

**UNIVERSIDADE DE BRASÍLIA - UnB  
FACULDADE DE TECNOLOGIA - FT  
DEPARTAMENTO DE ENGENHARIA ELÉTRICA - ENE**

**MODELO INTEGRADO PARA AVALIAÇÃO DE RISCOS DA  
SEGURANÇA DE INFORMAÇÃO EM AMBIENTE  
CORPORATIVO**

**CÉSAR SILVÉRIO MORALES**

**ORIENTADOR: FLÁVIO ELIAS GOMES DE DEUS**

**DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA**

**PUBLICAÇÃO: PPGENE.DM – 070/010**

**BRASÍLIA / DF: SETEMBRO/2010**

**UNIVERSIDADE DE BRASÍLIA  
FACULDADE DE TECNOLOGIA  
DEPARTAMENTO DE ENGENHARIA ELÉTRICA**

**MODELO INTEGRADO PARA AVALIAÇÃO DE RISCOS DA  
SEGURANÇA DE INFORMAÇÃO EM AMBIENTE  
CORPORATIVO**

**CÉSAR SILVÉRIO MORALES**

DISSERTAÇÃO DE MESTRADO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE PROFISSIONAL EM ENGENHARIA ELÉTRICA.

APROVADA POR:

---

**FLAVIO ELIAS GOMES DE DEUS, Doutor, UnB  
(ORIENTADOR)**

---

**RAFAEL TIMÓTEO DE SOUSA JUNIOR, Doutor, UnB  
(EXAMINADOR INTERNO)**

---

**ROBSON DE OLIVEIRA ALBUQUERQUE, Doutor, ABIN  
(EXAMINADOR EXTERNO)**

---

**DATA: BRASÍLIA/DF, 30 DE SETEMBRO DE 2010.**



## FICHA CATALOGRÁFICA

MORALES, CESAR SILVERIO  
MODELO INTEGRADO PARA AVALIAÇÃO DE RISCOS DA SEGURANÇA DE INFORMAÇÃO EM  
AMBIENTE CORPORATIVO [Distrito Federal] 2010.  
xxviii., 167 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2010).

Dissertação de Mestrado – Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica.

1. Gestão de Riscos 2. Segurança de Informação  
3. Monitoramento Contínuo

I. ENE/FT/UnB. II. Título (Série)

## REFERÊNCIA BIBLIOGRÁFICA

MORALES, C. S. (2010). Modelo integrado para avaliação de riscos da segurança de informação em ambiente corporativo. Dissertação de Mestrado, Publicação PPGENE.DM - 070/10, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 167 p.

## CESSÃO DE DIREITOS

NOME DO AUTOR: César Silvério Morales

TÍTULO DA DISSERTAÇÃO: Modelo integrado para avaliação de riscos da segurança de informação em ambiente corporativo.

GRAU/ANO: Mestre/2010.

É concedida à Universidade de Brasília permissão para reproduzir cópias desta Dissertação de Mestrado e para emprestar ou vender tais cópias somente para propósitos acadêmicos e científicos. Do mesmo modo, a Universidade de Brasília tem permissão para divulgar este documento em biblioteca virtual, em formato que permita o acesso via redes de comunicação e a reprodução de cópias, desde que protegida a integridade do conteúdo dessas cópias e proibido o acesso a partes isoladas desse conteúdo. O autor reserva outros direitos de publicação e nenhuma parte deste documento pode ser reproduzida sem a autorização por escrito do autor.

---

César Silvério Morales (csmorales@hotmail.com)  
Campus Universitário Darcy Ribeiro – Asa Norte  
CEP 70910-900 – Brasília – DF - Brasil



## DEDICATÓRIA

*À minha mãe e meu pai que com toda a  
dedicação deram significado a minha vida,  
minha esposa e  
minha linda filha Manuela.*



## AGRADECIMENTOS

A Deus pela saúde, disposição, discernimento e oportunidades que proporcionou, as portas que abriu e também aquelas que fechou para aprendizado e crescimento. Obrigado porque tudo que sou, o que tenho e o que vier a ser e a ter.

Aos meus pais Ana Gláucia e Lutgardo (em memória) que através dos seus exemplos me ensinaram a perseverar, enfrentar os obstáculos da vida com determinação, humildade e principalmente temor a Deus. Palavras não seriam suficientes para expressar a admiração, orgulho e agradecimento por tudo que passamos, conquistamos e superamos juntos.

À minha esposa Flávia que tem estado ao meu lado em todos os momentos alegres e difíceis, dando o suporte necessário sempre que precisei.

À minha filha Manuela, que me ensinou o grande significado de ser pai e que é uma fonte de inspiração, alegria e amor para vencer os desafios e conquistar mais um sonho da minha vida.

Ao corpo docente da Universidade de Brasília, em especial ao meu orientador Prof. Dr. Flávio Elias Gomes de Deus e co-orientador Laerte Peotta, que pacientemente dedicaram seu tempo, compartilharam conhecimento, contribuíram para o desenvolvimento deste trabalho e o meu como pesquisador.





## **RESUMO**

### **MODELO INTEGRADO PARA AVALIAÇÃO DE RISCOS DA SEGURANÇA DA INFORMAÇÃO EM AMBIENTE CORPORATIVO**

**Autor: César Silvério Morales**

**Orientador: Flávio Elias de Deus**

**Programa de Pós-graduação em Engenharia Elétrica**

**Brasília, setembro de 2010**

No ambiente de competição acirrada em que é necessária a flexibilidade, inovação e agilidade na implementação de soluções tecnológicas para satisfação dos clientes, redução de custos, aumento de receita e atendimento à exigências legais, é essencial implementar um ambiente com mecanismos de controle para proteger a informação e assegurar a integridade, confidencialidade e disponibilidade dos dados. Porém, a segurança da informação não pode custar mais que o benefício proporcionado ou expor a riscos que a organização não deseja tolerar. Para tanto, uma avaliação periódica deve ser realizada para que ações sejam tomadas pelos executivos da organização com base em informações claras, concisas e suficientes. Neste contexto, este trabalho propõe um método para monitoramento contínuo dos riscos e controles de segurança da informação, baseado em estudos das boas práticas descritas nas estruturas de trabalho CobiT e ITIL, normas ISO 27002, NIST 800-53, possibilitando a detecção de atitudes indevidas que podem acarretar em perdas financeiras, custos excessivos, prejuízo a imagem da companhia e até a continuidade dos negócios. Além disso, permitirá que a administração tenha a oportunidade de decidir sobre o que fazer e o que não fazer com os riscos residuais, evitando inclusive um direcionamento equivocado de investimentos ou a falta dele em recursos e processos.



## **ABSTRACT**

### **MODEL INTEGRATED FOR RISKS EVALUATION OF INFORMATION SECURITY ON CORPORATE ENVIRONMENT**

**Autor: César Silvério Morales**

**Supervisor: Flávio Elias de Deus**

**Programa de Pós-graduação em Engenharia Elétrica**

Brasília, september 2010

On an aggressive competition environment that requires flexibility, innovation and agility to implement technology solutions to ensure customer satisfaction, reduce costs, increase income and comply with legal requirements, it is essential to implement an environment with control mechanisms to protect information and ensure data integrity, confidentiality and availability. However, information security can not cost more than the obtained benefits or expose to risks which the organization does not wish to tolerate. Therefore, a periodic assessment should be made so that actions taken by the executives of the organization are based on clear, concise and sufficient information. In this sense, this dissertation proposes a method for continuous monitoring of risks and information security controls, based on the study of best practices described on CobiT and ITIL frameworks, ISO 27002 and NIST 800-53 standards, allowing the detection of misbehavior or mistakes which could lead to financial loss, excessive cost, image damage and ultimately business disruption. In addition, it will allow senior management to have an opportunity to decide whether or not take actions to mitigate residual risks, avoiding mistakes related to investments in resources and processes.

## SUMÁRIO

<b>1. Introdução .....</b>	<b>1</b>
1.1. Problema de Pesquisa .....	1
1.2. Hipótese .....	2
1.3. Objetivo geral .....	2
1.4. Estrutura do trabalho .....	3
<b>2. Segurança da Informação Corporativa .....</b>	<b>5</b>
2.1. Informações gerais sobre vulnerabilidades e ameaças de segurança da informação .....	7
2.2. Conceitos de Proteção da informação .....	9
2.3. Governança Corporativa .....	10
2.4. Governança de Tecnologia da Informação .....	12
2.5. Governança de Segurança da Informação .....	13
2.6. Gerenciamento de Riscos .....	14
<b>3. Visão geral das Estruturas de trabalho .....</b>	<b>22</b>
3.1. Premissa para as comparações dos processos .....	23
3.2. COBIT .....	24
3.3. ITIL .....	32
3.4. ISO 27001 e 27002 .....	36
3.5. NIST .....	40
3.6. Considerações sobre as análises individuais das estruturas de trabalho e normas .....	44
<b>4. Proposta de modelo para avaliação de riscos da segurança da informação .....</b>	<b>46</b>
4.1. Definição da matriz de riscos e controles unificada .....	46
4.2. Avaliação dos riscos identificados .....	50
4.3. Métricas e indicadores para o modelo de monitoramento contínuo .....	58
4.4. Identificação dos controles chaves .....	60
4.5. Definição dos Indicadores e Métricas .....	64
4.6. Critérios para Avaliação dos controles .....	78
4.7. Proposta do Modelo de Monitoramento Contínuo .....	79
<b>5. Conclusão .....</b>	<b>89</b>
<b>Referências bibliográficas .....</b>	<b>92</b>
<b>Anexos .....</b>	<b>98</b>

ANEXO A – Matriz de Riscos e Controles para o CobiT.....	98
ANEXO B – Matriz de Riscos e Controles para o ITIL.....	105
ANEXO C – Matriz de Riscos e controles para a ISO 27002.....	111
ANEXO D – Matriz de Riscos e controles para o NIST SP800-53 .....	123
ANEXO E – Seleção das atividades de controle da Matriz unificada.....	130
ANEXO F – Relação das atividades de controle substituídas por outras similares .....	132
ANEXO G – Questionário x riscos de segurança da informação .....	136
ANEXO H – Respostas da Pesquisa de avaliação de riscos.....	140
ANEXO I – Análise das respostas da pesquisa com desvio padrão superior a 10%.....	143
ANEXO J – Classificação dos Riscos de acordo com a pesquisa.....	145
ANEXO K – Controles Chaves selecionados.....	147

## LISTA DE TABELAS

Tabela 3. 1 – Quadro Resumo dos Riscos e Controles CobiT .....	30
Tabela 3. 2 – Relacionamento dos Processos CobiT com os do ITIL (IT GOVERNANCE INSTITUTE, 2008) .....	35
Tabela 3. 3 – Relacionamento dos Processos CobiT com requerimentos da ISO 27002 (IT GOVERNANCE INSTITUTE, 2006).....	38
Tabela 3. 4 – Relacionamento dos Processos CobiT com requerimentos do NIST 800-53 (IT GOVERNANCE INSTITUTE, 2007).....	43
Tabela 3. 5 – Quadro resumo das atividades de controles por boa prática .....	44
Tabela 4. 1 – Integração entre os modelos CobiT, ITIL, ISO 27002 e NIST 800-53.....	48
Tabela 4. 2 – Avaliação de riscos - dados de pesquisa e histórico de incidentes.....	55
Tabela 4. 3 – Métricas o desalinhamento dos objetivos de negócio .....	64
Tabela 4. 4 – Métricas para descumprimento das regras de segurança da informação.....	65
Tabela 4. 5 – Métricas para Plano de segurança incompatível com a infraestrutura tecnológica .....	66
Tabela 4. 6 – Métricas para impossibilidade de atribuição de responsabilidades.....	67
Tabela 4. 7 – Métricas para privilégios de acesso inadequados.....	68
Tabela 4. 8 – Métricas para contas de usuário inválidas ou fictícias .....	69
Tabela 4. 9 – Métricas para ausência de monitoramento de riscos .....	69
Tabela 4. 10 – Métricas para incidentes de segurança não detectados .....	70
Tabela 4. 11 – Métricas para inadequada proteção das ferramentas de segurança .....	72
Tabela 4. 12 – Métricas para mecanismos de não-repúdio .....	74
Tabela 4. 13 – Métricas para instalação e uso de softwares maliciosos.....	75
Tabela 4. 14 – Métricas para invasão do ambiente tecnológico por agentes externos.....	76
Tabela 4. 15 – Métricas para transações inválidas com parceiros de negócio .....	77
Tabela 4. 16 – Atividades para definição e implementação do monitoramento contínuo .....	81

## LISTA DE FIGURAS

Figura 2. 1 – O cubo do COSO (COSO, 2007).....	16
Figura 2. 2 – Componentes de Cenário de Risco (IT GOVERNANCE INSTITUTE, 2009)..	19
Figura 3. 1 – O cubo do CobiT (IT GOVERNANCE INSTITUTE, 2007) .....	24
Figura 3. 2 – Visão Geral do Framework CobiT (IT GOVERNANCE INSTITUTE, 2007) ..	26
Figura 3. 3 – Visão Geral do Framework ITIL (Office Government Commerce, 2007).....	33
Figura 3. 4 – Modelo PDCA aplicado aos processos da norma 27001 (ABNT, 2006) .....	37
Figura 4. 1 – Composição do Modelo Unificado .....	47
Figura 4. 2 – Distribuição em categorias de controle em quantidades.....	48
Figura 4. 3 – Etapas de seleção das atividades de controles .....	49
Figura 4. 4 – Avaliação dos riscos com base nas respostas dos questionários .....	52
Figura 4. 5 – Amostra das Respostas dos questionários .....	53
Figura 4. 6 – Histórico – Quantidade de Incidentes .....	54
Figura 4. 7 – Quadrante de Riscos – Avaliação de Riscos Inerentes .....	57
Figura 4. 8 – Processo para identificação dos controles chaves.....	63
Figura 4. 9 – Solução proposta de monitoramento contínuo.....	81
Figura 4. 10 – Monitoramento dos Processos de Segurança da Informação.....	85
Figura 4. 11 – Monitoramento dos Riscos de Segurança da Informação.....	87
Figura 4. 12 – Métricas do Risco de Impossibilidade de atribuição de responsabilidades .....	87
Figura 4. 13 – Gráfico das medições dos riscos ao longo do tempo .....	88





## **LISTA DE SÍMBOLOS, NOMENCLATURA E ABREVIACÕES**

COBIT	Control Objectives for Information and related Technology
ITIL	Information Technology Infrastructure Library
ISACA	Information Systems Audit and Control Association
THEIIA	The Institute of International Auditors
NIST	National Institute of Standards and Technology
ITGI	Information Technology Governance Institute
IT	Information Technology
ISO	International Organization for Standardization
GRC	Gestão de Riscos Corporativos
COSO	Committee of Sponsoring Organizations of the Treadway Commission
DNS	Domain Name Systems
IP	Internet Protocol
DHCP	Dynamic Host Configuration Protocol
ISP	Internet Service Provider
VPN	Virtual Private Network
PMBOK	Project Management Body Knowledge
PCAOB	Public Company Accounting Oversight Board
RITI	Riscos de Tecnologia da Informação
CTTI	Controles de Tecnologia da Informação

# 1. INTRODUÇÃO

A tendência global do mercado, baseado na pesquisa da consultoria Gartner<sup>1</sup>, tem sido a implementação de uma infraestrutura tecnológica flexível e moderna, que dê suporte a oferta de serviços e produtos convergentes e inovadores, com objetivo de fidelizar o cliente, bem como reduzir despesas operacionais.

É necessário que os processos da empresa que proporcionam a Segurança da Informação, estejam alinhados e interligados no mesmo contexto para que a estratégia da organização de aumentar receita e ou reduzir custos, sejam implementados com a agilidade e qualidade requerida para satisfação do cliente e da alta administração sem comprometer a integridade, confidencialidade e disponibilidade dos dados.

No entanto, a segurança de informação em muitos casos, não acompanha na mesma velocidade as definições e estratégias do negócio. Neste sentido, surge a necessidade de medir de forma tempestiva e periódica o nível de implementação da segurança para prover a alta administração informações relevantes que demonstrem a exposição ao risco e proporcione de forma mais assertiva a tomada de decisão pela alta administração.

