement 24](#_Toc311582624)

[5.3.2. ISO 27002 – *Code of Practice for Information Security Management* 25](#_Toc311582625)

[Esta norma encontra-se distribuídas em 11 seções que correspondem aos controles de segurança da informação. São elas: 26](#_Toc311582626)

[6. Recomendações 28](#_Toc311582627)

[6.1. Adoção de um ou uma combinação de referenciais metodológicos 28](#_Toc311582628)

[6.2. Criação de uma área de Auditoria Interna na organização 28](#_Toc311582629)

[6.3. Aumento de investimento em TI 29](#_Toc311582630)

[7. Conclusão e Trabalho Futuros 30](#_Toc311582631)

[7.1. Conclusão 30](#_Toc311582632)

[7.2. Trabalhos Futuros 31](#_Toc311582633)

[8. Referências Bibliográficas 32](#_Toc311582634)

**Lista de Figuras**

[Figura 1- Inter-relacionamento dos componentes do CobiT 25](#_Toc311294481)

[Figura 2 – Os Quatro Domínios Inter-relacionados do CobiT 26](#_Toc311294482)

[Figura 3 – Visão Geral do Modelo CobiT 28](#_Toc311294483)

[Figura 4 – Áreas de conhecimento do PMBOK 33](#_Toc311294484)

**Lista de Tabelas**

[Tabela 1 – Evolução do CobiT 23](#_Toc311289753)

# Introdução

Com base no crescimento que as organizações vêm tendo e em paralelo, com a evolução bastante acelerada da tecnologia, foi inevitável que as atividades manuais se tornassem automatizadas. O ambiente de negócios foi se tornando cada vez mais complexo e desafiador para os gestores das empresas de praticamente qualquer mercado e, conseqüentemente, as áreas produtivas e administrativas foram se automatizando por sistemas e ambientes de tecnologia da informação.

Tais ambientes tecnológicos são responsáveis pelo processamento e armazenamento de um dos bens mais valiosos de uma organização: a informação. Empresas e consumidores dependem da comunicação, integridade, disponibilidade destes dados para trabalho e negócios. Dessa forma, é essencial que, nos dias de hoje, as empresas invistam em recursos tecnológicos que dêem suporte e segurança às informações.

Diante deste contexto, o investimento em segurança da informação se torna vital para que uma empresa não esteja exposta a riscos. Logo, é necessário que as medidas de controle e segurança de sistemas sejam revisadas e avaliadas sistematicamente por auditores, a fim de assegurar a proteção dos bens e serviços existentes em todas as áreas da empresa.

Sendo assim a auditoria de sistemas se propõe a analisar as demonstrações financeiras, a partir da avaliação da adequação das tecnologias e sistemas de informação utilizados na organização, através da revisão e avaliação dos controles. Identificadas falhas, erros, irregularidades ou ineficiência nestes controles, cabe a auditoria fazer recomendações em seu parecer, para correção e melhoria dos controles internos com o intuito de minimizar os riscos encontrados.

Muito embora a informática seja vista como uma ferramenta de melhoria, diversas empresas não possuem a cultura de realizar grandes investimentos nesta área, uma vez que ela não traz retorno financeiro. Especialmente quando se trata em Segurança da Informação, vários aspectos são vistos de forma negativa, uma vez que há um aumento nos custos, perda de liberdade, aumento de complexidade e perda de desempenho, dificultando ainda mais tais investimentos.

É essencial que para que a organização esteja em conformidade com as boas práticas de TI, a mesma precisa realizar investimentos e dar o devido valor ao parecer de auditoria. Diante disso, este trabalho tem por objetivo destacar para as organizações, a importância da Segurança da Informação em uma Auditoria de Sistemas, cujo papel é imprescindível para garantir a confiança dos seus dados financeiros.

O trabalho que segue iniciará apresentando conceitos básicos de auditoria contábil e auditoria de sistemas, destacando a importância da segurança da informação para as organizações. Posteriormente, serão citados frameworks mais utilizados e que podem ser implantados para que as organizações tenham um bom ambiente de controles de segurança da informação. Por fim, seguem algumas recomendações que ajudem as organizações estarem em conformidade com as boas práticas de segurança da informação, uma conclusão breve sobre o trabalho e sugestões para trabalhos futuros.

# Auditoria Contábil

Nesse capítulo serão apresentados conceitos básicos sobre auditoria contábil e seu objetivo, fazendo inicialmente um breve histórico sobre auditoria e características necessárias de um auditor.

## História da Auditoria

Com o advento da Revolução Industrial do século XVIII na Inglaterra, houve um crescimento considerável das atividades e conseqüentemente uma procura muito grande por capital. Decorrente a isto, muitos problemas contábeis complexos começaram a surgir, até que se chegou a conclusão de que era necessário realizar controles internos com o objetivo de detectar erros e fraudes que por ventura poderiam estar acontecendo. [1]

Com o crescimento do capitalismo em 1900, a profissão do contador tornou-se mais reconhecida e difundida. Em 1934, com a criação do Exchange Security Commission, nos Estados Unidos, a profissão do auditor ganhou novo estímulo, uma vez que as empresas que possuíam ações nas Bolsas de Valores foram obrigadas a utilizar os serviços de auditoria para assegurar que as informações extraídas das demonstrações financeiras eram fieis a realidade e com isso os investidores pudessem comprar suas ações de maneira mais confiável.

Já aqui no Brasil, a auditoria foi formalmente organizada em março de 1957 quando foi formado o Instituto Público de Contadores do Brasil, em São Paulo, mas ela só foi reconhecida em 1968 por um ato do Banco Central. Esse ato teve influência pelo surgimento e crescimento de grandes filiais de empresas estrangeiras aqui no Brasil, onde a matriz passava a exigir auditorias destas filiais. Além disso, com o crescimento das empresas brasileiras e a evolução do mercado de capitais, sentiu-se a necessidade de se criarem normas de auditoria. Para assegurar o funcionamento eficiente e regular dos mercados de bolsa e de balcão foi criado a Comissão de Valores Mobiliários (CVM) [1] [2].

## Definição

De maneira geral, pode-se definir auditoria como uma atividade de exame e avaliação de procedimentos, processos, sistemas, registros e documentos com o objetivo de aferir o cumprimento dos planos, metas, objetivos e políticas da organização. A mesma é considerada como um método para constatar a integridade contábil de uma empresa. Segundo o Aurélio, auditoria é “o exame analítico e pericial que segue o desenvolvimento das operações contábeis desde o início até o balanço”.

A auditoria se divide em dois tipos:

* Auditoria Interna ou Operacional: é aquela onde o auditor é funcionário da empresa e a revisão das atividades é contínua.
* Auditoria Externa ou Independente: é aquela onde o auditor pertence a uma empresa terceira e independente e o exame das informações comprobatórias das demonstrações financeiras é periódica, geralmente semestral ou anual.