## 1.1. PROBLEMA DE PESQUISA

As grandes corporações, com o desafio de conquistar fatias de mercado, aproveitar a demanda existente através de fusões e incorporações com outras empresas, bem como a implementação de soluções inovadoras, aberturas de novos canais de vendas, como por exemplo, o e-commerce, adequação a legislação como o caso do Sistema Público de Escrituração Digital<sup>2</sup>, acabam em muitas situações aumentando o risco de vazamento de informações, perda da integridade dos dados por deixar a questão de segurança de informação para um segundo plano.

---

<sup>1</sup> <http://cio.uol.com.br/tecnologia/2010/02/05/nove-tendencias-de-ti-para-os-proximos-cinco-anos/>

<sup>2</sup> A Escrituração Fiscal Digital - EFD é um arquivo digital, que se constitui de um conjunto de escriturações de documentos fiscais e de outras informações de interesse dos fiscos das unidades federadas e da Secretaria da Receita Federal do Brasil, bem como de registros de apuração de impostos referentes às operações e prestações praticadas pelo contribuinte.

Neste sentido, identificam-se os seguintes problemas a serem resolvidos:

Qual a metodologia a ser adotada para avaliação dos riscos de Segurança de Informação em um ambiente corporativo?

Que métricas e indicadores poderão ser adotados para avaliar o nível de exposição aos riscos de Segurança de Informação?

Como demonstrar à alta administração o nível de exposição aos riscos em tempo hábil para a tomada de decisão?

## **1.2. HIPÓTESE**

As estruturas de trabalho ITIL (Office Government Commerce, 2007) e CobiT (IT Governance Institute, 2008), além das Normas de Segurança ISO 27002 (ABNT, 2005) e NIST 800-53 (Ross, 2007) possuem recomendações de controles para mitigação dos riscos de Segurança da Informação que ao trabalhar de forma integrada possibilitam uma avaliação mais abrangente e completa dos processos na companhia que asseguram a confidencialidade, integridade e disponibilidade dos dados, atendendo as perspectivas de governança, ciclo de vida de serviços e requerimentos de segurança da informação.

A adoção do conceito de auditoria contínua para avaliação dos riscos e controles de segurança da informação através de métricas e indicadores possibilitará a medição periódica do nível de exposição da empresa e a divulgação dos resultados para a alta administração.

## **1.3. OBJETIVO GERAL**

Apresentar um modelo integrado para o Gerenciamento de Riscos de Segurança de Informação.

### **1.3.1. OBJETIVOS ESPECÍFICOS**

Avaliar as estruturas de trabalho ITIL (Office Government Commerce, 2007), CobiT (IT Governance Institute, 2008), NIST (Ross, 2007) e norma 27002 (ABNT, 2005) e identificar as etapas similares e complementares requeridas para o processo de Gerenciamento da Segurança de Informação.

Propor uma matriz para gerenciamento de riscos e controles do processo de Segurança de Informação com base nas melhores práticas descritas no CobiT, ITIL, Normas ISO 27002 e NIST 800-53.

Estabelecer indicadores e métricas para medição contínua dos riscos definidos na matriz proposta.

Definir um modelo para medição e divulgação dos indicadores e métricas para avaliação dos riscos da Gestão da Segurança de Informação utilizando o conceito de Auditoria Contínua.

## **1.4. ESTRUTURA DO TRABALHO**

A primeira parte do trabalho visa criticar a forma de avaliação de riscos relacionados à Segurança da Informação em um ambiente corporativo e a periodicidade que são providos a alta administração dados para tomada de decisões.

O Capítulo 2 contextualiza a Segurança da Informação no ambiente corporativo, demonstrando a importância deste processo, apresenta conceitos de governança, gerenciamento de riscos, formas de controles de mitigação e apetite ao risco, utilizado para tomada de ações pelas organizações.

O Capítulo 3 aborda as principais estruturas de trabalho utilizadas nas corporações para tratar as questões relativas à governança de TI, realiza uma revisão bibliográfica de

estudos sobre as estruturas de controles e analisa individualmente os processos e ou objetivos de controle de cada uma sobre Segurança da Informação.

O Capítulo 4 é o resultado da consolidação e unificação dos modelos de segurança avaliados, com a classificação dos riscos baseada em pesquisa com os principais gestores da companhia analisada e histórico de incidentes. Além disso, apresenta os conceitos sobre auditoria contínua, define as métricas propostas para medição de controles chaves para mitigação dos riscos e apresenta um modelo para monitoramento periódico dos riscos de segurança da informação.

O Capítulo 5 apresenta a conclusão deste trabalho e sua aplicação no mercado.

## 2. SEGURANÇA DA INFORMAÇÃO CORPORATIVA

Em plena era da informação, podemos descrevê-la como um bem, que como qualquer outro ativo importante para os negócios da companhia, tem valor para a organização e conseqüentemente necessita ser protegido (ABNT, 2005), não importando a forma pelo qual é compartilhada ou armazenada. (Westerman, 2008)

A informação pode ser escrita ou impressa em papel, armazenada eletronicamente, transmitida por correio ou meios eletrônicos, apresentada em filmes ou falada em conversas (ABNT, 2005, p. IX).

As ações adotadas para proteção dos dados dentro de uma organização são chamadas de segurança da informação que visa através de um conjunto de controles, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware, a proteção dos dados de qualquer circunstância ou evento que possa causar impacto nos negócios da companhia. O planejamento e a implementação é orientada pelos atributos de segurança caracterizada pela tríade:

- **Confidencialidade:** Garante que a informação estará disponível apenas para as pessoas autorizadas, visando proteger o sigilo e revelação indevida de informação (legal, reguladora, patenteada, confidencial).
- **Integridade:** Garante que as informações mantenham as características atribuídas pelo proprietário, de forma que não tenham sido modificados, acrescentados ou excluídos ao serem transportados ou armazenados.
- **Disponibilidade da informação:** Assegura que a informação esteja acessível para usuários autorizados no momento que esta seja necessária de acordo com os requisitos de negócio, leis, normas e regulamentações.

Além destas características, também são considerados os atributos de:

- Autenticidade: Determina a identidade de uma entidade (usuário, aplicação ou sistema) e confirma se é quem o ou que afirma ser.
- Não repúdio: Garante que o emissor de uma mensagem ou transação não negue a sua autoria.

A ausência de mecanismos de proteção adequados pode expor a organização a riscos de roubo de informação, manipulação de dados e indisponibilidade, podendo afetar a imagem da companhia e levá-la inclusive a falência. De fato, em junho de 2005, a CardSystems Solutions, empresa que realizava o processamento das transações de pagamentos para empresas de cartões de crédito, como Visa e Mastercard, revelou que pessoas desconhecidas haviam conseguido acesso não autorizado a informações de 40 milhões de titulares de cartão de crédito<sup>3</sup>. Este fato levou a rescisão de contratos e posterior venda da empresa.

A Boeing, empresa da área de construção de aeronaves, foi alvo de espionagem industrial<sup>4</sup> por um funcionário, que vendia segredos comerciais de programas aeroespaciais para o governo da China<sup>5</sup>. Já em 2009, a Telefónica, após várias reclamações de clientes sobre a dificuldade de utilizar o serviço de banda larga, foi a público informar que parte da sua infraestrutura que suportava o acesso a Internet de seus clientes tinha sido alvo de ações deliberadas de origem externa e por este motivo o serviço estava instável<sup>6</sup>.

Apesar de muitas empresas possuírem uma estrutura para cuidar da segurança de informação, um dos principais motivos que as leva sofrer esses tipos de ataque é a ausência de mecanismos suficientes para monitoramento e tratamento dos riscos (ERNST & YOUNG, 2010).

---

<sup>3</sup> <http://www.nytimes.com/2005/06/18/business/18cards.html>

<sup>4</sup> Prática de obter informações de carácter secreto ou confidencial, sem autorização destes, para se alcançar certa vantagem militar, política, econômica ou social.

<sup>5</sup> <http://portalexame.abril.com.br/ae/economia/m0151427.html>

<sup>6</sup> <http://g1.globo.com/Noticias/Tecnologia/0,,MUL1079997-6174,00-VEJA+NA+INTEGRA+NOTA+DA+TELEFONICA+SOBRE+FALHAS+NO+SPEEDY.html>



## 2.1. INFORMAÇÕES GERAIS SOBRE VULNERABILIDADES E AMEAÇAS DE SEGURANÇA DA INFORMAÇÃO

“Conheça o inimigo e a si mesmo e você obterá a vitória sem qualquer perigo; conheça o terreno e as condições da natureza, e você será sempre vitorioso.” (Sun Tzu)

Da mesma forma, em tecnologia da informação, é essencial conhecer o ambiente de TI, as fraquezas associadas aos ativos da informação e qualquer circunstância ou evento, com o potencial de causar impacto no negócio, para combater os inimigos e o crime virtual.

Do ponto de vista de Segurança da Informação, vulnerabilidades são fraquezas associadas aos ativos da informação e ameaça é qualquer circunstância ou evento com o potencial de causar impacto sobre a confidencialidade, integridade ou disponibilidade de informação ou sistemas de informação. Há vários tipos de ameaças (Bernstein, 1997), e dentre as mais conhecidas estão:

- Espionagem – a identidade de um ou mais usuários envolvidos em algum tipo de comunicação é observada, e pode ser utilizada de maneira ilícita posteriormente. Isto pode ocorrer no ambiente tecnológico através de ferramentas conhecidas como sniffers que podem ser executadas em um computador conectado a rede para visualizar o tráfego de dados e assim capturar informações como usuários e senhas.
- Disfarce – um usuário finge ser outro para obter acesso as informações, podendo ocorrer através de ataques de spoofing ao IP (Internet Protocol), ou seja, um usuário A envia mensagens falsas como se fossem de um outro já conhecido pelo destino para obter acessos indevidos.
- Armadilha – pode ocorrer com a execução ou abertura de documentos que seja atrativo ao usuário, o qual contém internamente outros programas que são processados sem a ciência e consentimento da pessoa, possibilitando assim atividades mal-intencionadas.

- Repúdio – uma ou mais pessoas negam ter participado de uma comunicação. Isto é extremamente crítico para transações financeiras eletrônicas, acordo e negociações realizadas através do meio digital.
- Manipulação de dados – a integridade dos dados é danificada durante o armazenamento ou a transmissão sem que seja detectada.
- *Replay* – uma sequência de eventos ou comandos é observada e reproduzida posteriormente para que possa efetivar alguma ação não autorizada.
- Negação de serviço – o acesso a um sistema é interrompido ou impedido, deixando a aplicação indisponível.

O ataque pode ocorrer externamente ou internamente por funcionários. Os termos mais comuns para os agentes externos envolvidos com as ameaças são os:

- *Hackers* – indivíduos que elaboram e modificam software e hardware de computadores, seja desenvolvendo funcionalidades novas ou adaptando as antigas para melhorar os softwares de forma legalizada.
- *Crackers* – verdadeira expressão para invasores de computadores é o termo usado para designar quem pratica a quebra (ou *cracking*) de um sistema de segurança, de forma ilegal ou sem ética. Este termo foi criado em 1985 por hackers em defesa contra o uso jornalístico do termo hacker.
- *Script kiddies* - É um termo pejorativo, usado para designar que não tem muito conhecimento técnico, e por isto utilizam do trabalho intelectual dos verdadeiros especialistas através de scripts prontos, "receitas de bolo", para invadir sistemas ou causar estragos. Muitos dos scripts estão disponíveis na internet, revistas e livros que falam sobre segurança.

- Terroristas virtuais – são aqueles que cometem violência e intimidação contra pessoas, empresas e governos através da Internet. Ações como tentativa de invasão ao sistema de controle de distribuição de energia de uma cidade, sistema de alarmes, filmagens e registros das forças de um país e outros setores para desequilibrar uma sociedade, instituição ou governo, são tipos de ataques terroristas.

Em pesquisa realizada em 2009 pela consultoria KPMG sobre fraudes no Brasil com mais de 1000 empresas, 61% dos entrevistados acreditavam que o potencial mais alto para a prática de fraude existe dentro da própria organização e 64% responderam que insuficiência de controles é a área crítica de preocupação (KPMG, 2009). Por isso ter e demonstrar confiança nas pessoas com quem trabalha é importante, mas prevenir através de controles é o ideal; pois os motivos para que uma pessoa comprometa a segurança da empresa são os mais diversos, podendo ser para obter ganhos financeiros, vingança, necessidade de aceitação ou respeito, idealismo, curiosidade ou busca de emoção, anarquia, aprendizado, ignorância, espionagem industrial e ou nacional (Calder, 2008).

## **2.2. CONCEITOS DE PROTEÇÃO DA INFORMAÇÃO**

Para proteger as informações é necessário identificar os recursos tecnológicos críticos (hardware, software, dados, pessoas, documentação, suprimentos, etc.), as ameaças, os riscos da organização e definição de controles para evitar com que se materializem. Exemplos de controles são a utilização de senhas eficientes para evitar a fácil descoberta e uso indevido do acesso, mecanismos de autenticação de usuários nos sistemas da organização, criptografia de informações confidenciais e rastreabilidade das operações realizadas no ambiente computacional. Para isto é importante que haja um processo e uma entidade dentro da empresa com a missão de prover a segurança da informação (Westerman, 2008).

A implementação de um sistema de gestão da segurança da informação inicia com a definição a toda a companhia sobre os princípios a serem seguidos em uma política formal de Segurança da Informação, contendo as diretrizes e os comportamentos esperados. O cuidado a

ser tomado, é o de não criar uma política só para tê-la; pois é uma atitude que traz poucos benefícios, por isto é importante a aplicabilidade, para que reflita a realidade do ambiente computacional, implementabilidade de forma que seja razoavelmente fácil de implementar, pertinência para refletir os objetivos de negócio da organização, escalabilidade visando atender as necessidades futuras da empresa e atual para que reflita as boas práticas de mercado.

Além disso, devem ser promovidas atividades de conscientização dos cuidados que devem ser tomados com a informação a todos os funcionários e parceiros de negócio. Por fim, para que a implementação seja eficiente, a adoção de um processo de monitoramento e análise crítica do sistema de gestão de segurança da informação deve ser contemplado; para que medidas corretivas e disciplinares sejam tomadas quando da ocorrência do descumprimento das diretrizes da companhia.

### **2.3. GOVERNANÇA CORPORATIVA**

Governança é o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre os proprietários, conselho de administração, diretoria e órgãos de controle (IBGC, 2009). Para tanto, a equipe executiva, articula estratégias e comportamentos desejáveis para cumprir as determinações do conselho de administração (Weill, 2006). Segundo a empresa de auditoria e consultoria externa KPMG e o Instituto Brasileiro de Governança Corporativa, os quatro pilares das boas práticas de governança corporativa, são:

- Equidade – Caracteriza-se pelo tratamento justo de todos os sócios e demais partes interessadas (*stakeholders*). Atitudes ou políticas discriminatórias, sob qualquer pretexto, são totalmente inaceitáveis.
- Prestação de contas - Os sócios, administradores (conselhos de administração e executivos/gestores), conselheiros fiscais e auditores devem prestar contas de

sua atuação, assumindo integralmente as consequências de seus atos e omissões.

- **Transparência** - Mais do que a obrigação de informar é o desejo de disponibilizar para as partes interessadas as informações que sejam de seu interesse e não apenas aquelas impostas por disposições de leis ou regulamentos. A adequada transparência resulta em um clima de confiança, tanto internamente quanto nas relações da empresa com terceiros. Não deve restringir-se ao desempenho econômico-financeiro, contemplando também os demais fatores (inclusive intangíveis) que norteiam a ação gerencial e que conduzem à criação de valor.
- **Sustentabilidade corporativa** – Os agentes de governança devem zelar pela sustentabilidade das organizações, visando à sua longevidade, incorporando considerações de ordem social e ambiental na definição dos negócios e operações.