Muito embora existam dois tipos de auditoria, o trabalho executado tanto pela interna quanto pela externa é o mesmo. Ambas executam seu trabalho seguindo técnicas de auditoria, fazem avaliação dos controles internos da organização e formulam sugestões de melhoria para as falhas encontradas.

## Características e Habilidades Requeridas de um Auditor

Como dito anteriormente, a evolução da auditoria no Brasil se deu devido a expansão das atividades econômicas, associadas ao número de empresas que começaram a se estabelecer aqui. Com isso a profissão do auditor foi se expandindo, vem tomando grande espaço no mercado e se desenvolve em diferentes graus de especialização.

Esta profissão exige certas características e habilidades que são indispensáveis para ser assumida. Abaixo será detalhada cada uma delas:

* + 1. Independência

De acordo com NBC P 1.2, no tópico 1.2.2.1, “Entende-se como independência o estado no qual as obrigações ou os interesses das entidades de auditoria são suficientemente isento dos interesses dos clientes para permitir que os serviços sejam prestados com objetividade.”

Esta é uma das características mais importantes para a prática desta profissão. O auditor, a fim de assegurar sua independência, deve-se manter imparcial no seu julgamento em todas as fases do processo de auditoria, desde o planejamento, passando por execução até a emissão do seu parecer. Para isso, cabe ao auditor evitar envolver-se com a organização auditada, a fim de preservar sua independência e expressar opinião sem ser influenciado por circunstâncias externas e que comprometam o julgamento profissional. [3]

Determinadas situações caracterizam perda de independência em relação a entidade auditada. De acordo com Bendoraytes (2004, p. 16), as situações citadas abaixo são exemplos que caracterizam essa quebra de independência:

1. Envolvimento financeiro, inclusive com um não-cliente que possua relação de investidor – ou empresas coligadas ou controladas – com o cliente;
2. O exercício de cargo, qualquer que seja, dentro do período sob auditoria ou imediatamente antes a contratação;
3. A prestação de serviços que envolvam funções administrativas;
4. A existência de relacionamentos pessoais e familiares com o cliente;
5. A aceitação de bens e serviços, salvo em condições de negócios que não sejam mais favoráveis do que os disponíveis de maneira geral para terceiros.
	* 1. Integridade

Para que a integridade seja seguida, o auditor precisa realizar seus trabalhos com honestidade, responsabilidade, observar a lei, respeitar e contribuir para os legítimos e éticos objetivos da entidade.

Segundo Attie (1998), certas atitudes que colocariam em cheque esta característica são:

1. Omitir algum fato importante que conheça, não exposto as demonstrações financeiras, mas cuja exposição seja indispensável;
2. Deixar de relatar ou dissimular irregularidades, informações ou dados incorretos que estejam contidos nas demonstrações financeiras;
3. Negligenciar efeitos graves na execução de qualquer trabalho profissional e no seu respectivo relato;
4. Não reunir evidências suficientes para justificar a expressão de sua opinião;
5. Ocultar a existência de desvios importantes ou não expor qualquer omissão relevante dos preceitos legais ou contábeis, ou das normas e procedimentos da organização.
	* 1. Eficiência

Tendo em vista o escopo do trabalho a ser realizado, o auditor deve fazer um exame para medir sua aptidão e julgar sua viabilidade técnica para sua execução. Com essa aptidão o rendimento será mais efetivo. Dessa forma, minimizam-se os custos operacionais e aumenta-se a qualidade do serviço prestado. [4]

* + 1. Confidencialidade

Sabendo que o auditor tem acesso a certas informações, muitas vezes confidencias, o mesmo é obrigado a utilizar dados e informações que estão ao seu acesso exclusivamente durante a execução do serviço que lhe foi prestado. Salvo em casos em que a alta administração sob autorização expressa permita a divulgação de algum dado. Caso contrário, é regra mandatória que nenhum dado, informação, documento ou demonstração seja utilizado para interesse próprio ou de terceiros.

Muito embora um auditor tenha que ter determinadas características e habilidades desenvolvidas para exercer sua função, o mesmo deve possuir certos atributos pessoais desenvolvidos, como: discrição, raciocínio lógico e, principalmente, um sentimento real de independência.

## Objetivo da Auditoria Contábil

O objetivo da auditoria consiste em apoiar os membros da empresa no desempenho de suas atividades. Para tanto, ela é responsável pelo exame das demonstrações financeiras de um determinado período, a fim de verificar se as mesmas estão de acordo com os princípios da contabilidade. Dessa forma, tais demonstrações devem assegurar que elas representem adequadamente a posição patrimonial e financeira da organização, inclusive avaliando o processo da economicidade, eficiência e eficácia na utilização dos recursos recebidos de órgãos públicos ou privados [5].

A auditoria tem por objetivo de emitir um parecer sobre a adequação das demonstrações analisadas. Este documento reflete a compreensão do auditor sobre estas análises e tem por objetivo dar aos leitores uma visão geral do trabalho realizado e, principalmente, o que foi concluído sobre ele. Este parecer destina-se em geral aos acionistas, diretores, administradores, analistas de mercado, entidades financeiras, etc. Dessa forma, o produto final de uma auditoria é de extrema importância devido às informações nele contidas [6].

Seguindo essa linha de raciocínio, o auditor precisa de um suporte para gerar este relatório de auditoria. Esse suporte é dado através de fundamentos de auditoria que permitam ele conhecer melhor o ambiente no qual está inserido.

Um fator importante a ser considerado é que a auditoria não pode ser baseada apenas na opinião e avaliação de pessoas envolvidas no trabalho. As conformidades e não conformidades encontradas devem ser embasadas em evidências, ou seja, em registros, documentos e outras informações que confirmem estas evidências.

Dentre os diversos tipos de auditoria existentes, um deles é a auditoria de Sistemas de Informação que é o ramo da auditoria que revisa e avalia os controles internos dos sistemas. No próximo capítulo, aprofundaremos neste segmento de auditoria a fim de entendermos a sua importância para a auditoria contábil e então analisar a importância que o mesmo pode gerar para as demonstrações financeiras.

## Materialidade em Auditoria

De acordo com a SAS nº 47 (AU 312.08), “o auditor deve considerar em conjunto o risco de auditoria e materialidade no (a) planejamento da auditoria e no desenho dos procedimentos de auditoria e (b) avaliando se as demonstrações financeiras, tomadas como um todo, estão apresentadas de forma imparcial e honesta e em conformidade com os princípios contabilísticos geralmente aceites”. [7]

Como faz nota o FASB na SFAC nº 2, a materialidade refere-se “à magnitude de uma omissão ou relato errado da informação financeira que, à luz das circunstâncias envolventes, torne provável que o julgamento de uma pessoa razoável e confiante nessa informação possa ser alterado ou influenciado pela omissão ou erros”; Em outras palavras, o FASB considera que a informação é relevante se tiver uma capacidade de fazer a diferença nas decisões de investidores e demais *stakeholders*. [7]

Este conceito de materialidade é importante, pois não necessariamente todos os sistemas precisam ser avaliados em um processo de auditoria de sistemas, mas sim aqueles que suportam saldos materiais, ou seja, são aqueles que podem causar impactos nas demonstrações financeiras da organização.

# Auditoria de Sistemas de Informação

Nesse capítulo será apresentado a definição e objetivo sobre auditoria de sistemas de informação e serão introduzidos conceitos básicos sobre segurança da informação a fim de realizar uma contextualização maior sobre o tema abordado.

## Objetivo

Com a evolução da tecnologia e o crescimento das organizações, grande parte das empresas atuais tem suas áreas produtivas e administrativas automatizadas por sistemas e ambientes de tecnologia de informação. Tais ambientes se tornam cada vez mais críticos para estas empresas, umas vez que os mesmo armazenam e processam informações de suma importância. Informações estas que podem impactar as demonstrações financeiras. A indisponibilidade de algum desses recursos de TI pode comprometer significativamente as operações de uma organização mesmo que por um período curto de tempo.

Devido ao alto grau de automatização dos processos que antes eram manuais e o aumento da complexidade do processamento das informações fez-se necessário um melhor gerenciamento e criação de controles mais rigorosos para tais atividades. Ou seja, a implementação de controles, políticas e requisitos de segurança é de extrema importância, pois ajudam a minimizar os riscos associados a TI, tendo em vista o alinhamento dos objetivos da organização.

Diante desse contexto, a Auditoria de Sistemas de Informação se propõe a validar e avaliar os controles internos de sistemas de informação que envolve processamento de informações críticas para a tomada de decisão. Para isso, durante o processo de auditoria, o auditor deve reunir, agrupar e avaliar evidências que ajudem a determinar se um certo sistema de informação suporta adequadamente um ativo de negócio, de modo a manter a integridade das informações, e realiza os objetivos esperados pela alta administração, atendendo as regulamentações e leis estabelecidas.

## Segurança da Informação

### O valor da Informação

As organizações hoje, sejam elas públicas ou privadas, se encontram cada vez mais inseridas em um cenário digital, integrado, complexo e dinâmico. Em meio a isto é inerente o valor dado a segurança de suas informações para assegurar o ativo mais importante destas empresas: a informação.

“Podemos definir segurança da informação como um área do conhecimento dedicada a proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade” SÊMOLA (2003, p.43)

A informação é um bem, que como qualquer outro é importante para o negócio, tem grande valor para a organização e, conseqüentemente, precisam ser adequadamente protegida. Dispor de informações corretas, no momento adequado, significa tomar uma decisão de maneira ágil e eficiente. A informação é a essência da inteligência competitiva, portanto deve ser bem administrada e salvaguardada. [8]

Imagine um sistema de informação que apresenta cotações atualizadas de produtos de mercado ficar fora do ar. A indisponibilidade destas informações pode acarretar em prejuízos enormes à empresas e perda de clientes.

### Princípios da Segurança da Informação

Para reduzir os riscos de vazamentos, fraudes, erros, sabotagens, acessos indevidos, roubos de informações ou qualquer outro tipo de ameaça que possa prejudicar a organização, é necessário que a informação atenda a determinados princípios básicos para que ela seja considerada segura, são eles:

* Integridade: a integridade consiste em proteger a informação sem que haja permissão explícita do proprietário da mesma para qualquer tipo de modificação sem permissão. Este princípio garante a totalidade e exatidão das informações, ou seja, integridade significa garantir que se o dado está lá, então não foi corrompido e encontra-se íntegro.
* Disponibilidade: princípio que assegura o usuário ter acesso a informação sempre que precisar e de modo que ela esteja utilizável.
* Confidencialidade: princípio que assegura a informação esteja disponível apenas para pessoas que devem ter acesso a mesma. Consiste em proteger a informação contra leitura e cópias por pessoas que não tenham sido explicitamente permitidas pelo proprietário da informação.

Adicionalmente, podem ser consideradas outras propriedades presentes no NBR ISO/IEC. São elas:

* Legalidade
* Responsabilidade
* Autenticidade
* Autoridade
* Não-repúdio
* Auditoria

### A Importância da Segurança da Informação

Com a globalização e o desenvolvimento do mundo moderno e empresarial, as informações foram se tornando bastante volumosas. Os negócios foram se expandindo e aliado a isso, tomadas de decisões importantes precisavam ser realizadas em tempo hábil. Com isso, surgiu a necessidade de mecanismos mais eficientes de manipulação das informações a fim de que os mesmos processassem de maneira mais rápida o que era desejado e antes feito manualmente. [9]

Estas informações processadas geram relatórios contábeis e financeiros que são apresentados a usuários interessados na saúde financeira da organização, como: acionistas, investidores, analista de mercado financeiro, entre outros. Como a maioria das empresas, principalmente as de grande porte, são obrigadas a se submeter a auditorias independentes, nas quais muitas vezes, está incluída a auditoria de sistemas, tais usuários avaliam o valor das ações a partir de relatórios gerados por tais sistemas. Para que os mesmos possam ter confiabilidade sobre as informações que estão sendo apresentadas, as organizações precisam de controles internos e processos definidos que garantam a integridade das informações apresentadas por tais sistemas e contribuam com a qualidade das informações. [8]

 Como pode-se perceber, a informação possui grande valor para uma empresa e tal informação deve ser adequadamente protegida, uma vez que é considerada o principal patrimônio da organização e está sob constante risco. Diante deste cenário, uma empresa que se propõe a implantação de um sistema integrado informatizado, necessita respeitar alguns aspectos de muita importância para que não fique exposta a tais riscos. Para que os mesmos sejam mitigados, é necessário a criação de controles que devem estabelecer um processo formal para avaliar, identificar e desenvolver respostas aos riscos analisados pela auditoria. Por conta disso, as organizações devem demonstrar controles crescentes em segurança. Para isso utilização de frameworks como o CobiT auxiliam os gerentes de TI nos seus objetivos alinhados com os objetivos da organização. No próximo capítulo será apresentado uma visão geral do CobiT e como este modelo pode auxiliar as organizações a melhorarem o seu ambiente de controle em segurança da informação dos recursos de TI.

# CobiT

Como foi dito anteriormente, a informação é o bem mais valioso de uma organização e quem suporta este bem tão valioso é a tecnologia. Normalmente, as organizações mais bem-sucedidas dão o devido valor a tecnologia a fim de minimizar os riscos que podem estar associados a informação. Logo, o gerenciamento de riscos, bem como as crescentes demandas regulatórias e dependência crítica de muitos processos de TI são fatores que ajudam as organizações perceberem o devido valor que determinados frameworks possuem, tais como: o CobiT. [10]

## O Modelo

O *Control Objectives for Information and related Technology* (CobiT) é um guia de boas práticas dirigido para a gestão de Tecnologia da Informação e que representa um consenso de especialistas da área. Tais práticas são fornecidas através de um modelo de domínios e processos e apresenta atividades em uma estrutura lógica e gerenciável.