O tema Governança Corporativa tornou-se mais difundido após uma série de escândalos em empresas norte-americanas ocasionados por atitudes ilícitas por parte da administração, como os casos da Enron e Worldcom, que atuavam respectivamente nos setores de distribuição de gás e telecomunicações. Como resultado, ambas as empresas decretaram falência e conseqüentemente causaram prejuízos a investidores, empregados, fornecedores, parceiros, clientes, além do descrédito no mercado financeiro (Weill, 2006).

Muitas das ações ilegais poderiam ter sido evitadas se houvesse monitoramento e medidas adequadas para que eventos ou condições incertas fossem prevenidos ou detectados antes que causasse um efeito negativo à organização. O nome dado a este processo é gerenciamento de risco, o qual será visto mais adiante neste capítulo, onde será abordado critérios para identificação, avaliação e tipos de tratamentos aos riscos.

Por isto a palavra comportamentos desejáveis e transparência são termos comumente utilizados quando se fala em governança corporativa, uma vez que estão associados às crenças

e cultura da organização definidas e praticadas não somente através da estratégia, mas também através de declarações de valor corporativo, missão institucional, princípios de negócio e estruturas de controle (Calder, 2008).

Para investidores, analistas de mercado, bancos, instituições de investimentos, agências de rating e private equities, a governança corporativa é um fator crítico para avaliar e valorizar uma empresa. De fato, em 2006 e 2007, as empresas no Brasil que fizeram as ofertas primárias de ações (*Initial Public Offering - IPO*) decidiram por aderir aos níveis diferenciados de governança corporativa estabelecido pela Bovespa, classificados como nível I, nível II e novo mercado (KPMG, 2007). Além disso, de acordo com a pesquisa Investor Opinion Survey da McKinsey de 2002, mais de 70% dos investidores estão dispostos a pagar mais por quotas de empresas com boa governança corporativa em relação a empresas com o mesmo desempenho financeiro.

#### **2.4. GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO**

A governança de TI consiste na especificação dos direitos decisórios e das responsabilidades por estimular comportamentos desejáveis na utilização dos recursos tecnológicos.

Desta forma, uma boa governança de TI assegura o envolvimento das pessoas necessárias na tomada de decisões, proporcionando melhor resultado nas implementações. Em um processo de Governança, há pelo menos cinco decisões (Weill, 2006) importantes e estratégicas que são consideradas a saber:

1. Declarações de alto nível sobre como a TI é utilizada no negócio;
2. Padronização de processos, dados e infraestrutura;
3. Planejamento da capacidade da infraestrutura de TI, para evitar o investimento excessivo e a implementação de componentes incorretos, resultando em desperdício de recursos, atrasos e incompatibilidade de sistemas;

4. Investimento em aplicações que atendam as necessidades de negócio e que geram valor diretamente;
5. Definições de orçamentos, decidindo quanto gastar, em que gastar e como reconciliar as necessidades de diferentes grupos de interesse.

Vale ressaltar, para que a governança seja bem sucedida, as cinco decisões não podem ser tomadas isoladamente.

## **2.5. GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO**

A Segurança da informação é um tema que não envolve apenas aspectos técnicos em ambientes cada vez mais interconectados e portanto, não está restrita a infraestrutura tecnológica como sistemas operacionais, banco de dados, redes de comunicação, firewalls de uma organização. Desta forma, deve ser tratado além da governança de TI, envolvendo o mais alto nível da organização uma vez que a dependência da informação tem aumentado e os riscos associados podem ameaçar a existência da corporação. Uma organização pode sobreviver a perda de ativos como equipamentos, construções, ferramentas, mas poucas podem continuar com a perda de informações críticas.

Além disto, para implantação e manutenção de um sistema de segurança da informação, é fundamental que o responsável, esteja vinculado a um nível hierárquico que forneça a independência necessária para monitorar e divulgar as deficiências não somente ao responsável pela área de TI, mas à alta administração. Aumentando a transparência e atribuindo a responsabilidade da tomada de decisões a um conselho executivo que tenha a autonomia suficiente para tratar cada risco identificado.

A Governança da Segurança da Informação consiste da liderança, estrutura organizacional e processos que salvaguardam a informação e prove o direcionamento estratégico, assegura que os objetivos de negócio sejam atendidos, gerencia apropriadamente os riscos, utiliza adequadamente os recursos da companhia e monitora o sucesso ou falha do programa de segurança corporativo.

Para implantar a Governança da Segurança da Informação de maneira eficiente, a organização deve estabelecer uma estrutura de trabalho (*framework*) para guiar o desenvolvimento e manutenção de um programa compreensivo.

A estrutura de trabalho deve contemplar uma metodologia de gestão de riscos de segurança de informação, estratégias de segurança alinhadas com os objetivos de negócio e de TI, estrutura de segurança organizacional adequada, estratégia de segurança que demonstre o valor da informação protegida, política de segurança que enderece cada aspecto estratégico, de controle e regulatório, conjunto completo de procedimentos com cada aspecto da política e um processo institucionalizado de monitoramento para assegurar a conformidade e o resultado da exposição ao risco.

Os benefícios de uma boa Governança da Segurança da Informação podem ser:

- Aumento no valor das ações para empresas que possuem capital aberto.
- Maior previsibilidade e redução das incertezas para organização dos riscos de segurança da informação.
- Proteção de potenciais responsabilidades civis e legais que poderiam ser atribuídas pela ausência ou imprecisão de informações.
- Rápida resposta a incidentes de segurança devido a agilidade da obtenção dos dados.
- Política eficaz de segurança da informação.
- Decisões críticas baseadas em informações precisas.
- Salvaguarda de informações durante processos de negócio críticos, como fusões e aquisições.

## **2.6. GERENCIAMENTO DE RISCOS**

Risco é um termo proveniente da palavra em latim *Risicu* ou *riscu*, que significa ousar, é um evento ou condição incerta que pode causar um efeito negativo a organização. As



perguntas pertinentes, portanto tratam de quão provável é que determinado evento ocorra (probabilidade) e que danos sobreviriam se ocorresse (impacto) (COSO, 2007). Eventos cujo impacto é positivo, representam oportunidades que podem influenciar favoravelmente na realização dos objetivos da organização.

Nas corporações se bem administrado, possibilita aos executivos tratar as incertezas e melhorar a capacidade de aumentar seus ganhos financeiros. Para tal, é necessário implementar um processo de gerenciamento de riscos corporativos, para alinhar a tolerância ao risco com a estratégia adotada, fortalecer as decisões em resposta aos riscos, reduzir as surpresas e prejuízos operacionais, identificar e administrar riscos múltiplos e entre empreendimentos, aproveitar oportunidades e otimizar o capital (COSO, 2007).

Para implementação do processo de gerenciamento de riscos, segundo a estrutura de trabalho COSO (*Committee of Sponsoring Organizations of the Treadway Commission*), há oito componentes integrados que devem ser contemplados:

1. Ambiente interno – compreende o tom de uma organização e fornece a base pela qual os riscos são identificados e abordados pelo seu pessoal.
2. Fixação de objetivos – os objetivos devem existir antes que a administração possa identificar os eventos em potencial que poderão afetar a sua realização.
3. Identificação de eventos – eventos internos e externos que influenciam o cumprimento dos objetivos.
4. Avaliação de riscos – riscos analisados de acordo com o impacto e a probabilidade de ocorrência.

5. Resposta a risco – forma que a administração responde aos riscos, definindo uma série de medidas que alinham os riscos com a tolerância e com o apetite<sup>7</sup>, podendo evitar, aceitar, reduzir ou compartilhar.
6. Atividades de controle - assegura que as respostas aos riscos sejam executadas com eficácia, através da implementação de políticas e procedimentos.
7. Informações e comunicações – informação relevante comunicada eficazmente em todos os sentidos da organização para cumprimento das responsabilidades.
8. Monitoramento – monitoramento da integridade da gestão de riscos corporativos.

O relacionamento entre os objetivos de uma organização e os componentes de gerenciamento de riscos corporativos é representado pela Figura 2.1:



Figura 2. 1 – O cubo do COSO (COSO, 2007)

<sup>7</sup> Apetite ao risco refere-se ao nível de riscos que de forma ampla, uma organização dispõe-se a aceitar na busca de valor. O apetite a risco reflete na filosofia de gestão de riscos corporativos e, por sua vez, influencia a cultura e o estilo de operação.

Desta forma, se os objetivos da organização estiverem claramente definidos, os riscos identificados e classificados, os controles mitigatórios devidamente monitorados e as informações disponíveis para a resposta da administração ao risco alinhado a tolerância, o processo de gestão de riscos estará adequado.

### **2.6.1. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO**

O processo de identificação e avaliação de riscos pode ser realizado através de modelos e métodos previamente definidos como o que será discutido no capítulo 4, possibilitando comparativos com outras organizações e otimização de tempo na implementação do gerenciamento e tratamento dos riscos. Além disso, permite que a organização foque em eventos, compare medições e resultados utilizando métricas comuns com o ramo de negócio em que atua. Esta abordagem possibilita tratar os riscos inerentes<sup>8</sup> de forma imediata após a etapa de identificação dos ativos do processo de avaliação e medir o resultado para entendimento do risco residual<sup>9</sup>.

Para organizações que desejam iniciar o processo, é necessário a definição do cenário de risco, que descreve o impacto aos negócios quando ou se um evento vier a ocorrer (IT GOVERNANCE INSTITUTE, 2009). Deve ser construído considerando os componentes demonstrados na Figura 2.2 e de acordo com as atividades descritas a seguir (ISO, 2008).

1. Definição do escopo e fronteiras – o escopo deve ser definido para assegurar que todos os ativos relevantes sejam considerados no processo de avaliação de riscos, incluindo detalhes e justificativas para quaisquer exclusões do escopo.
2. Identificação dos ativos – esta é uma atividade obrigatória para qualquer uma das abordagens apresentadas. Deve ser realizado com um nível adequado de detalhes que permita a avaliação de riscos, sendo dois os tipos de ativos que podem ser definidos,

---

<sup>8</sup> Risco inerente é o risco que uma organização terá de enfrentar na falta de medidas que a administração possa adotar para alterar a probabilidade ou o impacto dos eventos.

<sup>9</sup> Risco residual é aquele que ainda permanece após a resposta da administração.

os primários e os secundários. Os primários estão relacionados a processos de negócio e informação e o secundário como o responsável por suportar o primário, contendo dentre outros: hardware, software, rede, pessoas, localização e estrutura organizacional.

3. Identificação das ameaças – ameaças podem ser de origem natural ou humana, acidental ou deliberada, e tem o potencial de causar danos a ativos como informação, processos e sistemas. Exemplos de ameaças são ações não autorizadas, como uso indevido de equipamento, adulteração de dados, e os já citados Na seção 2.1.
4. Identificação de vulnerabilidades – vulnerabilidades são fraquezas e pontos fracos de um ativo como sistemas e processos, que pode ser explorada por ameaças que causam danos a organização. Exemplos de vulnerabilidades são: ausência de controle de mudança, uso de senhas fracas, dentre outros.
5. Identificação das consequências – esta atividade identifica os danos ou consequências para a organização, se um incidente ocorrer. Podem ser utilizados como referência custo de interrupção das operações, multas decorrentes da violação de leis e regulamentos, etc.



Figura 2. 2 – Componentes de Cenário de Risco (IT GOVERNANCE INSTITUTE, 2009)

Há duas maneiras básicas de se avaliar os riscos (ISO, 2008), a estimativa quantitativa e a qualitativa. A estimativa qualitativa usa uma escala de qualificação dos atributos em alto, médio e baixo para descrever o impacto e a probabilidade das potenciais ocorrências. A vantagem da análise qualitativa é a facilidade do entendimento por todas as pessoas envolvidas, porém tem como desvantagem a dependência de escolhas subjetivas na escala. Por este motivo, é importante que a avaliação ocorra por pessoas que tenham um bom conhecimento do ambiente de controle.

A análise quantitativa usa uma escala com valores numéricos para avaliação de impacto e probabilidade, utilizando informações de diversas origens. A qualidade da análise depende da acuracidade das informações geradas e o modelo utilizado para a avaliação. Na maioria dos casos a estimativa quantitativa, utiliza dados de histórico de incidentes, que tem como vantagem a associação dos objetivos e preocupações da organização. A principal desvantagem está relacionada à ausência de informações para riscos novos ou deficiências na Segurança da Informação.

## 2.6.2. MONITORAMENTO, TRATAMENTO E RESPOSTA AOS RISCOS

Uma vez identificados e avaliados os riscos, deve-se definir qual o tratamento que será dado para que a resposta a cada risco esteja alinhada aos objetivos estratégicos e o nível de exposição desejado pela organização. As alternativas para tratamento dos riscos conforme detalhada a seguir, são a de evitar, reduzir, compartilhar, aceitar ou até explorar, sendo esta última a menos usual nas referências bibliográficas.

- Evitar – decisão de não se envolver ou agir de forma a se retirar de uma situação de riscos. Por exemplo, a empresa pode optar pela descontinuação de uma linha de produtos, o declínio da expansão em um novo mercado geográfico ou a venda de uma divisão.
- Aceitar – nenhuma medida é adotada para afetar a probabilidade ou o grau de impacto dos riscos, pois em algumas situações a mitigação pode ter um custo maior que o risco propriamente. Exemplo: a diretoria da empresa decide não investir em um local alternativo para recuperação da infraestrutura tecnológica em uma situação de desastre.
- Reduzir – são adotadas medidas através da seleção e implementação de controles para reduzir a probabilidade ou impacto dos riscos, ou até mesmo ambos. Exemplo: A organização investiu no aprimoramento do processo de autodetecção de falhas e de cópias de segurança para minimizar a probabilidade de indisponibilidade dos sistemas.
- Transferir e/ou compartilhar – redução da probabilidade ou do impacto pela transferência ou pelo compartilhamento de parte do risco. As técnicas comuns compreendem a aquisição de produtos de seguro ou a terceirização de atividades.
- Explorar – aumentar o grau de exposição ao risco na medida em que isto possibilita vantagens competitivas, como por exemplo, uma empresa produtora

de petróleo utiliza as informações sobre o mercado futuro<sup>10</sup> para especular no mercado de derivativos<sup>11</sup>, aumentando sua exposição ao preço de commodity<sup>12</sup>.

Para manter um nível de exposição e o adequado tratamento do risco, cabe a alta administração a avaliação contínua da eficácia do modelo de gestão de riscos, que deve ser constantemente monitorado com o objetivo de assegurar a presença e o funcionamento de todos os seus componentes ao longo do tempo. Para isto, é essencial que uma organização defina um conjunto de métricas para servir como indicadores de risco, denominados de KRI's (Key Risk indicators), os quais devem ser relevantes o suficiente para predizer ou indicar uma exposição de risco importante.

---

<sup>10</sup> É um acordo entre duas partes para comprar ou vender um ativo numa data específica por um determinado preço e geralmente negociado no pregão da Bolsa de Valores, onde as partes em questão não precisam se conhecer necessariamente. Os ajustes de preços são liquidados dia-a-dia.

<sup>11</sup> Contrato financeiro cujo valor deriva de outro ativo, ou seja, o valor do contrato é derivado do valor de outro bem, como uma ação, um título, uma commodity, uma moeda ou uma taxa de juro.

<sup>12</sup> Usada como referência aos produtos de base em estado bruto (matérias-primas) ou com pequeno grau de industrialização, de qualidade quase uniforme, produzidos em grandes quantidades e por diferentes produtores.

### 3. VISÃO GERAL DAS ESTRUTURAS DE TRABALHO

A necessidade de padrões e metodologias para implementação de um ambiente de controle tecnológico confiável vem sendo discutido desde 1967 pelo ISACA (*Information Systems Audit and Control Association*) (IT GOVERNANCE INSTITUTE, 2007).

Neste sentido, vários estudos e pesquisas foram realizados para definir um conjunto de objetivos que a área de tecnologia da informação deveria alcançar para prover eficiência, eficácia, confidencialidade, integridade, disponibilidade, conformidade e confiabilidade nos recursos e dados processados por TI (IT GOVERNANCE INSTITUTE, 2009).