O CobiT foi criado inicialmente para a auditoria de TI e representava uma compilação de itens a serem verificados na auditoria. A medida que este foi evoluindo em suas diversas versões, o mesmo acabou se tornando um modelo de controle de governança de TI.

O CobiT define Governança de TI da seguinte forma:

“Responsabilidade da alta direção, consiste em liderança, estruturas organizacionais e processos que garantem que a TI corporativa sustenta e estende as estratégias e objetivos da organização”.[9]

Vale salientar que o CobiT não é um padrão definitivo, ele serve como apoio para a implementação de controles na governança de TI. Abaixo segue um a evolução do modelo:

Tabela 1 – Evolução do CobiT

|  |  |  |
| --- | --- | --- |
| 1996 | Primeira Edição do CobiT | ISACA (Information System Audit and Control Association – www.isaca.org) lança um conjunto de objetivos de controle para aplicações de negócio. |
| 1998 | Segunda Versão do CobiT | Inclui uma ferramenta de suporte a implementação e a especificação de objetivos de alto nível de detalhes. |
| 2000 | Terceira Versão do CobiT | Inclui normas e guias associadas a gestão. O ITGI (IT Governance Institute – www.itgi.org) torna-se o principal editor do framework. |
| 2002 | Sarbanes-Oxley Act | O *Sarbanes-Oxley Act* foi aprovado. Este acontecimento teve um impacto significativo na adoção do CobiT nos EUA e empresas globais que atuam nos Estados Unidos. |
| 2005 | Quarta Versão do CobiT | Melhoria dos controles para assegurar a segurança e disponibilidade dos ativos de TI na organização. |

A ISACA disponibilizou recentemente o COBIT v.5 para sua revisão e feedback em seu site. O principal objetivo desta exposição é a obtenção de comentários do público em relação à integridade, qualidade e valor do trabalho de desenvolvimento realizado. A expectativa é que a versão final e publicação do CobiT v.5 seja no início de 2012.

Atualmente o Cobit possui a seguinte missão:

“Pesquisar, desenvolver, publicar e promover um modelo de controle para governança de TI atualizado e internacionalmente reconhecido para ser adotado por organizações e utilizado no dia-a-dia por gerentes de negócios, profissionais de TI e profissionais de avaliação.”[9]

Existem diversas vantagens para adotar um padrão já definido, uma vez que este padrão foi desenvolvido e amadurecido diversas vezes por centenas de *experts* e especialistas qualificados de várias organizações de todo o mundo tornando este modelo cada vez mais robusto. Desta forma, não faz muito sentido gastar tempo e esforço para desenvolver um novo modelo baseado na experiência limitada de uma empresa ao invés de adotar um framework tão amadurecido e reconhecido internacionalmente. Adicionalmente, o CobiT está em manutenção contínua e periodicamente uma nova versão é lançada, mais amadurecida e melhor desenvolvida para ser implantada em empresas de pequeno e grande porte. Além de tudo isso, o CobiT é um modelo auditável, ou seja, sem padrões definidos seria muito mais complicado para os auditores avaliarem os controles, pois em organizações que possuem este modelo implantado, os auditores estão seguros que irão obter informações necessária para a execução do seu trabalho.

Como podemos perceber, existe uma série de vantagens em implantar controles baseados em frameworks já reconhecidos, como é o caso do CobiT. Este modelo lida com todos os aspectos relacionados com Governança de TI, inclusive controles relacionados a Segurança da Informação. A seguir, entenderemos melhor a estrutura do CobiT e destacaremos os pontos relevantes sobre segurança da Informação.[9]

## Visão Geral

Tudo no CobiT gira em torno das necessidades de negócio e é com base nas necessidades de negócio que são definidos os processos de TI. Para garantir que estas necessidades serão atendidas, é necessário que um conjunto de atividades seja definido e estas atividades só serão executadas de acordo com papéis pré-definidos, como mostrado na primeira linha de atuação da Figura 1.

Na segunda linha de atuação, para garantir de fato que estes processos atingem suas metas é necessário medir. Esta medição é realizada através de indicadores e utilizando modelos de maturidade a fim verificar se os processos estão atingindo o alvo desejado.

Seguindo esta linha de raciocínio, para garantir o alcance dos objetivos é necessário a implementação de controles e para isso o CobiT possui objetivos de controle. Tais controles indicam com o que se deve preocupar com cada um dos processos. [9]

Por fim, conforme comentado anteriormente, como este framework nasceu através da necessidade da auditoria, existem os testes que são necessários para avaliar se os controles definidos estão sendo realmente efetivos.



Figura 1- Inter-relacionamento dos componentes do CobiT

## Princípios Básicos

O modelo CobiT foi criado com as principais características de ser focado em negócios, orientado a processos, baseado em controles e orientado por medições.[9]

Para o negócio funcionar, ele precisa de informação e esta informação deve atender a determinados critérios de qualidade, segurança e confiabilidade. A fim de produzir estas informações, é necessário recursos de TI (dados, aplicações, infra-estrutura e pessoas). Para garantir que os recursos são usados corretamente e a informação sai da maneira esperada, é necessário a definição de processos, pois são estes que irão gerenciar os recursos de TI. Por sua vez, para garantir que os processos sejam executados da maneira correta, é necessário haver controles, indicadores de desempenho e indicadores de resultado.[9]

A fim de que a governança de TI seja eficiente, é importante avaliar os riscos e as atividades de TI que precisam ser gerenciadas. Para isso, o CobiT considera que os seus processos, no total 34, estão agrupados em 4 grandes domínios que trabalham em conjunto, conforme a Figura 2. Os objetivos de controle de TI do CobiT são organizados em processos de TI e totalizam 318. Dessa maneira, o CobiT proporciona uma ligação entre os requerimentos de governança de TI, processos de TI e os controles de TI. Os domínios são:

* Planejar e Organizar (PO – Plan and Organize)
* Adquirir e Implementar (AI – Acquire and Implement)
* Produzir e Suportar (DS – Deliver and Support)
* Monitorar e Avaliar (ME – Monitor and Evaluate)

##

Figura 2 – Os Quatro Domínios Inter-relacionados do CobiT

### Planejar e Organizar (PO – Plan and Organize)

Este domínio define as estratégias e táticas que ajudam a identificar quais as melhores maneiras de TI contribuir para as organizações atingirem seus objetivos de negócio. Este domínio ajuda a alinhar as estratégias de negócio às estratégias de TI, indicam se as empresas estão utilizando bem os seus recursos, se a qualidade dos sistemas de TI estão adequadas às necessidades de negócio, se todos da organização entendem os objetivos de TI e verifica se os riscos de TI são entendidos e estão sendo gerenciados.