Como resultado, foi publicado em 1995 o framework CobiT (*Control Objectives for Information and related Technology*), que baseado no COSO, provê uma visão do ambiente de controle de Tecnologia da Informação. Vale ressaltar, que após aprovação da Lei americana Sarbanes-Oxley<sup>13</sup> tem sido um dos mais utilizados e recomendados para a implementação da Governança de TI (PCAOB, 2004).

Além disso, em 1987 o departamento de comércio e indústria do Reino Unido criou um centro de Segurança da Informação, o CCSS (*Commercial Computer Security Centre*), que dentre outras responsabilidades tinha a incumbência de definir uma norma de segurança de informação para o próprio Reino Unido. Desta forma, em 1995 surgiu a BS7799, que depois de alguns anos foi atualizada para a ISO 17799 e posteriormente para 27002 (ABNT, 2005).

Da mesma forma, o Governo Britânico, através da agência *Central Computer and Telecommunications Agency (CCTA)* criou em 1980 um conjunto de melhores práticas para um adequado Gerenciamento de Serviços de TI, denominado de ITIL.

---

<sup>13</sup> Lei federal dos EUA sancionada em 30 de julho de 2002, em resposta aos inúmeros escândalos corporativos e contábeis de grandes proporções ocorridos à época. Tem por objetivo estabelecer sanções que coibam procedimentos não éticos e em desacordo com as boas práticas de governança corporativa por parte das empresas atuantes no mercado norte americano.



Todos os órgãos citados tinham e ainda tem uma preocupação em comum, a adoção de processos claramente definidos e estruturados, para que seja possível gerenciar os recursos de TI, de forma a reduzir custos, garantir a disponibilidade e gerar dados íntegros e confiáveis. Além disso, vem trabalhando na atualização de suas estruturas de trabalho e terminologias visando inclusive alinhar conceitos para facilitar a integração entre eles.

Com base em um estudo do *IT Governance Institute* em conjunto com o *UK's Office of Government Commerce* denominado the “*Aligning CobiT 4.1, ITIL v3 e ISO 27002*” (IT GOVERNANCE INSTITUTE , 2008) verificou-se que é possível relacionar o CobiT, ITIL e a Norma de Segurança ISO 27002.

Neste sentido, o próximo capítulo, avalia individualmente cada modelo, com o objetivo de torná-los um modelo de processos unificado e mais completo para a avaliação dos processos de Segurança da Informação em um ambiente Corporativo. Em adição, também será utilizado para comparação as recomendações de Segurança da Informação do NIST – National Institute of Standards and Technology publicadas no documento 800-53.

### **3.1. PREMISSA PARA AS COMPARAÇÕES DOS PROCESSOS**

Para comparação de qualquer objeto é importante definir uma referência, ou seja, um atributo comum. Neste sentido, para propor uma solução, foi definido como base de comparação, o processo do CobiT, denominado de DS5 - segurança de sistemas, pelo fato de ser voltado à governança de TI facilitando assim o entendimento dos riscos e os objetivos do controle, e por já existir estudos individuais visando a convergência com a ISO 27002, ITIL e NIST.

Além disso, será utilizado para cada análise das estruturas de trabalho e norma as seguintes informações: nome do processo, risco associado e prática de controle. Esta atividade visa à preparação para a consolidação apresentado no capítulo 4, das avaliações individuais de cada estrutura de trabalho.

### 3.2. COBIT

O COBIT é uma estrutura de trabalho adotada como referência para a implementação de governança de TI e controle, que foca no que “precisa ser alcançado” ao invés de se preocupar em “como alcançar”. Tem como características principais o fato de ser focado nos negócios, orientado a processos, baseado em controles e orientado por métricas, buscando estabelecer uma conexão entre as metas de negócio com as de TI (IT GOVERNANCE INSTITUTE, 2007).

A premissa do CobiT é de que TI precisa entregar a informação que a empresa necessita para alcançar seus objetivos, a qual deve atender os requisitos de qualidade (qualidade, custo e entrega), segurança (confidencialidade, integridade e disponibilidade) e os fiduciários (eficácia e eficiência das operações, confiabilidade e conformidade com leis e regulamentos).

O COBIT, conforme mostra a Figura 3.1 é representado por um cubo com três componentes chaves, a saber: processos de TI, formado por domínios, processos e atividades; recursos de TI composto por aplicações, informação, infraestrutura e pessoas; e critérios de informação contendo os requisitos eficácia, eficiência, confidencialidade, integridade, disponibilidade, conformidade e confiabilidade.

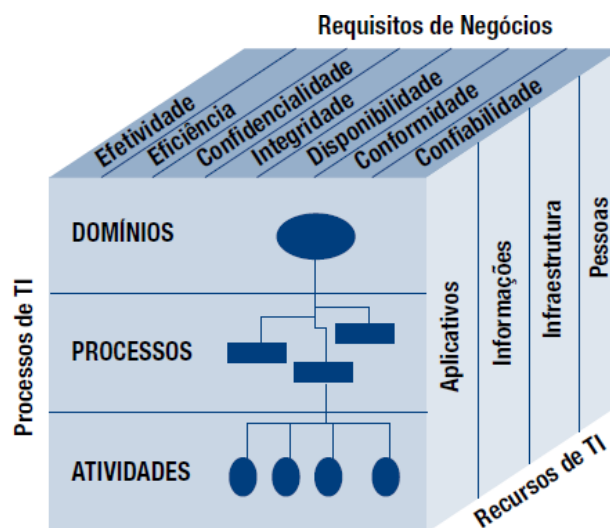


Figura 3. 1 – O cubo do CobiT (IT GOVERNANCE INSTITUTE, 2007)

Oferece um modelo para a Governança de TI desmembrado em quatro domínios, denominados de Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte e Monitoração e Avaliação.

Planejamento e Organização está relacionado aos processos que visam assegurar que as estratégias e táticas da área de TI estão alinhadas aos objetivos de negócio da companhia, através da elaboração de um adequado planejamento estratégico, otimização de recursos, gerenciamento dos riscos, projetos, dentre outras atividades.

Aquisição e Implementação diz respeito aos processos que contribuem para a identificação, desenvolvimento e aquisição de soluções que visam implementar as definições estratégicas. Além disso, trata das questões pertinentes a manutenção e mudanças das soluções após a implementação.

Entrega e Suporte tem como objetivo assegurar que os processos são suficientes para atingir os níveis de serviço esperado pelos clientes internos e externos da TI, através da gestão da segurança, desempenho, capacidade, continuidade do serviço, custos, pessoas, dentre outras.

Monitoração e Avaliação está relacionado às atividades de controle que visam assegurar que os processos definidos estão em conformidade com as diretrizes, políticas, leis e regulamentos estabelecidos.

O CobiT contém 34 processos subdividido em cada um dos quatro domínios conforme demonstrado na Figura 3.2. Há uma relação de 3 a 15 objetivos de controle por processo e 5 a 10 práticas de controle por objetivo, totalizando 210 objetivos de controle e mais de 1500 práticas de controle.

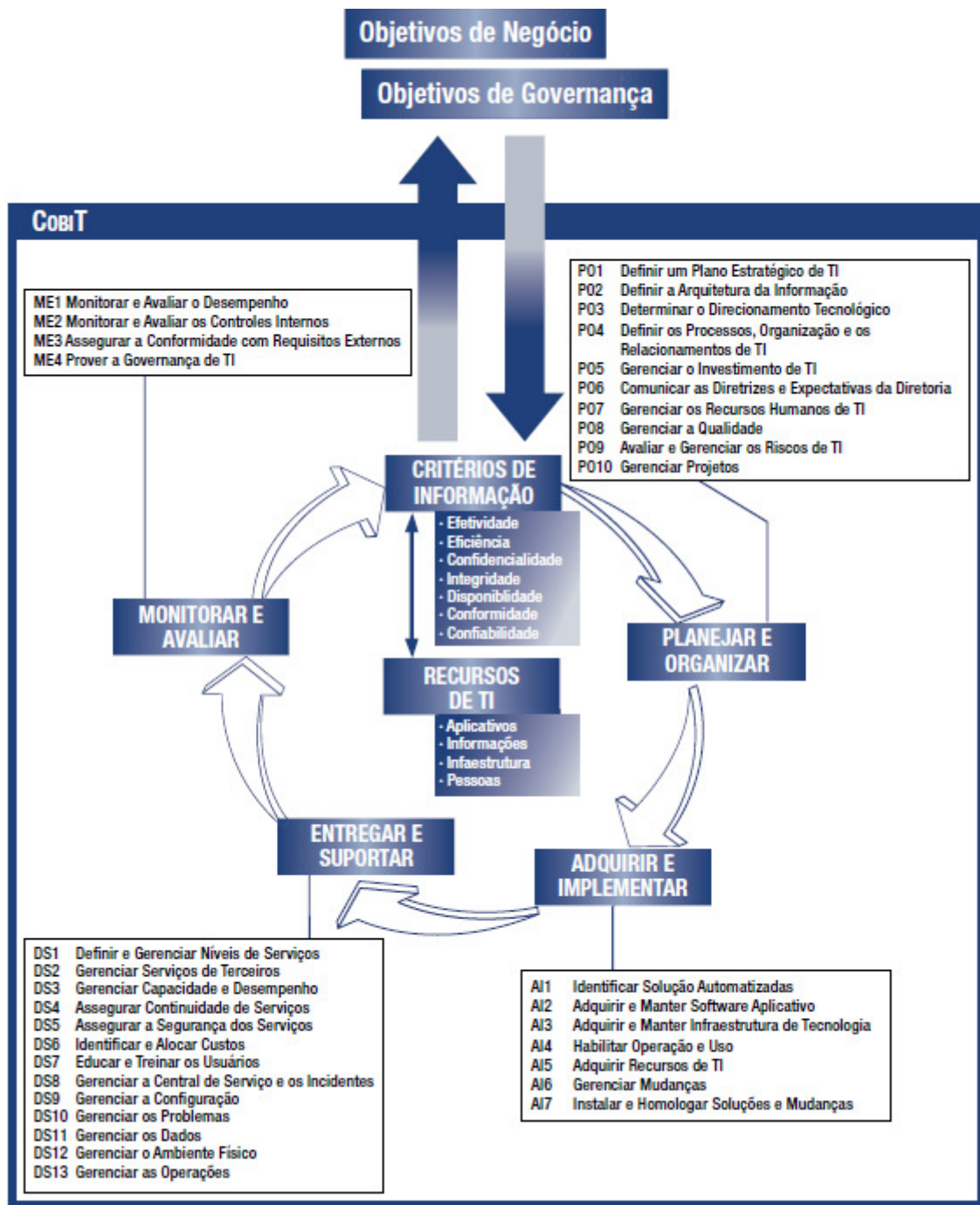


Figura 3. 2 – Visão Geral do Framework CobiT (IT GOVERNANCE INSTITUTE, 2007)

### 3.2.1 SEGURANÇA DE INFORMAÇÃO SOB A PERSPECTIVA DO COBIT

O CobiT trata segurança de sistemas no processo definido como DS (Entrega e Suporte) 5 – Assegurar Segurança dos Sistemas, cujo objetivo é o de manter a integridade da

informação e proteger os ativos, visando minimizar os impactos de vulnerabilidades de segurança e incidentes.

Neste processo há 11 objetivos de controles, que servem para estabelecer o que é importante implementar no processo de segurança de informação para que haja proteção adequada. Como serão utilizados como base de comparação é importante descrever cada um dos objetivos de controle, conforme a seguir:

- DS5.1 Gerenciamento da Segurança - gerencia a segurança de TI no nível organizacional apropriado mais elevado, de forma que a gestão das ações de segurança esteja em linha com os requerimentos de negócio.
- DS5.2 Plano de Segurança de TI – traduz requerimentos do negócio, riscos e conformidade em um plano abrangente de segurança de TI, considerando a infraestrutura tecnológica e a cultura de segurança. Assegura que o plano é implementado em políticas de segurança e procedimentos junto com investimentos apropriados em serviços, pessoas, software e hardware. Comunica políticas de segurança e procedimentos para os interessados e usuários.
- DS5.3 Gestão de Identidade – assegura que todos os usuários (interno, externo e temporário) e suas atividades nos sistemas de TI (aplicações de negócio, ambiente de TI, sistemas operacionais, desenvolvimento e manutenção) são unicamente identificados. Habilita usuários através de mecanismos de autenticação. Confirma que todos os direitos de acesso aos sistemas e dados estão em linha com as necessidades de negócio definidas e documentadas e que os requerimentos de trabalho estão associados a identidades dos usuários. Assegura que os direitos de acesso são requisitados por gerenciamento dos usuários, aprovados por proprietários dos sistemas e implementados por pessoal responsável por segurança. Mantém a identidade dos usuários e direitos de acesso no repositório central. Implementa técnicas de custo efetivo e procedimentos de medição, e mantém

atualizada a identificação do usuário, implementa autenticação e reforça os direitos de acesso.

- DS5.4 Gerenciamento de contas de usuários – endereça a requisição, estabelecendo, emitindo, suspendendo, modificando e encerrando as contas de usuários e privilégios de usuários relacionados com um grupo de procedimentos de gestão de contas de usuários. Incluindo um procedimento aprovado que defina os proprietários de sistemas ou dados que concedem os privilégios de acesso. Estes procedimentos devem ser aplicados para todos os usuários, incluindo administradores (usuários privilegiados) e internos e usuários externos, para casos normais e de emergência. Direitos e obrigações relativas para acesso aos sistemas corporativos e informações devem ser contratualmente estabelecidos para todos os tipos de usuários. Executa revisão periódica de todas as contas e privilégios relacionados,
- DS5.5 Testando Segurança, Inspeção e Monitoramento - monitorar a implementação de segurança de TI de forma proativa. Segurança de TI deve assegurar de que o baseline de segurança de informação corporativos é aprovado e se mantém atualizado. A rastreabilidade e a função de monitoramento permitirão a prevenção em tempo hábil e ou detecção e subsequente relatório tempestivo de atividades anormais e/ou não usuais que podem ser endereçadas.
- DS5.6 Definição de Incidente de Segurança – Definir claramente e comunicar as características de potenciais incidentes de segurança, para que eles possam ser devidamente classificados e relacionados pelo processo de gestão de problemas e incidentes.
- DS5.7 Proteção de Tecnologia de Informação - torna tecnologia relacionada a segurança resistente a fraudes, e não revelam documentação de segurança desnecessariamente.

- DS5.8 Gerenciamento de chave criptográfica - determina que políticas e procedimentos estão implementados para organizar a geração, mudança, revogação, destruição, distribuição, certificação, armazenamento, entrada, uso e arquivamento de chaves criptográficas para assegurar a proteção das chaves contra modificação e revelação não autorizada.
- DS5.9 Prevenção, detecção e correção de software malicioso - medidas preventivas, detectivas e corretivas implementadas na organização para proteger sistemas de informação e tecnologia de malware (exemplo: vírus, worms, spyware, spam).
- DS5.10 Segurança de Rede – uso de técnicas de segurança e procedimentos de gerenciamento relacionados (Exemplos, firewalls, ferramentas de segurança, detecção, intrusão e segmentação da rede) a autorização de acesso e controle de fluxo de informação de e para a rede.
- DS5.11 Intercâmbio de dados sensíveis – troca de dados sensíveis somente são realizadas através de caminhos confiáveis ou com controles que permitam assegurar a autenticidade de conteúdo, prova de submissão, recebimento e não repúdio da origem.

### **3.2.1.1 MATRIZ COBIT DE RISCOS DE SEGURANÇA DA INFORMAÇÃO**

O objetivo desta avaliação é o de identificar os controles e riscos sugeridos pela estrutura de trabalho CobiT no processo Segurança de Sistemas para posterior comparação com o ITIL, ISO 27002 e NIST SP800-53, visando à definição de um modelo integrado de avaliação de riscos e controles (ISACA, 2009).

A matriz de riscos foi preparada através de:

- Identificação, através do Cobit Online<sup>14</sup>, dos riscos de segurança da informação baseado nos “Risk Drivers” que descrevem potenciais vulnerabilidades nos processos de tecnologia da informação e “Value Drivers” que apresentam aspectos gerais e críticos que devem ser implementados para atendimento dos objetivos de controle.
- Mapeamento dos controles através da leitura e interpretação dos “Control Practices” (Práticas de Controle), onde são descritas as atividades para implementação de controles e o “Generic Control Practices” (Práticas de Controle Genéricas) que sugere a abordagem, responsabilidade e forma de comunicação. Ambos apresentados no CobiT Online.
- Associação das atividades de controles aos riscos e processo de segurança de sistemas do domínio DS5 da estrutura de trabalho CobiT.

Como resultado, foram identificadas 35 atividades de controles e 13 riscos de segurança da informação, conforme detalhado no Anexo A – Matriz de Riscos e controles para o CobiT.

Para uma visão geral, a tabela 3.1 apresenta um quadro resumo dos riscos e controles CobiT identificados.

Tabela 3. 1 – Quadro Resumo dos Riscos e Controles CobiT

Processo	Riscos	Controles
DS5.1	RITI.01: Ações de segurança de informação desalinhada aos objetivos de negócio	<ul style="list-style-type: none"> <li>• Definição formal de responsabilidades</li> <li>• Política de Segurança da Informação</li> <li>• Estrutura Organizacional</li> </ul>

<sup>14</sup> <http://www.cobitonline4.info/Pages/Public/Browse/Browse.aspx?t=CP&p=DS5&v=1>



Processo	Riscos	Controles
DS5.2	RITI.02: Descumprimento das regras de segurança de informações	<ul style="list-style-type: none"> <li>• Definição e comunicação do Plano de Segurança de TI alinhada a tolerância a riscos</li> </ul>
	RITI.03: Plano de segurança de informações incompatível com os requisitos de negócio da companhia	<ul style="list-style-type: none"> <li>• Profissionais capacitados</li> <li>• Programas de conscientização de Segurança da Informação</li> </ul>
DS5.3	RITI.04: Dificuldade ou impossibilidade de atribuição de responsabilidades	<ul style="list-style-type: none"> <li>• Cadastro, autenticação, autorização e revisão dos privilégios de acesso das contas de usuários</li> </ul>
	RITI.05: Operações realizadas por pessoas com privilégios de acesso inadequados	<ul style="list-style-type: none"> <li>• Política de Segurança da Informação</li> </ul>
DS5.4	RTTI.06: Operações realizadas por contas de usuários inválidas ou fictícias	<ul style="list-style-type: none"> <li>• Cadastro, manutenção de senhas</li> <li>• Rastreabilidade das operações realizadas no ambiente tecnológico</li> <li>• Revisão de acesso</li> </ul>
DS5.5	RTTI.07: Ausência de monitoramento e revisão dos riscos de segurança da informação	<ul style="list-style-type: none"> <li>• Cadastro, autorização e remoção das contas de usuários</li> <li>• Rastreabilidade</li> <li>• Teste de vulnerabilidades</li> </ul>
DS5.6	RTTI.08: Fraudes e desfalques decorrente de incidentes de segurança não detectados e tratados tempestivamente.	<ul style="list-style-type: none"> <li>• Comunicação e tratamento de incidentes</li> <li>• Rastreabilidade</li> </ul>
DS5.7	RTTI.09: Inadequada proteção das ferramentas utilizadas para segurança de informações	<ul style="list-style-type: none"> <li>• Comunicação e tratamento de incidentes</li> <li>• Rastreabilidade</li> </ul>
DS5.8	RTTI.10: Comprometimento dos mecanismos de controle que evitam o não-repúdio de operações críticas	<ul style="list-style-type: none"> <li>• Geração, renovação, revogação, armazenamento e proteção das chaves criptográficas.</li> </ul>
DS5.9	RTTI.11: Instalação e uso de softwares maliciosos no ambiente tecnológico.	<ul style="list-style-type: none"> <li>• Política de Segurança da Informação</li> <li>• Filtro de tráfego de rede</li> <li>• Identificação e remoção de softwares maliciosos</li> <li>• Acesso restrito para instalação de softwares</li> </ul>
DS5.10	RTTI.12: Invasão do ambiente tecnológico	<ul style="list-style-type: none"> <li>• Análise e aprovação de regras de firewall</li> </ul>

Processo	Riscos	Controles
	da empresa por pessoas mal intencionadas.	<ul style="list-style-type: none"> <li>• Planejamento e revisão da arquitetura de rede</li> <li>• Monitoramento de potenciais ações maliciosas na rede de comunicações</li> </ul>
DS5.11	RTTI.13: Transações eletrônicas inválidas e/ou não autorizadas efetuadas com parceiros de negócio.	<ul style="list-style-type: none"> <li>• Proteção dos dados transferidos e recebidos</li> <li>• Proteção dos equipamentos utilizados para transações eletrônicas com parceiros de negócio</li> <li>• Análise e aprovação de regras de firewall</li> </ul>

### 3.3. ITIL

O ITIL (*Information Technology Infrastructure Library*) é um modelo de referência para gerenciamento de serviços de TI<sup>15</sup>. A metodologia foi criada pela secretaria de comércio (*Office of Government Commerce, OGC*) do governo Inglês, a partir de pesquisas realizadas por consultores, especialistas e doutores, para desenvolver as melhores práticas para a gestão de serviços de tecnologia da informação nas empresas privadas e públicas (HP, 2004). A primeira versão foi criada em 1980 focada na gestão de tecnologia da informação, a segunda publicada em 1990, mudou o foco para a implementação de gestão de serviços buscando a satisfação dos clientes da área de tecnologia da informação, através da eficiência e eficácia dos processos. A terceira versão, concluída em 2007, é a mais atual e focou no conceito de ciclo de vida do serviço, que embora seja novo para TI não é para o negócio, uma vez que um serviço nasce, se desenvolve, vai para a operação e um dia morre.

As melhores práticas propostas no ITIL são suportadas pela British Standards Institution's for IT Service Management (BS15000), sendo esta um anexo da ISO 9000/2000. O foco é descrever os processos necessários para gerenciar a infraestrutura de TI, com o objetivo de assegurar os níveis de serviço acordados com os clientes internos e externos.

<sup>15</sup> Gerenciamento de serviços é um conjunto de habilidades da organização para fornecer valor para o cliente em forma de serviços, de acordo com o propósito do cliente (utilidade) e adequado para uso (garantia).

O ITIL, conforme Figura 3.3, está dividido em 5 disciplinas: Estratégia, Desenho, Transição, Operação e Melhoria de Serviço Continuada. Cada uma contém a visão geral do gerenciamento de serviços, fundamentos, princípios, processos, funções, papéis e responsabilidades em cada estágio.

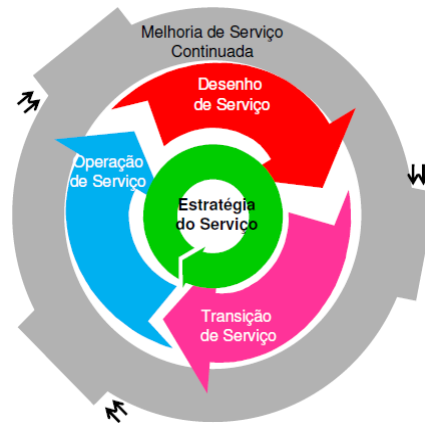


Figura 3. 3 – Visão Geral do Framework ITIL (Office Government Commerce, 2007)

Possibilita através dos seus processos, que TI seja mais que um provedor de serviço, seja de fato um parceiro de negócio que provê um conjunto de serviços necessários para o atingimento dos objetivos da companhia. O ITIL com o conceito de Ciclo de Vida do Serviço conecta todas as fases da solução, desde sua criação até a implementação e suporte, facilitando a integração da TI com o negócio. O “Ciclo de Vida do Serviço” é composto pelas seguintes fases:

1. Estratégia de serviço: prevê e conceitua um conjunto de serviços que contribui para que o negócio alcance seus objetivos.
2. Desenho de serviço: desenha o serviço considerando os objetivos de utilidade e garantia.

3. Transição de serviço: transfere os serviços de um ambiente de desenvolvimento e homologação para o de produção
4. Operação de serviço: gerencia os serviços em produção para assegurar que os objetivos de utilidade e garantia sejam alcançados.
5. Melhoria de serviços continuada: avalia os serviços e identifica formas de melhorar sua utilidade e garantia no suporte aos objetivos de negócio.

### **3.3.1 SEGURANÇA DA INFORMAÇÃO SOB A PERSPECTIVA DO ITIL**

O ITIL trata segurança da informação como parte de um serviço que deve ser provido ao cliente de TI, abordando o assunto principalmente na fase de arquitetura para definição dos requerimentos de segurança e na de operação para implementação do que foi definido (Office Government Commerce, 2007). Descreve como um processo que deve proteger os interesses de quem confia na informação através da proteção dos sistemas e meios de comunicação contra falhas de disponibilidade, confidencialidade e integridade.

Além disso, define como meta do processo a função de alinhar segurança de TI com segurança do negócio e assegurar que está devidamente gerenciada em todos os serviços.

#### **3.3.1.1 MATRIZ DE RISCOS DE SEGURANÇA DA INFORMAÇÃO PARA O ITIL**

Na identificação dos controles descritos no ITIL para os processos de segurança da informação, as disciplinas (livros) que endereçam os riscos associados, com exceção dos de chave criptográfica, instalação de softwares maliciosos, invasão do ambiente tecnológico por agentes externos e transações eletrônicas realizadas com parceiros de negócio, são o SD 4.6 – Gestão da Segurança da Informação, SO 4.5 – Gestão de Acesso, SO 5.13 – Gestão da Segurança da Informação e Operação do Serviço, SO 5.4 – Gestão do Servidor e Suporte e SO 5.5 – Gerenciamento de Rede (Office Government Commerce, 2007).

Com base na tabela 3.2 obtida a partir do estudo publicado pelo ISACA “*Mapping of ITILv3 with CobiT 4.1*” (IT Governance Institute, 2008), foi realizado o entendimento de cada um dos processos do ITIL referenciados e abstraídos os controles através de interpretação. O resultado desta análise pode ser encontrado no Anexo B - Matriz de Riscos e controles para o ITIL, onde foram relacionadas 16 atividades de controle aos 13 riscos de segurança da informação identificados na análise da estrutura de trabalho CobiT.

Tabela 3. 2 – Relacionamento dos Processos CobiT com os do ITIL (IT GOVERNANCE INSTITUTE, 2008)

Processo Cobit	Processos ITIL
DS5.1	SD 4.6 – Gestão da segurança da informação SO 5.13 – Gestão da segurança da informação e operação do serviço
DS5.2	SD 4.6.4 – Conceitos básicos, princípios e políticas SD 4.6.5.1 – Controles de Segurança
DS5.3	SO 4.5 – Gestão do acesso
DS5.4	SO 4.5 – Gestão do acesso SO 4.5.5.1 – Requisição de acesso SO 4.5.5.2 – Verificação SO 4.5.5.3 – Concessão de acessos SO 4.5.5.4 – Monitoração da situação da conta de usuário SO 4.5.5.5 – Registro e rastreabilidade do acesso SO 4.5.5.6 – Remoção ou restrição de acessos
DS5.5	SO 4.5.5.6 – Remoção ou restrição de acessos SO 5.13 – Gestão da segurança da informação e operação do serviço
DS5.6	SD 4.6.5.1 – Controles de Segurança SD 4.6.5.2 – Gestão de brechas de segurança e incidentes
DS5.7	SO 5.4 – Gerenciamento do servidor e suporte
DS5.8	Não há processos relacionados no ITIL com relação a este domínio.
DS5.9	Não há processos relacionados no ITIL com relação a este domínio.

Processo Cobit	Processos ITIL
DS5.10	SO 5.5 Gestão de rede
DS5.11	Não há processos relacionados no ITIL com relação a este domínio.

### 3.4. ISO 27001 E 27002

A *International Organization for Standardization, (ISO)*, é uma organização fundada em 1946 e sediada em Genebra, na Suíça. Seu objetivo é promover normas que possam ser utilizadas como padrões em todos os países. As normas 27001 e 27002 são reconhecidas internacionalmente para implementação de um sistema de Gestão de Segurança de Informação e de melhores práticas.

A norma ISO/IEC 27001:2005 - Tecnologia da informação - Técnicas de segurança - Sistemas de gerência da segurança da informação (ABNT, 2006) é um padrão publicado em outubro de 2005, baseado no modelo PDCA (Plan-Do-Check-Act) conforme ilustrado na Figura 3.4. O objetivo da norma é promover uma abordagem para manter e melhorar o Sistema de Gestão de Segurança da Informação, através de um processo para estabelecer, implementar, operar, monitorar e analisar criticamente a implementação para a melhoria contínua. Contempla 11 cláusulas de controle que trata política de segurança, organização da segurança de informação, gestão de ativos, segurança em recursos humanos, segurança física e do ambiente, gerenciamento das operações e comunicações, controle de acesso, aquisição, desenvolvimento e manutenção de sistemas, gestão de incidentes de segurança de informação, gestão da continuidade dos negócios e conformidade.

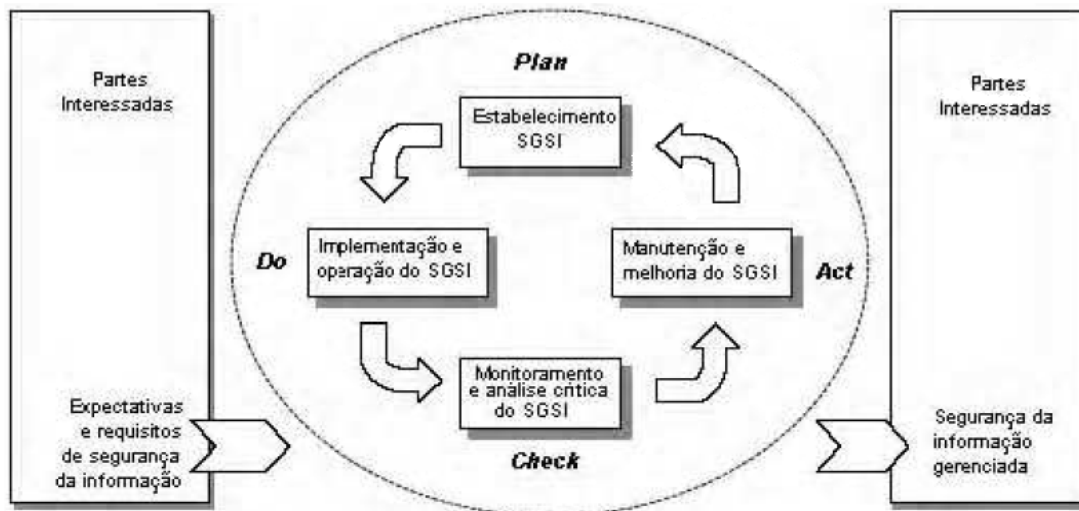


Figura 3. 4 – Modelo PDCA aplicado aos processos da norma 27001 (ABNT, 2006)

A ISO/IEC 27002:2005 - Tecnologia da Informação – Técnicas de Segurança – Código de Prática para Gestão de Segurança da Informação, anteriormente denominada de ISO/IEC 17799 (ABNT, 2005), fornece um conjunto de 39 objetivos de controle e 133 controles de segurança considerados as melhores práticas de Segurança da Informação, para auxiliar e servir como um guia prático no desenvolvimento dos procedimentos.

### 3.4.1 MATRIZ DE RISCOS DE SEGURANÇA DA INFORMAÇÃO PARA A ISO 27002

A identificação dos controles foi realizada através do entendimento e interpretação de cada um dos requerimentos referenciados na tabela 3.3 obtida a partir do estudo publicado pelo ISACA “*Mapping of ISO/IEC 17799:2005 with CobiT 4.0*” (IT GOVERNANCE INSTITUTE, 2006). Como resultado foram encontrados 73 atividades associados a 31 objetivos de controle da ISO. Todas as mapeadas para a ISO 27001 também foram identificadas na ISO 27002, por este motivo foram mantidas apenas uma delas. O detalhamento das atividades de controle e a associação a cada um dos 13 riscos de segurança pode ser encontrado no Anexo C - Matriz de Riscos e controles para a ISO 27002.