### Adquirir e Implementar (AI – Acquire and Implement)

Este domínio tem como objetivo efetuar a estratégia de TI, desenvolvendo as necessidades de tecnologia, sempre relacionados aos negócios da organização. Além disso, alterações e manutenções nos sistemas existentes são cobertas por este domínio para assegurar que as soluções continuem a atender os objetivos de negócios. Este domínio trata de questões como as que seguem abaixo:

* Os novos projetos fornecerão soluções que atendam às necessidades de negócios?
* Os novos projetos serão entregues no tempo e orçamento previstos?
* Os novos sistemas ocorreram apropriadamente quando implementado?
* As alterações ocorrerão sem afetar as operações de negócios atuais?

### Entregar e Suportar (Deliver and Support)

Este domínio compreende a entrega dos serviços, o gerenciamento da mudança e continuidade, serviços de suporte para os usuários e o gerenciamento de dados e recursos operacionais, ou seja, “Adquirir e Implementar” foca aspectos de entrega de tecnologia da informação. Sendo assim, este domínio consegue avaliar se os custos de TI estão otimizados e se os serviços de TI estão sendo entregues de acordo com as prioridades de negócio. Além disso, indicam se as pessoas envolvidas na utilização dos sistemas de TI estão habilitadas para usá-los de maneira produtiva e segura e consegue indicar se as características básicas de segurança da informação (confidencialidade, integridade e disponibilidade) estão sendo obedecidos para garantir a segurança da informação.

### Monitorar e Avaliar (Monitoring and Evaluate)

Este domínio avalia se o sistema de TI está atingindo os objetivos para os quais ele foi especificado e controla os requisitos para atender os objetivos regulatórios. Ou seja, ele trata do gerenciamento de performance, monitoramento do controle interno, a aderência regulatória e a governança. Sendo assim, este domínio consegue responder perguntas, como estas:

* A performance de TI é mensurada para detectar problemas antes que seja muito tarde?
* O gerenciamento assegura que os controles internos sejam efetivos e eficientes?
* O desempenho da TI pode ser associado aos objetivos de negócio?
* Existem controles adequados para garantir confidencialidade, integridade e disponibilidade das informações?

 É importante salientar que dificilmente todas as organizações possuirão a mesma estrutura para aplicar os mesmos 34 processos-chaves do CobiT . O CobiT fornece uma relação completa que podem ser utilizados para verificar a totalidade das atividades e responsabilidades. No entanto, nem todos precisam ser utilizados e podem ser combinados conforme a necessidade do negócio. [9] Na Figura 3, segue todos os processos definidos pelo CobiT divididos nos 4 domínios:



Figura 3 – Visão Geral do Modelo CobiT

Para cada um desses 34 processos, uma ligação foi feita com os objetivos de negócios e de TI suportados. Também são fornecidas informações sobre como os objetivos podem ser medidos, quais são as atividades-chave, as principais entregas e quem é responsável por elas.

1.
2.
3.
4. 1.
	2.
	3.

## Garantir a Segurança dos Sistemas

Dentre os processos que o CobiT abrange, é importante destacar aquele que evidencia a importância da Segurança da Informação para a organização: “DS5 – Garantir a Segurança dos Sistemas”.

Este processo do Cobit foi criado a fim manter seguros os ativos de TI e as informações, conseqüentemente, garantindo sua integridade, confidencialidade, não-repudiação, disponibilidade (tanto da informação como dos recursos de TI), autenticação e controle de acesso aos dados apenas por pessoas permitidas. Este controle inclui o estabelecimento e a manutenção de papéis, responsabilidades, políticas, padrões e procedimentos de segurança de TI.[9]

Desta forma a gestão de segurança abrange o monitoramento, detecção, reporte e solução de vulnerabilidades e incidentes de segurança que uma organização está exposta a correr. Sendo assim, uma gestão eficaz de segurança consegue proteger os ativos de TI e diminuir o impacto sobre os negócios.

A fim de compreender melhor como garantir a segurança de sistemas, o CobiT Possi os objetivos de controle detalhados. São eles:

* Gestão da Segurança de TI

Gerenciar as ações de segurança de TI de modo que elas estejam alinhas com os requisitos do negócio. [9]

* Plano de Segurança de TI

Definição de um plano de segurança que envolva a infra-estrutura de TI e cultura de segurança, com o objetivo de traduzir os requisitos de negócio, de riscos e conformidades em um plano abrangente de segurança de TI. Este plano deve ser realizado em forma de políticas e procedimentos e levando em consideração os investimentos adequados para a sua implementação no que se refere a pessoas, hardware, software e serviços. Após a elaboração destas políticas e procedimentos, é necessária a sua divulgação para os usuários e as partes interessadas. [9]

* Gestão de Identidade

Todos os usuários (sejam eles permanentes, temporários, internos ou externos) devem ser identificados unicamente, não sendo aceitável a criação de usuários genéricos, que não permitam a identificação exclusiva da pessoa que o utiliza. O direito de acesso destes usuários deve estar de acordo com a função que será executada e deve estar em conformidade com as necessidades de negócio da organização para aquela função. Deve haver um processo definido, onde para que o direito de acesso seja concedido, o mesmo deve ser solicitado pela gestão de usuários, aprovados pelo proprietário do sistema e implementado pelo responsável de segurança. É necessário implementar e manter atualizadas medidas técnicas e de procedimentos com boa relação custo-benefício para determinar a identificação dos usuários, implementar a devida autenticação e impor direitos de acesso. [9]

* Gestão de Contas de Usuários

Assegurar a existência de um procedimento de gestão de contas de usuários que trate de solicitações de novas contas, bloqueio, remoção, suspensão e modificação. Levando em consideração que deve haver um procedimento de concessão de acesso de novas contas no sistema, passando pela aprovação dos devidos responsáveis. Neste procedimento deve ser aplicado os tipos de usuário, sejam eles administradores ou usuários comuns, internos ou externos, para casos normais ou emergenciais. Os direitos e obrigações relacionados a acesso a sistemas e informações devem ser definidos e assinados em contrato para todos os tipos de usuários. Revisões de todas as contas e seus devidos privilégios devem ser feitas freqüentemente. [9]

* Testes de Segurança, Vigilância e Monitoramento

Diante de incidentes ou situações anormais no ambiente de TI, muitas empresas são pegas de surpresa por não realizarem testes e monitoramentos previamente nestes ambientes e acabam tendo maiores danos do que se já tivessem simulados situações parecidas antes. Esta atividade serve para garantir a implementação de segurança de TI seja testada e monitorada antecipadamente. O armazenamento de *logs* e monitoramento dos mesmos ajudam na prevenção ou detecção prematura de atividades incomuns e que precisem ser tratadas. A fim de garantir que o nível de segurança aprovado seja mantido, é importante que a segurança de TI seja revalidada com periodicidade. [9]

* Definição de Incidente de Segurança

Definir claramente as características de incidentes de segurança em potencial que podem ser tratados adequadamente pelos processos de gestão de incidentes e gestão de problemas, comunicando esta definição para as partes interessadas. [9]

* Proteção da Tecnologia de Segurança

Garantir que as tecnologias de segurança sejam invioláveis e que as documentações não sejam reveladas desnecessariamente. [9]