Tabela 3. 3 – Relacionamento dos Processos CobiT com requerimentos da ISO 27002 (IT GOVERNANCE INSTITUTE, 2006)

Processo Cobit	Requerimentos ISO 27002	
DS5.1	6.1.1 Comprometimento da direção 6.1.2 Coordenação da segurança da informação	6.2.3 Acordos de terceiros 8.2.2 Conscientização, educação e treinamento
DS5.2	5.1.1 Documentação da política de segurança 5.1.2 Análise crítica da segurança 6.1.2 Coordenação da segurança da informação 6.1.5 Acordos de confidencialidade	8.2.2 Conscientização, educação e treinamento 11.1.1 Política de controle de acesso 11.7.1 Computação e comunicação móvel 11.7.2 Trabalho remoto
DS5.3	11.2.3 Gerenciamento de senha do usuário 11.3.1 Uso de senhas 11.4.1 Política de uso dos serviços de rede 11.5.1 Procedimentos de entrada no sistema	11.5.2 Identificação e autenticação de usuário 11.5.3 Sistema de gerenciamento de senha 11.5.5 Desconexão de terminal por inatividade 11.5.6 Limitação de horário de conexão 11.6.1 Restrição de acesso a informação
DS5.4	6.1.5 Acordos de confidencialidade 6.2.1 Identificação de riscos com partes externas 6.2.2 Segurança quando tratando com clientes 8.1.1 Papéis e responsabilidades 8.3.1 Encerramento de atividades 10.1.3 Segregação de funções 11.1.1 Política de controle de acesso	11.2.1 Registro de usuário 11.2.2 Gerenciamento de privilégios 11.2.4 Análise dos direitos de acesso de usuário 11.3.1 Uso de senhas 11.5.1 Procedimentos de entrada no sistema 11.5.3 Sistema de gerenciamento de senha 11.6.1 Restrição de acesso a informação
DS5.5	6.1.8 Análise crítica independente 10.10.2 Monitoramento do uso do sistema 10.10.3 Proteção das informações dos registros 10.10.4 Registros de administrador e operador	12.6.1 Controle de vulnerabilidades técnicas 13.1.2 Notificando fragilidades de segurança 15.2.2 Verificação da conformidade técnica 15.3.1 Controle de auditoria de sistemas
DS5.6	8.2.3 Processo disciplinar 13.1.1 Notificando de eventos de segurança	13.2.1 Responsabilidades e procedimentos 13.2.3 Coleta de evidências



Processo Cobit	Requerimentos ISO 27002	
DS5.7	<p>6.1.4 Processo de autorização aos recursos de TI</p> <p>9.1.6 Acesso do público, áreas de entrega e de carregamento</p> <p>9.2.1 Instalação e proteção do equipamento</p> <p>9.2.3 Segurança do cabeamento</p> <p>10.6.2 Segurança dos serviços de rede</p> <p>10.7.4 Segurança da documentação dos sistemas</p> <p>10.10.1 Registros de auditoria</p> <p>10.10.3 Proteção das informações dos registros</p> <p>10.10.4 Registros de administrador e operador</p> <p>10.10.5 Registros de falhas</p> <p>10.10.6 Sincronização dos relógios</p> <p>11.3.2 Equipamento de usuário sem monitoração</p> <p>11.3.3 Política de mesa limpa e tela limpa</p> <p>11.4.3 Identificação de equipamento em redes</p>	<p>11.4.4 Proteção e configuração de portas de diagnóstico remotas</p> <p>11.5.1 Procedimentos de entrada no sistema</p> <p>11.5.4 Uso de utilitários de sistema</p> <p>11.5.5 Desconexão de terminais por inatividade</p> <p>11.5.6 Limitação de horário de conexão</p> <p>11.6.2 Isolamento de sistemas sensíveis</p> <p>11.7.1 Computação e comunicação móvel</p> <p>11.7.2 Trabalho remoto</p> <p>12.4.1 Controle de software operacional</p> <p>12.6.1 Controle de vulnerabilidades técnicas</p> <p>13.1.2 Notificando fragilidades de segurança</p> <p>13.2.3 Coleta de evidências</p> <p>15.2.2 Verificação de conformidade técnica</p> <p>15.3.2 Proteção de ferramentas de auditoria</p>
DS5.8	<p>10.8.4 Mensagens eletrônicas</p> <p>12.2.3 Integridade de mensagens</p> <p>12.3.1 Política para controles criptográficos</p>	<p>12.3.2 Gerenciamento de chaves</p> <p>15.1.6 Regulamentação de controles de criptografia</p>
DS5.9	<p>10.4.1 Controles contra códigos maliciosos</p>	<p>10.4.2 Controles contra códigos móveis</p>
DS5.10	<p>6.2.1 Identificação de riscos com partes externas</p> <p>10.6.1 Controles de redes</p> <p>10.6.2 Segurança dos serviços de rede</p> <p>11.4.1 Política de uso dos serviços de rede</p> <p>11.4.2 Autenticação para conexão externa</p>	<p>11.4.4 Proteção e configuração de portas de diagnóstico remotas</p> <p>11.4.5 Segregação de redes</p> <p>11.4.6 Controle de conexão de rede</p> <p>11.4.7 Controle de roteamento de redes</p> <p>11.6.2 Isolamento de sistemas sensíveis</p>

Processo Cobit	Requerimentos ISO 27002	
	11.4.3 Identificação de equipamento em redes	
DS5.11	6.1.5 Acordos de confidencialidade	10.8.3 Mídias em trânsito
	6.2.1 Identificação de riscos com partes externas	10.8.4 Mensagens eletrônicas
		10.9.1 Comércio eletrônico
	10.8.1 Políticas e procedimentos para troca de informações	11.4.2 Autenticação para conexão externa
	10.8.2 Acordos para troca de informações	

### 3.5. NIST

NIST (*National Institute of Standards and Technology*) é uma agência federal americana pertencente ao departamento de comércio (*U.S. Departamento of Commerce*) com a missão de promover a inovação e a competitividade industrial dos Estados Unidos, através da metrologia, padrões e tecnologia, de forma a aumentar a segurança econômica e melhorar a qualidade de vida (NIST, 2010).

Há quatro programas conduzidos pelo NIST que auxiliam no alcance da missão:

1. *NIST Laboratories*, o qual conduz pesquisas de infraestrutura tecnológica que promovem a melhoria contínua dos produtos e serviços da indústria americana.
2. *Baldrige National Quality Program*, responsável por promover a excelência de desempenho entre os fabricantes americanos, prestadores de serviços, institutos de educação e organizações sem fins lucrativos.
3. *Hollings Manufacturing Extension Partnership*, uma rede nacional de centros locais que oferecem assistência técnica e comercial para empresas de menor porte.

4. *Technology Innovation Program* compartilha custos com indústria, universidade e consórcios que realizam pesquisas em tecnologias potencialmente revolucionárias e que atendem as necessidades sociais e nacionais.

### **3.5.1. SEGURANÇA DE INFORMAÇÃO SOB A PERSPECTIVA DO NIST**

Há aproximadamente 250 documentos sobre segurança de informação publicados pelo NIST composto pelos:

- *Federal Information Processing Standards (FIPS)* é a série oficial das publicações relacionadas aos padrões de segurança e diretrizes para atendimentos da lei americana *Federal Information Security Management Act de 2002*, promulgada em 2002.
- *Special Publication 800-series* descreve as pesquisas, diretrizes e outros esforços em segurança de sistemas de informação, bem como atividades colaborativas com indústria, governos e organizações acadêmicas.
- *ITL (Information Technology Laboratory) Bulletins* são publicados pelo Laboratório de Tecnologia da Informação que apresenta em cada discussão tópicos de interesses significativos da comunidade de sistemas de informação.
- *NIST Interagency Report* é uma série que pode relatar os resultados de projetos de interesses temporários ou limitados. Podem incluir também, versão intermediária ou final de trabalhos executados pelo NIST aos patrocinadores.

Para comparação com as demais estruturas descritas neste trabalho, adotou-se o documento SP800-53 publicado em dezembro de 2007 (Ross, 2007); pois estabelece diretrizes para a seleção e especificação de controles para sistemas de informação. Desta

forma, possibilita verificar a relação com os principais riscos de integridade, confidencialidade e disponibilidade das informações, identificados neste trabalho.

Os controles de segurança descritos no SP800-53 estão organizados em 03 estruturas, a saber:

1. Técnico – conhecidos também como controles automatizados, são implementados e executados diretamente pelos sistemas de informação através de mecanismos contidos nos hardwares, softwares e aplicações.
2. Gerencial — controles indiretos, cujo foco é no gerenciamento do risco e o de segurança de sistemas de informação.
3. Operacional — controles realizados diretamente por pessoas, também conhecidos como controles manuais.

### **3.5.1.1 MATRIZ DE RISCOS DE SEGURANÇA DA INFORMAÇÃO PARA O NIST SP800-53**

Para cada um dos riscos associados aos processos de segurança da informação descritos no CobiT, foram mapeadas as atividades de controles através do entendimento e interpretação de cada um dos requerimentos referenciados na tabela 3.4 obtida a partir do estudo publicado pelo ISACA “*Mapping of NIST SP800-53 Rev 1 with CobiT 4.1*” (Ross, 2007). Como resultado, foram identificados 34 controles que endereçavam 12 dos 13 riscos apresentados (IT GOVERNANCE INSTITUTE, 2007), cujo detalhamento pode ser encontrado no Anexo D - Matriz de Riscos e controles para o NIST SP800-53.

Tabela 3. 4 – Relacionamento dos Processos CobiT com requerimentos do NIST 800-53 (IT GOVERNANCE INSTITUTE, 2007)

Processo Cobit	Requerimentos NIST 800-53
DS5.1	Não há processos relacionados no NIST 800-53 com relação a este domínio.
DS5.2	PL-1 Políticas e procedimentos de planejamento da segurança PL-2 Plano de segurança de sistemas PL-4 Regras de conduta SC-1 Políticas e procedimentos de proteção de comunicação e sistema
DS5.3	IA-1 Políticas e procedimentos de Identificação e Autenticação IA-2 Identificação e autenticação de usuário IA-4 Gestão de Identidade
DS5.4	AC-2 Gerenciamento de conta de usuário IA-4 Gestão de identidade PS-6 Acordos de acesso
DS5.5	AU-6 Comunicação, Análise e Monitoramento de Auditoria CA-2 Avaliação de Segurança CA-6 Certificação de Segurança CA-7 Monitoramento Contínuo CM-4 Monitoramento das mudanças de configuração RA-5 Mapeamento de vulnerabilidades SI-4 Técnicas e ferramentas de monitoramento do sistema de segurança
DS5.6	IR-1 Políticas e procedimentos de resposta a incidentes IR-6 Comunicação dos incidentes
DS5.7	PE-4 Controle de acesso para os meios de transmissão SC-3 Isolamento da função de segurança SA-5 Documentação dos sistemas de informação
DS5.8	SC-12 Gerenciamento e geração de chave criptográfica SC-13 Uso de criptografia válida
DS5.9	SC-18 Código Móvel SI-3 Proteção de código malicioso SI-7 Integridade de software e informação SI-8 Proteção de Spam
DS5.10	AC-4 Aplicação do fluxo de informação SC-7 Proteção das fronteiras SI-4 Técnicas e ferramentas de monitoramento do sistema de segurança
DS5.11	AU-10 Não repúdio SC-9 Confidencialidade da transmissão SC-16 Transmissão de parâmetros de segurança SC-23 Autenticidade da sessão

Processo Cobit	Requerimentos NIST 800-53
	SC-11 Caminho confiável

### 3.6. CONSIDERAÇÕES SOBRE AS ANÁLISES INDIVIDUAIS DAS ESTRUTURAS DE TRABALHO E NORMAS

As análises individuais do CobiT, ITIL, ISO 27002 e NIST SP800-53 possibilitaram a identificação de 201 atividades de controle para mitigação dos riscos relacionados aos processos de segurança da informação conforme demonstrado no quadro resumo da tabela 3.5. O detalhamento de cada matriz de riscos e controles pode ser encontrado nos Anexos A, B, C e D.

Na avaliação dos controles, foi possível perceber similaridades entre as boas práticas, pelo fato de serem voltados a objetivos comuns; por isto no capítulo 4 houve uma análise comparativa entre eles, visando definir um modelo unificado de riscos e controles de segurança da informação sem que sejam consideradas atividades que tenham a mesma abordagem, porém apenas com descrição distinta.

Tabela 3. 5 – Quadro resumo das atividades de controles por boa prática

Processos	Atividades de controle por boa prática:				
	CobiT	ISO	ITIL	NIST	Total
DS5.1 Gerenciamento da segurança	3	4	2	0	9
DS5.2 Plano de segurança de TI	5	8	2	4	19
DS5.3 Gestão de Identidade	5	9	4	3	21
DS5.4 Gerenciamento de contas de usuários	3	15	7	3	28
DS5.5 Testando Segurança	6	8	2	7	23
DS5.6 Definição de	2	5	2	2	11

<b>Processos</b>	<b>Atividades de controle por boa prática:</b>				
Incidente de Segurança					
DS5.7 Proteção de Tecnologia de Informação	2	28	1	3	34
DS5.8 Gerenciamento de chave criptográfica	4	5	0	2	11
DS5.9 Prevenção, detecção e correção de software malicioso	4	2	0	4	10
DS5.10 Segurança de Rede	4	11	1	3	19
DS5.11 Intercâmbio de dados sensíveis	3	8	0	5	16
Total Geral	41	103	21	36	201

## **4. PROPOSTA DE MODELO PARA AVALIAÇÃO DE RISCOS DA SEGURANÇA DA INFORMAÇÃO**

O modelo proposto para avaliação de segurança da informação é a base da solução de auditoria contínua deste trabalho; pois é onde serão definidos os riscos e controles passíveis de monitoramento, quanto ao grau de exposição.

Para definição de um modelo unificado foram consideradas as boas práticas e recomendações descritas em cada uma das estruturas de trabalho do CobiT e ITIL, e nas normas de segurança ISO 27002 e NIST 800-53. O objetivo foi o de preparar uma matriz de riscos e controles mais abrangente e completa, pois apesar de haver estudos iniciados nesta área, todos eram voltados a comparações individuais (IT Governance Institute, 2006-2008) entre os modelos de segurança e não apresentavam a descrição dos controles, mas apenas a referência onde seria encontrado.

Foi definido como base de comparação entre as boas práticas, o processo do CobiT, denominado de DS5 - segurança de sistemas, pelo fato de ser voltado a governança de TI e por já existir estudos visando a convergência com outros modelos de segurança utilizados neste trabalho. Neste sentido, no capítulo 3, foram associados cada controle recomendado individualmente pelo ITIL, NIST 800-53 e ISO 27002 com o processo de Segurança da Informação e riscos descritos no CobiT, para que ao final fosse possível o relacionamento e comparação entre eles.

### **4.1. DEFINIÇÃO DA MATRIZ DE RISCOS E CONTROLES UNIFICADA**

Para a consolidação e preparação do modelo unificado foram analisadas as 201 atividades de controle identificadas no capítulo 3, sendo 41 (20%) do CobiT, 103 (51%) da ISO, 21 (10%) do ITIL e 36 (18%) do NIST conforme demonstrado na Figura 4.1. A partir de comparações visando identificar complementaridade, similaridade e sobreposição entre os controles, foram selecionados aquelas que apresentavam a descrição mais clara e completa da boa prática e as que apareciam somente em uma das estruturas de trabalho ou normas. Neste



sentido, 43 foram desconsideradas por existirem outras com a mesma abrangência, conforme apresentado no ANEXO F.