* Gestão de Chave Criptográfica

A fim de proteger contra modificação e ou revelação pública não autorizada de chave, é importante que seja definido políticas e procedimentos de geração, mudança, revogação, destruição, distribuição, certificação, armazenamento, inserção, utilização e arquivamento das chaves criptográficas. [9]

* Prevenção, Detecção e Correção de Software Malicioso

Garantir que medidas preventivas, corretivas e de detecção, como correções de segurança (*patches*) e controles de vírus, sejam estabelecidas a nível corporativo a fim de proteger os sistemas de informação e tecnologias contra *malwares* (vírus, *worms, spywares, spam*). [9]

* Segurança de Rede

É necessário que técnicas de segurança e procedimentos de gestão sejam utilizadas a fim de autorizar apenas o acesso de usuários permitidos e controlar o fluxo externo com o interno da rede. Para isso, é necessária a utilização de ferramentas como firewall, aplicativos de segurança, segregação de rede e de funções e detecção de intrusões, ou seja, através destas técnicas e procedimentos esta atividade deve garantir a segurança da rede.[9]

* Comunicação de Dados Confidenciais

Garantir que o fluxo de informações confidenciais transite por caminho confiável ou controlado de modo a fornecer autenticação de conteúdo, comprovação de envio e recebimento e não-rejeição de origem. [9]

Mas de nada adianta ter políticas, procedimentos, padrões de segurança criados e formalizados que garantem a integridade dos recursos de TI, se as pessoas que operacionalizam certas atividades não possuem conhecimento adequado sobre segurança da informação. Estas precisam de um treinamento eficaz para fazer uso efetivo e eficiente das soluções tecnológicas, reduzindo assim, erros de usuário e aumentando a conformidade com as políticas e procedimentos definidas pela organização, especialmente as que se referem a segurança de informação.

Ao se investir em parques tecnológicos, não se pode deixar de lado o fator humano. A engenharia social explora essa vulnerabilidade. Em Segurança da informação, chama-se Engenharia Social a prática de extrair informações confidenciais ou sigilosas de um determinado ambiente ou sistema utilizando técnicas de persuasão. Dessa forma, além da conscientização e treinamento, as empresas devem possuir um plano de contingência para eventuais ataques e assim garantir a continuidade dos negócios. [11]

# Outros Referenciais Metodológicos

## ITIL

O ITIL foi desenvolvido pela agência central de computação e telecomunicações do Reino Unido (CCTA) a partir do início dos anos 80 e este modelo de gestão é um dos mais adotados pelas organizações. O ITIL é um modelo público que define as melhores práticas a serem aplicadas uniformemente pelas diferentes vertentes que compõem a gerência de TI. Cada módulo do ITIL define uma biblioteca de práticas para melhorar a eficiência de TI, reduzindo os riscos e aumentando a qualidade dos serviços e o gerenciamento de sua infra-estrutura. Entre suas várias disciplinas, o ITIL define um modelo de gerenciamento de Segurança da Informação. Na perspectiva do ITIL, os controles pertinentes são centralizados nos processos de gerenciamento de segurança da informação. Por conta disso, este modelo de gestão prega que as outras disciplinas do conjunto devem adotar técnicas de segurança dentro de seus processos. O ITIL muda a perspectiva das corporações, que passam a enxergar segurança atrelada a outras áreas de negócio. Dessa forma, cada unidade tem a responsabilidade de desenvolver seus processos pensando em segurança. [12]

## PMBOK

O Project Mangement Body of Knowledge – PMBoK – é uma metodologia que consiste em um conjunto de conhecimentos em gerenciamento de projetos, desenvolvido pelo PMI – Project Management Institute - uma organização internacional sem fins lucrativos que reúne profissionais da área de gerência de projeto. O PMI promove a ampliação do conhecimento existente sobre gerenciamento de projeto, bem como melhora o desempenho e *expertise* dos profissionais e organizações da área. No manual do PMBoK são descritos as habilidades e ferramentas técnicas para gerenciamento de um projeto. Por este motivo, muitas empresas consideram adequada a utilização do PMBoK para o planejamento e gerenciamento da implantação de normas de segurança, como a ISO 27002, de forma satisfatória na maioria das empresas. O PMBOK propõe que o gerenciamento de projetos compreende cinco processos – Início, Planejamento, Execução, Controle e Fechamento, bem com nove áreas de conhecimento, que caracterizam os principais aspectos envolvidos em um projeto e no seu gerenciamento: Integração, escopo, tempo, custo, qualidade, recursos humanos, comunicação, análise de risco e aquisição. [13]



Figura 4 – Áreas de conhecimento do PMBOK

## ISO 27001 e ISO 27002

A ISO 27001 e ISO 27002 são normas internacionais que possibilitam as organizações a implementação de um Sistema de Gerenciamento da Informação (SGSI), através do estabelecimento de uma política de segurança, controles e gerenciamento de riscos. Elas contemplam:

### ISO 27001 – Information Security Management Systems Requirement

Esta norma foi publicada em outubro de 2005 e substituiu a norma BS 7799-2. Esta norma pode ser aplicada a todos os tipos de organizações (por exemplo, empreendimentos comerciais, agências governamentais, organizações sem fins lucrativos) e propõe um modelo robusto para direcionar a análise/avaliação de riscos, especificação e implementação de segurança, gerenciamento de segurança e reavaliação. Ela indica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto dos riscos de negócio globais da organização. Além disso, especifica requisitos para a implementação de controles de segurança personalizados para as necessidades individuais de organizações ou suas partes. [14]

O SGSI é projetado para assegurar a seleção de controles de segurança adequados e proporcionados para proteger os ativos de informação e propiciar confiança às partes interessadas.

### ISO 27002 – Code of Practice for Information Security Management

Anteriormente, esta norma era conhecida como ISO 17799, mas a partir de 2007, foi incorporado um novo sistema de numeração e passou a ser conhecida por ISO 27002. A ISO 27002 tem por objetivo estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Em outras palavras, significa que esta norma assegura que as informações que são consideradas importantes para a continuidade e manutenção dos objetivos do negócio estarão protegidas. [15]

#  Esta norma encontra-se distribuídas em 11 seções que correspondem aos controles de segurança da informação. São elas:

* Seção 5 – Política de Segurança da Informação

Definição e formalização de uma política de segurança da informação da organização e sua devida divulgação a todos. Esta política deve ser revisada criticamente em períodos regulares de tempo.

* Sessão 6 – Organizando a segurança da Informação

Estabelecimento de uma estrutura para gerenciamento para a implantação de segurança da informação em uma organização. Para isso, é necessário que as atividades de segurança da informação sejam coordenadas por representantes de diversas partes da organização, com funções e papéis relevantes.

* Sessão 7 – Gestão de Ativos

Esta norma prega proteger todos os ativos da organização, e de acordo com a ISO 27002, ativo é considerado qualquer coisa que tenha valor para a organização.