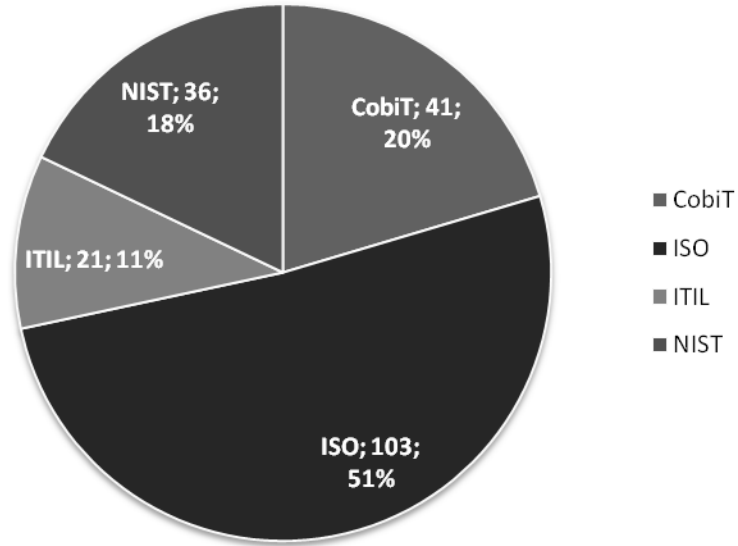


Figura 4. 1 – Composição do Modelo Unificado

Como resultado, foram identificadas 158 controles conforme demonstrado na tabela 4.1, dos quais 38 mitigavam mais de um risco e, portanto foram contados mais de uma vez. Desta forma, ao desconsiderar a repetição, a matriz de riscos e controles unificada totaliza um número real de 114 atividades de controle cujo detalhe pode ser encontrado no Anexo E. Destas, 25% estão relacionadas a atividades de controle de acesso, 15% de avaliação de riscos, controles e monitoramento, 13% definição de políticas e procedimentos, 7,5% rastreabilidade, 7% planejamento e revisão da arquitetura de rede, 6,5% parâmetros de segurança, 5,5% questões legais, 5% comunicação e tratamento de incidentes, 4,5% proteção de mensagens eletrônicas, 3,5% papéis, responsabilidades, autoridade, independência e segregação de funções, 3,5% proteção de equipamentos e mídias eletrônicas e 1,5% criptografia. As quantidades por categoria de controle estão representadas na Figura 4.2.

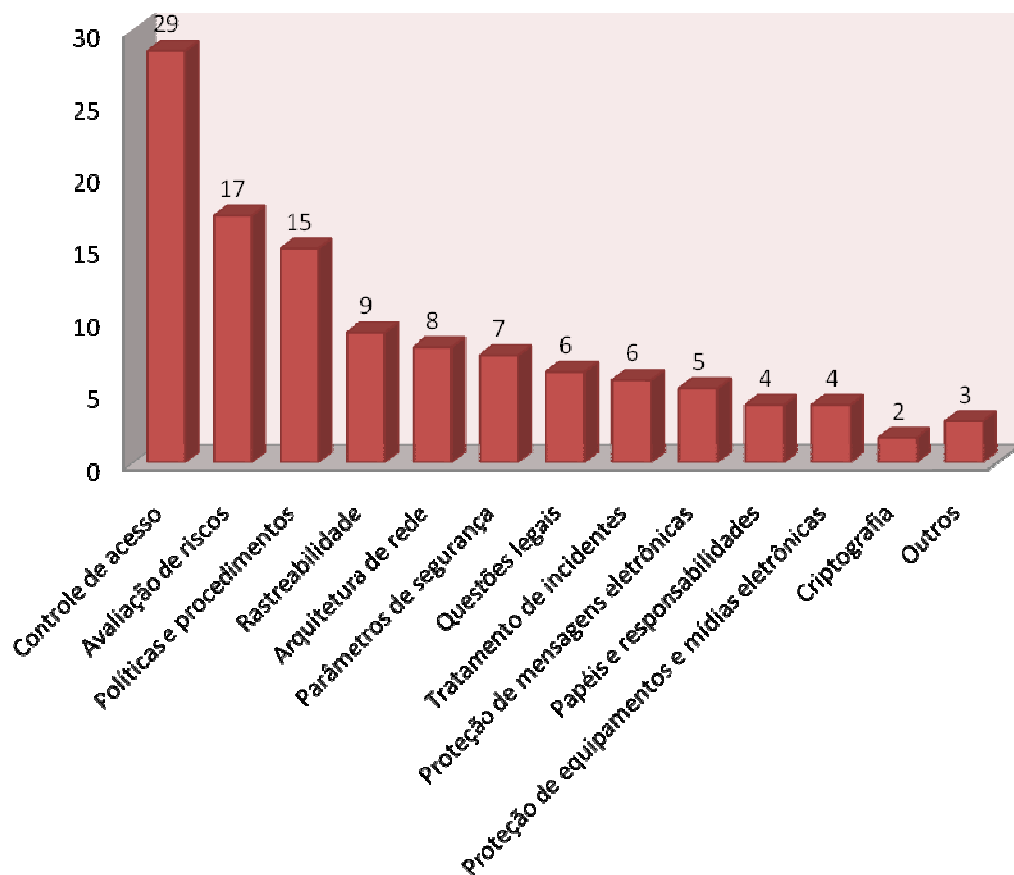


Figura 4. 2 – Distribuição em categorias de controle em quantidades

Tabela 4. 1 – Revisão dos controles após consolidação dos modelos CobiT, ITIL, ISO 27002 e NIST 800-53

Processos	Atividades de controle por boa prática:				
	CobiT	ISO	ITIL	NIST	Total
DS5.1 Gerenciamento da segurança	1	4	2		7
DS5.2 Plano de segurança de TI	2	6	2	1	11
DS5.3 Gestão de Identidade	3	9	4	2	18
DS5.4 Gerenciamento de contas de usuários	1	9	7	2	19
DS5.5 Testando Segurança	1	5	2	7	15
DS5.6 Definição de	2	5	2	2	11

<b>Processos</b>	<b>Atividades de controle por boa prática:</b>				
Incidente de Segurança					
DS5.7 Proteção de Tecnologia de Informação	2	26	1	2	31
DS5.8 Gerenciamento de chave criptográfica	3	4		1	8
DS5.9 Prevenção, detecção e correção de software malicioso	3	2		3	8
DS5.10 Segurança de Rede	2	11	1	3	17
DS5.11 Intercâmbio de dados sensíveis	3	7	0	3	13
Total Geral	23	88	21	26	158

As etapas adotadas para seleção dos controles da matriz de riscos estão representadas de forma gráfica na figura 4.3

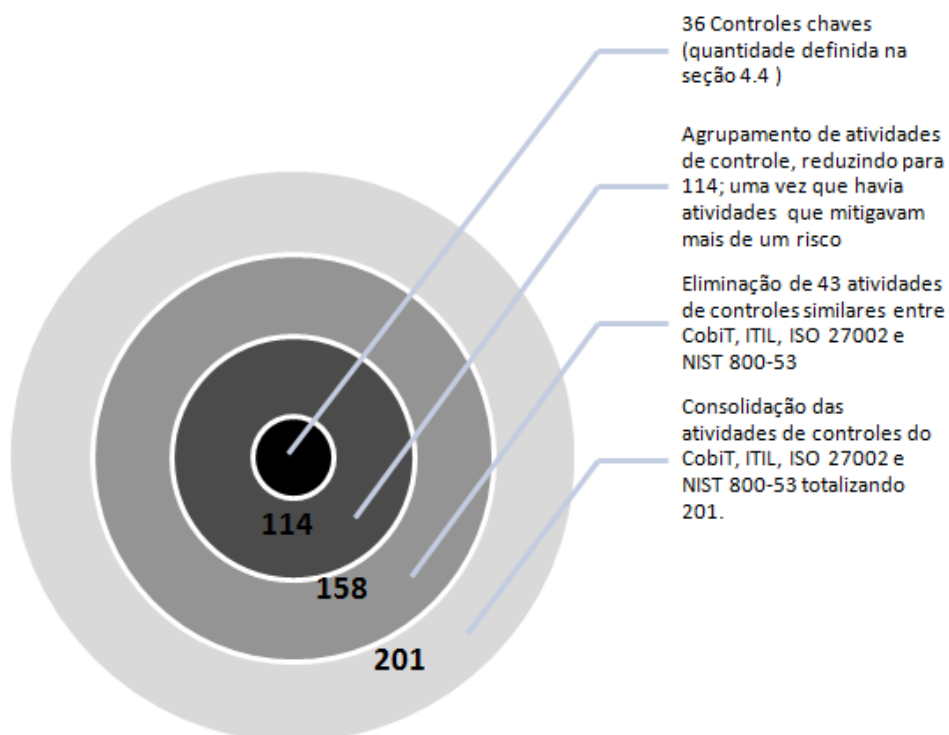


Figura 4.3 – Etapas de seleção das atividades de controles

Do resultado das comparações, foi possível perceber que as atividades de controle do CobiT eram um tanto genéricas, até pelo seu propósito de oferecer direcionamento a todos os

### **4.3. MÉTRICAS E INDICADORES PARA O MODELO DE MONITORAMENTO CONTÍNUO**

As avaliações da efetividade dos controles nas grandes corporações são efetuadas por auditores internos (Coderre, 2005), geralmente com bases amostrais, em intervalos cíclicos e depois de meses que as atividades já ocorreram, ou seja, durante períodos prolongados a empresa pode permanecer com a exposição ao risco sem que ao menos tenha condições de decidir se vai aceitar, transferir, mitigar ou evitar.

Um grande desafio do gerenciamento dos riscos é realizar a medição tempestiva, para que a tomada de decisão, seja realizada com base em informações claras, objetivas e oportunas.

Questões como (Jaquith, 2007) “Os controles estão promovendo o comportamento desejado? Quanto estou perdendo ou posso vir a perder por não investir em Segurança da Informação? ou a Segurança da Informação está melhor este ano? poderiam ser realizadas sem que respostas em tempo hábil para decisão da alta administração fossem apresentadas.

A implementação de um processo de monitoramento contínuo, baseado na definição de indicadores e métricas para acompanhamento e avaliação de riscos (Deloitte, 2009), pode responder a estas questões e apoiar a organização no gerenciamento de riscos e tomada de decisão.

O COBIT define o controle de monitoramento como um processo para medir a eficácia da gestão de TI, o qual inclui a definição de indicadores de desempenho relevantes, informes sistemáticos e oportunos, bem como o estabelecimento de uma ação em caso de desvios encontrados. Adicionalmente, define que o monitoramento é necessário para assegurar que as atividades sejam feitas de forma correta e alinhadas às políticas e diretrizes estabelecidas, além de permitir quantificar valores para verificar se as atividades podem ser feitas ainda melhor (IT GOVERNANCE INSTITUTE, 2009).

Desta forma, um componente crucial do processo de monitoramento, é a definição de uma boa métrica, a qual deve ser completa, concisa, consistente, clara, relevante e transparente. A seguir, detalhamos um pouco mais cada um destes requisitos (Jaquith, 2007).

Completa para abranger todas as áreas de segurança, envolvendo a tríade clássica de pessoas, processos e tecnologias. O risco de alguns painéis de controle é o de focar somente na tecnologia, especificamente em um sistema operacional ou banco de dados, e não cobrir outros aspectos como a capacitação técnica dos profissionais ou até um processo de avaliação de riscos.

Concisa, uma vez que profissionais de segurança são tentados a informar detalhes importantes, porém pouco esclarecedores para o público da área de negócio que não tem o conhecimento técnico ou tempo suficiente para entender. Desta forma, informar o suficiente para compreensão do indicador é um dos desafios. Certa vez o famoso Blaise Pascal<sup>17</sup> redigiu “Eu escrevi esta carta mais longa que o usual, porque não tive tempo para escrevê-la mais curta”.

Clara, não significa que a métrica seja simplificada, mas sim que seja apresentada através de uma linguagem simples para comunicar o que se deseja, utilizando também os recursos gráficos para facilitar o entendimento. Além disso, pode ser informada com anotações, principalmente quando medida ao longo do tempo. Por exemplo, em um determinado período houve o aumento significativo de tentativas de acesso inválidas, possivelmente, pelo fato de que à época a empresa havia realizado uma demissão em massa. Além disso, o *layout* do painel de controle deve ser devidamente preparado, para evitar a confusão do público com a mistura de assuntos na visualização. Recomendável que tenha um conjunto de visões maior que três e menor que seis.

Relevante, pois não adianta incluir uma série de métricas simplesmente porque é possível medir e demonstrar o quão técnico é a área de Segurança da Informação, se não forem relevantes para uma tomada de decisão. Uma das perguntas que se deve fazer ao construir uma métrica é, para que serve isto?

Transparente, uma vez que apresentar cores em vermelho, amarelo ou verde como um semáforo é fácil. Se as pessoas não entendem o que significa ou o que tornou a cor vermelha, ou até de quanto está se falando, pode por exemplo, induzir tomada de decisão de demitir funcionários sem saber o motivo. Neste sentido, as métricas devem ser apresentadas em

---

<sup>17</sup> Blaise Pascal contribuiu decisivamente para a criação de dois novos ramos da matemática: a Geometria Projetiva e a Teoria das probabilidades.

unidades de medidas e com dados que permitam entender se a situação vem ocorrendo ao longo do tempo, se são casos isolados, etc.

#### **4.4. IDENTIFICAÇÃO DOS CONTROLES CHAVES**

Conforme vimos anteriormente, implementar métricas só porque é possível medir, não traz os resultados necessários para tomada de decisão no processo de monitoramento contínuo. Neste sentido, para focar no que de fato é relevante para a organização, utiliza-se o conceito de controle chave.

Segundo PCAOB<sup>18</sup> (*Public Company Accounting Oversight Board*) (PCAOB, 2004) e GAIT (*Guide to the Assessment of IT Risk*) for Business and IT Risk (THE INSTITUTE OF INTERNAL AUDITORS, 2008), controle chave é aquele que sozinho pode mitigar os riscos em níveis aceitáveis, ou seja, se falhar há uma probabilidade razoável de que erros materiais não sejam prevenidos ou detectados tempestivamente.

O tema controle chave tornou-se um pouco mais popular dentro das organizações, após 30 de julho de 2002, quando foi assinada a lei Sarbanes Oxley. A lei determinava que as empresas de capital aberto que tivessem ações negociadas na bolsa de Nova Iorque deveriam ter seus controles internos certificados por uma empresa de auditoria externa (One Hundred Seventh Congress of the United States of America, 2002). Com isto, foram recomendados critérios para identificação de controles pelo PCAOB, visando auxiliar na definição do que era é mais importante.

Desta forma, para determinar os controles chaves dentro de um universo de 114 atividades para a empresa analisada, foi adotado o conceito de que para ser um chave o controle deve prevenir que determinado risco se materialize. Por exemplo, a atividade de somente cadastrar uma conta de usuário e atribuir privilégios de acesso mediante a autorização do responsável é um controle que visa prevenir que pessoas não autorizadas realizem atividades dentro dos sistemas da companhia. No caso, de atividades de revisão como a, de perfis de acesso, o objetivo é de detectar eventuais erros, visando corrigir alguma

---

<sup>18</sup> Agência reguladora estabelecida pela Lei Sarbanes-Oxley, que tem o encargo de supervisionar, regulamentar, inspecionar e disciplinar as empresas de auditoria externa em seus papéis de auditores de companhias abertas.

falha do controle preventivo de autorização de acesso. Neste sentido o controle de revisão somente seria selecionado caso não existisse o controle de autorização ou não houvesse confiança o suficiente na sua efetividade.