* Seção 8 – Segurança em Recursos Humanos

No ato da contratação de um novo funcionário, é necessário que o mesmo entenda quais são suas responsabilidades, especialmente no que tange às responsabilidades de segurança da informação. A intenção é mitigar o risco de roubo, fraude ou mau uso dos recursos.

* Seção 9 – Segurança Física e do Ambiente

As instalações de processamento de informações críticas ou sensíveis devem ser mantidas em áreas seguras, com níveis de controle de acesso apropriados.

* Seção 10 – Gestão das Operações e Comunicações

Definição dos procedimentos e responsabilidades pela gestão e operação de todos os recursos de processamento das informações. Visando o risco de mau uso ou uso indevido dos sistemas, é importante, sempre que possível, realizar segregação de funções.

* Seção 11 – Controle de Acesso

Deve haver um controle sobre o acesso às informações, aos recursos e aos processos de negócio, baseado nos requisitos do negócio e na segurança da informação.

* Seção 12 – Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

Antes do desenvolvimento e implementação dos requisitos de segurança dos sistemas de informação, é necessário que estes sejam identificados e acordados antes. Visando a manutenção da confidencialidade, autenticidade e integridade das informações é essencial que elas estejam protegidas.

* Seção 13 – Gestão de Incidentes de Segurança da Informação

A fim de que eventos de segurança da informação sejam mais brevemente possíveis comunicados, devem ser estabelecidos procedimentos formais que assegurem que tomada de ação corretiva ocorra em tempo hábil.

* Seção 14 – Gestão da Continuidade do Negócio

Devem ser estabelecidos planos de continuidade de negócio, incluindo controles para identificar e reduzir os riscos, de modo a impedir a parada das atividades de negócio contra falhas ou desastres significativos.

* Seção 15 – Conformidade

Deve-se estar em conformidade com todas as leis e estatutos, regulamentações ou obrigações contratuais de quaisquer requisitos de segurança da informação.

A adoção destes frameworks por organizações de TI variam de escala. Empresas de maior porte, de determinado segmento, com um nível de complexidade do negócio maior necessitam de maior formalidade quanto a implementação de processos e seus controles. Analisando as práticas de segurança que estes frameworks sugerem, é notável que, muito provavelmente, a organização terá sucesso na sua gestão de segurança da informação, entretanto se forem ignorados, a empresa é colocada em risco. Para aquelas organizações de pequeno porte que não possuem investimento suficiente para realizar em segurança da informação, cabe a ela dar prioridades naqueles controles mais críticos e criar outros controles compensatórios que mitiguem completamente riscos de alta criticidade.

# Recomendações

Sendo a informação considerada um ativo de uma empresa, a segurança deve fazer parte de sua gestão. Dessa maneira, ignorar os riscos não os faz deixar de existir. Cada vez mais as organizações se tornam dependentes das informações contidas em seus sistemas de informação, mas para que estas informações estejam realmente seguras e não estejam expostas a riscos é necessário que os processos de negócio (entre os quais os de gestão de SI) e os recursos de SI envolvidos (pessoas, aplicações, tecnologias, etc) também estejam em conformidade com as boas práticas de TI. Abaixo, estão listadas algumas recomendações sugeridas para as organizações melhorarem a segurança sobre suas informações:

## Adoção de um ou uma combinação de referenciais metodológicos

As melhores práticas a serem implantadas e praticadas pelas empresas podem estar baseadas na combinação de referenciais metodológicos consagrados e reconhecidos internacionalmente, como o CobiT, ITIL, PMBoK, ISO 27001 e ISO 27002. Sendo o CobiT, o referencial mais direcionado a atividades relacionadas com auditoria de sistemas e as ISOs (ISO 27001 e ISO 27002) sendo normas relacionadas as conformidades de segurança da informação que atendem aos requisitos de Auditoria de SI, é bastante interessante que as empresas combinem estes referenciais com os outros citados anteriormente a fim de que o ambiente de TI possa estar o mais robusto e seguro possível. Como os pareceres de auditoria de sistemas estão alinhados com estas boas práticas de TI, uma organização que atende aos requisitos propostos nestes referenciais, conseqüentemente atenderá aos requisitos de autoria e ainda estarão com as suas informações íntegras, disponíveis, geridas por pessoas capacitadas e com seu parque tecnológico assegurado e confiável. .

## Criação de uma área de Auditoria Interna na organização

Com a finalidade de garantir que as boas práticas estão sendo seguidas, é aconselhado a criação de um departamento de auditoria interna na organização que será independente no seio da empresa e que se reportará diretamente com a direção. Este departamento seria encarregado de revelar as fraquezas, determinar as causas, avaliar as conseqüências e encontrar uma solução de modo a convencer os responsáveis a agir. Tudo isso sendo feito através verificação da existência, suficiência e aplicação dos controles internos e, quando necessário, aperfeiçoamento destes. Em suma, este departamento seria o responsável por atender às expectativas da alta administração sobre os maiores riscos que a empresa pode estar exposta, sendo estes bastante relacionados à segurança da informação, e então implantar ações corretivas necessárias para mitigar estes riscos. [17].

## Aumento de investimento em TI

Mas para que as empresas garantam um ambiente onde as informações são confiáveis, é necessário investimentos que sejam condizentes com a sua evolução. Segundo pesquisa realizada nos Estados Unidos em 2002 pela revista Information Secutiry, os investimentos em segurança não acompanham o crescimento das empresas. A maioria das empresas ainda não considera a segurança das suas informações um investimento prioritário, embora, curiosamente, dependam dela para operar e sobreviver. Investir em segurança é mais que simplesmente justificar seus custos frente aos prejuízos causados pelos incidentes que ela evita. É necessário que as organizações tenham consciência que investimento em segurança não traz retorno sobre investimento (ROI), ou seja, não trazem benefícios financeiros, mas reduzem a exposição da empresa a eventos que poderiam trazer grandes prejuízos. Infelizmente, a maioria das organizações investe em segurança da informação gastando seu orçamento em medidas corretivas, ao invés de aplicarem em medidas preventivas e estratégicas. [18].

Sendo assim, esta recomendação também é importante para que as organizações passem a mudar esse ponto de vista e ajam de maneira proativa para que situações indesejadas não ocorram. Essa mudança de ponto de vista pode ser iniciada com a avaliação do parecer de auditoria, verificação dos controles falhos ou inexistentes e, se for o caso, implementação de dos referenciais metodológicos acima citados.

# Conclusão e Trabalho Futuros

## Conclusão

Não há dúvidas que a tecnologia aplicada aos negócios traz bastantes benefícios. Entretanto, as organizações devem compreender e controlar os riscos associados à utilização das novas tecnologias.

Este trabalho procurou mostrar a importância da segurança da informação para as empresas, frente a uma nova realidade de um mundo globalizado, inter-relacionando este tema com o processo de auditoria de sistemas. Podemos dizer que estes conceitos são interdependentes, uma vez que um depende do outro para produzirem efeitos desejáveis pela alta administração, ou seja, a confiabilidade das informações financeiras [8].

Enquanto que a segurança deve garantir a integridade das informações, a auditoria de sistemas deve garantir que estas informações estejam realmente íntegras (uma vez que a auditoria tem como verificar se os requisitos para segurança da informação estão implementados satisfatoriamente) proporcionando um processamento ideal para obter os resultados esperados [14].

Para compreender e contextualizar melhor auditoria de sistemas, iniciei este trabalho apresentando o conceito de auditoria contábil, uma vez que esta tem por objetivo examinar as demonstrações financeiras dentro de um determinado período, a fim de verificar se as mesmas estão de acordo com os princípios da contabilidade. Como, diante do contexto atual, grande parte destas informações está armazenada e é processada em sistemas, é necessário garantir que estas informações estejam obedecendo três princípios básicos da segurança da informação: integridade, confidencialidade e disponibilidade. Foi dentro deste contexto que segui o propósito do trabalho, apresentado o conceito de auditoria de sistemas da informação.[5]

Diante disto, foi destacado o valor da informação e a importância que ela exerce para as decisões estratégicas da empresa e, conseqüentemente, diante deste bem tão precioso é necessário que haja segurança. Daí, apresentei referenciais metodológicos que auxiliam que estes dados estejam seguros e em conformidade com as boas práticas de segurança da informação, onde estas práticas são avaliadas em um processo de auditoria de sistemas.

Por fim, fiz recomendações sobre o tema abordado a fim de atingir o objetivo da monografia que é “destacar para as organizações, a importância da Segurança da Informação em uma Auditoria de Sistemas, cujo o papel é imprescindível para garantir a confiança dos seus dados financeiros”.

## Trabalhos Futuros

Os controles gerais de TI (são aqueles inseridos nos processos de TI) estão distribuídos em 4 domínios, são eles:

* Desenvolvimento de sistemas
* Gerenciamento de mudanças
* Segurança
* Operação de computadores

Dado que neste trabalho, foi abordado o domínio de segurança, fica uma sugestão para em trabalhos futuros aprofundarem mais nos controles pertencentes aos outros domínios. O intuito de cada um destes domínios é:

* Desenvolvimento de sistemas – assegurar que os sistemas são desenvolvidos, configurados e implementados de modo a alcançar seus objetivos de controle, ou seja, garantir que os sistemas que são desenvolvidos funcionam realmente como necessários.
* Gerenciamento de mudanças – Garantir que as mudanças relacionados com programas e componentes de infra-estrutura são solicitadas, autorizadas, realizadas, testadas e implementadas para obter seus objetivos de controle funcionando adequadamente.
* Operação de computadores – assegurar que os sistemas em produção são processados completamente e com o valor correto de acordo com seus objetivos de controle, e que os problemas encontrados estejam identificados e resolvidos completamente e com o valor correto, a fim de manter a integridade das informações.

# Referências Bibliográficas

x

|  |  |
| --- | --- |
| 1. | VINAGRE, M. D. F. M. A Importância da Evidência em Auditoria, João Pessoa, 2004. |
| 2. | CREPALDI, S. A. Contabilidade - Auditoria: Origem, evolução e desenvolvimento da auditoria. **netlegis**, 2006. Disponivel em: <http://www.netlegis.com.br/indexRC.jsp?arquivo=/detalhesDestaques.jsp&cod=8157>. Acesso em: 20 Outubro 2011. |
| 3. | CÉZAR, P.; SILVA, D.; FERNANDES, F. A Mulher Contabilista: Participação e perfil das profissionais que atuam nas empresas de auditoria independente do Distrito Federal, São Paulo, Fevereiro 2007. |
| 4. | CÓDIGO e Ética e Conduta da Auditoria Interna Sistema SEBRAE. **auditoriasebrae**, 2009. Disponivel em: <http://auditoriasebrae.files.wordpress.com/2009/08/gestao-de-risco.pdf>. Acesso em: 04 Novembro 2011. |
| 5. | NIÉLI, A. et al. Fundamentos da auditoria: uma abordagem analítica. **netlegis**, 2011. Disponivel em: <http://www.netlegis.com.br/indexRC.jsp?arquivo=detalhesArtigosPublicados.jsp&cod2=574>. Acesso em: 28 Setembro 2011. |
| 6. | CARLOS, E.; CANDIDO, A. O Parecer dos Auditores Independentes sobre Demonstrações Contábeis: uma abordagem sobre o parecer-padrão,atualmente em vigor no Brasil. **Revista Administração On Line**, v. 5, n. 3, p. 26-38, Agosto 2004. |
| 7. | PRINCÍPIOS da Materialidade. **thinkfn**, 2009. Disponivel em: <http://www.thinkfn.com/wikibolsa/Princ%C3%ADpio\_da\_materialidade>. Acesso em: 07 Outubro 2011. |
| 8. | AURELIO, M. GESTÃO DE SEGURANÇA DA INFORMAÇÃO, 01 Junho 2005. 96-99. |
| 9. | RAFAEL, M.; SQUINZANI, T. Auditoria dos Sistemas de Informação Aliada à Gestão Empresarial. **Revista Contábeis**, Santa Maria , Outubro 2088. |
| 10. | ISACA, C. **CobiT 4.1**. ISACA. [S.l.], p. 1-200. 2007. |
| 11. | ANTONIO, M.; TONIZETTI, J. ENGENHARIA SOCIAL - Um perigo eminente, Florianópolis, 2008. |
| 12. | GOVERNANÇA de TI: comparativo entre CobiT e ITIL. **trainning**. Disponivel em: <http://www.trainning.com.br/download/Apostila\_ITIL\_Cobit.pdf>. Acesso em: 08 Novembro 2011. |
| 13. | O EMPREGO DA METODOLOGIA PMBOK PARA SUBSIDIAR A IMPLANTAÇÃO DA NORMA DE SEGURANÇA DA INFORMÇÃO ISO17799, Florianópolis, 25 Outubro 2002. |
| 14. | ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems - Requirements. **iso27001security**, 2011. Disponivel em: <http://www.iso27001security.com/html/27001.html>. Acesso em: 20 Novembro 2011. |
| 15. | ISO/IEC 27002:2005 Information Technology - Security Techniques - Code of practices for information security management. **iso27001security**, 2011. Disponivel em: <http://www.iso27001security.com/html/27002.html>. Acesso em: 20 Novembro 2011. |
| 16. | MANUEL, P. A Função Auditoria de Sistemas de Informação: Modelo Funcional e de Competências, Braga, Setembro 2007. 153-163. |
| 17. | MARTINS, I.; MORAIS, G. AUDITORIA INTERNA - Função e Processo. **ipv**, 1999. Disponivel em: <http://www.ipv.pt/millenium/ect13\_3.htm>. Acesso em: 27 nov. 2011. |
| 18. | FAUSTINI, R. SEGURANÇA É INVESTIMENTO? **faustiniconsulting**. Disponivel em: <http://www.faustiniconsulting.com/artigo10.htm>. Acesso em: 27 Novembro 2011. |