As etapas para realização das atividades de identificação dos controles chaves, seguiram os passos do PCAOB, conforme a seguir:

1. Definição da materialidade<sup>19</sup> pela alta administração em conjunto com os auditores externos. Na companhia avaliada o valor da materialidade correspondia a 5% da receita bruta.
2. Identificação dos processos críticos. Para identificação dos processos críticos foram relacionados às contas contábeis impactadas por cada um deles, visando determinar a relevância de cada processo para a organização. Do total de 3278 contas contábeis dentro do plano de contas da companhia, 661 foram selecionadas através do critério de materialidade.
3. Identificação dos sistemas aplicativos que suportavam os processos classificados como críticos. Para esta atividade foram identificadas mais de 100 aplicações que suportavam os processos críticos, como contas a pagar, contas a receber, tesouraria, compras, recebimento de mercadorias, estoques e outros sistemas de negócio da companhia. Neste caso, para determinar a relevância de cada sistema, foram realizadas as seguintes análises para classificação de cada um e atribuídos notas, considerando se:
  - poderia causar impacto direto ou indireto nas demonstrações financeiras;
  - o valor das transações processadas na aplicação estava acima da materialidade definida;
  - poderia ser utilizado para realização de fraudes;
  - continha informações confidenciais;
  - causaria danos à imagem da companhia em caso de incidentes;
  - tinha impacto regulatório;

---

<sup>19</sup> qualquer valor que possa distorcer as demonstrações financeiras da companhia e afetar inclusive a opinião dos auditores externos e impactar os acionistas, está diretamente ligada à tolerância aos riscos da companhia.

- poderia afetar a continuidade dos negócios.
4. Relacionamento dos sistemas aplicativos com cada um dos 13 riscos de Segurança da Informação.
  5. Associação dos controles aos sistemas aplicativos classificados como críticos
  6. Definição dos controles chaves em conjunto com os auditores externos e internos, área de tecnologia de informação e gestão de riscos.

Para identificação de cada controle chave foi realizada uma análise do nível de confiança que deveria ser estabelecido para cada um, levando em consideração a infraestrutura tecnológica (Exemplo: sistema operacional, banco de dados, plataforma tecnológica, etc.) que suportava cada uma das aplicações, tolerância da administração, classificação do risco associado e a probabilidade de que o controle pudesse operar efetivamente, incluindo a seguinte avaliação:

- Mudanças ocorridas no volume ou natureza das transações que pudessem afetar adversamente o desenho ou efetividade do controle;
- Mudanças no desenho do controle ou de pessoas chaves que executavam o controle ou efetuavam o monitoramento;
- Nível de confiança no controle, conforme histórico de incidentes, pesquisa de avaliação de controles, desempenho da pessoa que executava o controle ou automação do processo;
- Complexidade do controle (Ex: Quantidade de transações processadas, tipo de autenticação)
- Opinião dos auditores externos e internos, área de riscos e de tecnologia da informação.

Neste sentido, do total de 114 atividades de controle, foram identificados 36 (32%) que foram considerados suficientes, ou seja chave, para minimizar em nível aceitável cada risco associado. O processo para definição dos controles chaves está representado na Figura 4.8 e a relação dos controles chaves selecionados está descrito no ANEXO K.



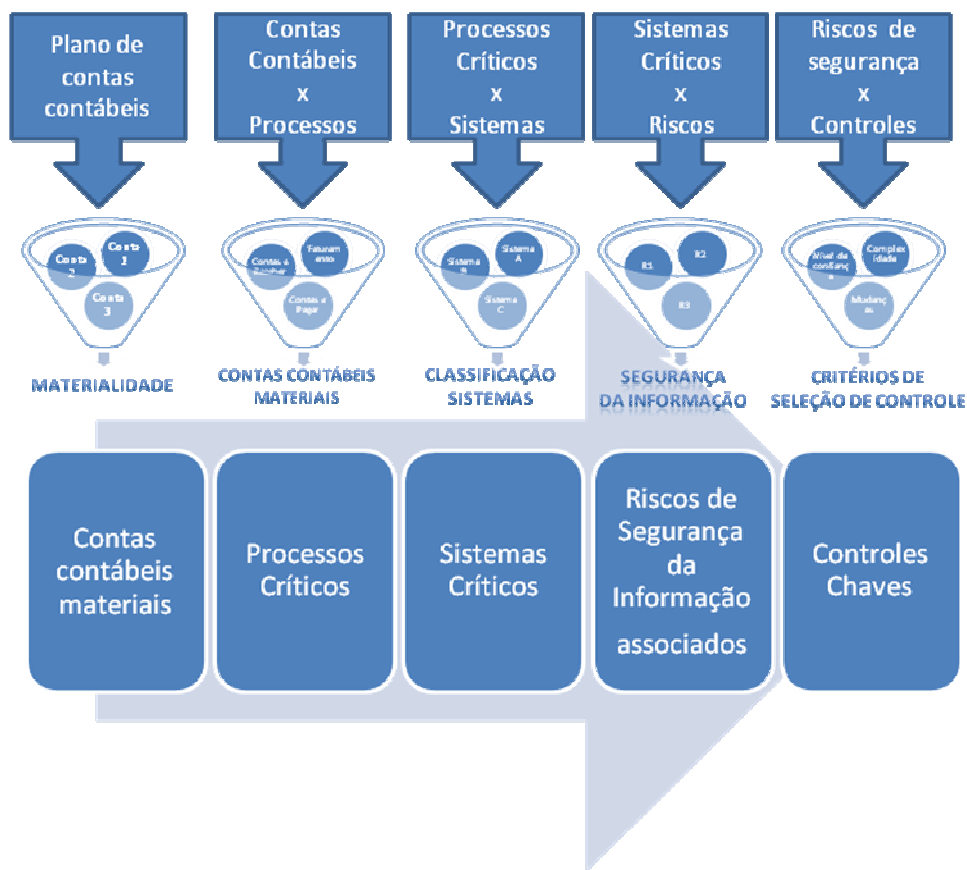


Figura 4. 8 – Processo para identificação dos controles chaves

O principal objetivo, da identificação de controles chaves, foi o de permitir que a administração priorizasse os mais relevantes e assegurasse que estes funcionavam conforme planejado. Importante ressaltar, que não significa que as demais atividades de controle não fossem importantes e que deveriam ser abandonadas, o objetivo foi o de envidar esforços para implementação do que de fato era prioritário de acordo com a tolerância ao risco e materialidade definida pela alta administração.

Após a definição dos controles chaves dos processos de Segurança da Informação, conclui-se a última etapa da definição da matriz de riscos unificada, contemplando a classificação dos riscos inerentes alto, médio e baixo. Na próxima seção, serão tratadas as métricas e indicadores necessários para implementar o modelo de monitoramento contínuo.

#### 4.5. DEFINIÇÃO DOS INDICADORES E MÉTRICAS

Os conceitos de indicadores apresentados na seção 4.3 e as análises que originaram no modelo unificado de matriz de riscos com os respectivos controles chaves, foram estudos realizados para estruturar o modelo para avaliação contínua dos processos de Segurança da Informação.

Neste sentido, o monitoramento será realizado através de acompanhamento dos indicadores de riscos, composto pelos 13 apontados na matriz de riscos e as métricas por sua vez criadas, conforme veremos a seguir, com base em técnicas de auditoria para avaliação dos 36 controles classificados como chaves (Bellino, 2007) e métricas sugeridas em literaturas e fóruns de discussão (Jaquith, 2007).

**RITI.01:** Ações de segurança de informação desalinhada com os objetivos de negócio da companhia.

As métricas e as regras aplicadas para apuração dos indicadores relacionadas ao risco RITI.01 estão descritas na tabela 4.3 .

Tabela 4. 3 – Métricas o desalinhamento dos objetivos de negócio

<b>Métricas</b>	<b>Regra aplicada</b>	<b>Ponto de Inflexão</b>
<b>M01.</b> Quantidade de riscos altos que não possuem controles mitigatórios ou que falharam mais de uma vez nos últimos 12 meses	Comparação do resultado dos indicadores do mês atual com os dos últimos 12 meses	Incidência de indicadores de risco alto nos último 12 meses.

<b>Métricas</b>	<b>Regra aplicada</b>	<b>Ponto de Inflexão</b>
<b>M02.</b> Quantidade de incidentes de segurança recorrentes	Agrupamento dos registros de incidentes de segurança recorrentes classificados como críticos	<ul style="list-style-type: none"> <li>• Registros de incidentes de segurança classificados como críticos e que foram recorrentes nos últimos 12 meses</li> <li>• Incidentes concentrados em um mesmo tipo de evento</li> <li>• Incidentes concentrados em um sistema ou recurso tecnológico</li> </ul>
<b>M03.</b> Quantidade de riscos altos não cobertos por políticas, normas e procedimentos.	Comparação das regras de segurança formalizadas em políticas, normas e procedimentos com as regras implementadas nos indicadores do monitoramento contínuo	Ausência de regras de segurança para qualquer um dos indicadores de riscos monitorados.

**RITI.02:** Descumprimento das regras de Segurança da Informação por ausência de planos para divulgação e conscientização das políticas, normas e procedimentos vigentes na empresa.

As métricas e as regras aplicadas para apuração dos indicadores relacionadas ao risco RITI.02 estão descritas na tabela 4.4.

Tabela 4. 4 – Métricas para descumprimento das regras de segurança da informação

<b>Métricas</b>	<b>Regra aplicada</b>	<b>Ponto de Inflexão</b>
<b>M04.</b> Quantidade de funcionários ou terceiros que não realizaram treinamento de segurança de informação.	Confronto da relação de funcionários e prestadores de serviço com a grade de treinamentos de segurança requeridos pela companhia e a lista de presença dos treinamentos.	Funcionários ou prestadores de serviços que não realizaram os treinamentos de segurança de informação em um período de 12 meses após a admissão.

<b>Métricas</b>	<b>Regra aplicada</b>	<b>Ponto de Inflexão</b>
<b>M05.</b> Quantidade de políticas, normas e procedimentos não divulgados	Comparação das políticas divulgadas por canais de comunicação da companhia com as publicadas e aprovadas pela administração.	Qualquer política de segurança, procedimento ou norma de segurança de informação que não foi divulgada até um mês da publicação.

**RITI.03:** Plano de Segurança da Informação incompatível com a infraestrutura tecnológica, cultura, legislação, investimentos e os requisitos de negócio da companhia, dificultando a implementação e expondo a companhia a ameaças.

As métricas e as regras aplicadas para apuração dos indicadores, relacionadas ao risco RITI.03 estão descritas na tabela 4.5.

Tabela 4.5 – Métricas para Plano de segurança incompatível com a infraestrutura tecnológica

<b>Métricas</b>	<b>Regra aplicada</b>	<b>Ponto de Inflexão</b>
<b>M01.</b> Quantidade de riscos altos que não possuem controles mitigatórios ou que falharam mais de uma vez nos últimos 12 meses	Comparação do resultado dos indicadores do mês atual com os dos últimos 12 meses	Incidência de indicadores de risco alto nos últimos 12 meses.
<b>M02.</b> Quantidade de incidentes de segurança recorrentes	Agrupamento dos registros de incidentes de segurança recorrentes classificados como críticos	<ul style="list-style-type: none"> <li>• Registros de incidentes de segurança classificados como críticos e que foram recorrentes nos últimos 12 meses</li> <li>• Incidentes concentrados em um mesmo tipo de evento</li> <li>• Incidentes concentrados em um sistema ou recurso tecnológico</li> </ul>

**RITI.04:** Dificuldade ou impossibilidade de atribuição de responsabilidades por ações realizadas no ambiente computacional, expondo a companhia a fraudes e desfalques.

As métricas e as regras aplicadas para apuração dos indicadores relacionadas ao risco RITI.04 estão descritas na tabela 4.6.

Tabela 4. 6 – Métricas para impossibilidade de atribuição de responsabilidades

<b>Métricas</b>	<b>Cálculo</b>	<b>Ponto de Inflexão</b>
<b>M06.</b> Quantidade de operações críticas sem rastreabilidade	Comparação de todas as transações consideradas críticas com os logs contendo os registros eletrônicos das operações realizadas no ambiente tecnológico	<ul style="list-style-type: none"> <li>• Operação crítica que não gera logs</li> <li>• Operação crítica que não registra informações do tipo de operação ou data ou a conta de usuário responsável pelo acesso.</li> <li>• Operação crítica que registra somente a última atividade</li> </ul>
<b>M07.</b> Quantidade de contas de usuários que não podem ser atribuídas a uma pessoa	Comparação de todas as contas de usuários cadastradas nos sistemas críticos e as respectivas infraestruturas com o cadastro de funcionários e terceiros que trabalham na companhia	Conta de usuário não associada a um prestador de serviço ou funcionário, excluindo as de sistema e de serviço.

**RITI.05:** Operações realizadas por pessoas com privilégios de acesso inadequados e/ou incompatíveis com a função, acarretando em perdas financeiras, interrupção dos negócios e/ou prejuízo a imagem da companhia.

As métricas e as regras aplicadas para apuração dos indicadores relacionadas ao risco RITI.05 estão descritas na tabela 4.7.

Tabela 4. 7 – Métricas para privilégios de acesso inadequados

Métricas	Regra Aplicada	Ponto de Inflexão
<p><b>M08.</b> Excessivo número de contas de usuários com acesso irrestrito ao sistema</p>	<ul style="list-style-type: none"> <li>• Comparação das contas de usuários privilegiados com a relação de funcionários e prestadores de serviço que trabalham na companhia</li> <li>• Comparação das contas de sistema e serviço com a relação de um proprietário responsável por cada uma</li> </ul>	<ul style="list-style-type: none"> <li>• Contas de usuários privilegiados maior que 2 por recurso tecnológico</li> <li>• Contas de serviço e sistema sem um responsável formal</li> </ul>
<p><b>M09.</b> Quantidade de contas de usuários com acesso indevido</p>	<ul style="list-style-type: none"> <li>• Comparação dos privilégios de acesso das contas de usuários com as respectivas aprovações eletrônicas</li> <li>• Confronto entre os privilégios de acesso atribuídos aos usuários com a matriz que aponta conflitos de segregação de funções em transações</li> <li>• Comparação da relação de funcionários e prestadores de serviços transferidos de funções com os seus respectivos privilégios de acesso</li> </ul>	<ul style="list-style-type: none"> <li>• Contas de usuário sem a aprovação do privilégio de acesso</li> <li>• Contas de usuário com inadequada segregação de funções nos acessos concedidos</li> <li>• Contas de usuários pertencentes a funcionários ou prestadores de serviço transferidos e cujos perfis de acesso não tenham sido removidos.</li> </ul>

**RTTI.06:** Operações realizadas por contas de usuários inválidas ou fictícias, aumentando a exposição a fraudes e desfalques.

A métrica e as regras aplicadas para apuração dos indicadores relacionadas ao risco RITI.06 estão descritas na tabela 4.8.

Tabela 4. 8 – Métricas para contas de usuário inválidas ou fictícias

Métricas	Cálculo	Ponto de Inflexão
<b>M10.</b> Quantidade de contas de usuários cadastradas de forma não autorizada ou que permanecem com acesso ativo indevidamente	<ul style="list-style-type: none"> <li>• Comparação da relação de funcionários e prestadores de serviços ativos, em férias, demitidos e de licença médica com a relação de cadastro de usuários de todos os sistemas críticos e infraestruturas relacionadas.</li> <li>• Conciliação entre a relação de todas as contas de usuários registradas nos sistemas críticos e infraestrutura relacionada com as respectivas aprovações do acesso.</li> </ul>	<ul style="list-style-type: none"> <li>• Contas de usuários em férias ou afastados com acesso ativo</li> <li>• Contas de usuário cadastradas sem a devida aprovação</li> <li>• Contas de usuário que não puderam ser associadas a um funcionário ou prestador de serviço</li> <li>• Contas de usuários pertencentes a funcionários ou prestadores de serviço demitidos e com acesso ativo ao sistema.</li> </ul>

**RTTL07:** Ausência de monitoramento e revisão dos riscos de Segurança da Informação, possibilitando que vulnerabilidades decorrentes do descumprimento de políticas, mudança do ambiente tecnológico e novas brechas sejam exploradas por pessoas mal intencionadas.

As métricas e as regras aplicadas para apuração dos indicadores relacionadas ao risco RITI.07 estão descritas na tabela 4.9.

Tabela 4. 9 – Métricas para ausência de monitoramento de riscos

Métricas	Cálculo	Ponto de Inflexão
<b>M01.</b> Quantidade de riscos altos que não possuem controles mitigatórios ou que falharam mais de uma vez nos últimos 12 meses	Comparação do resultado dos indicadores do mês atual com os dos últimos 12 meses	Incidência de indicadores de risco alto nos últimos 12 meses.

<b>Métricas</b>	<b>Cálculo</b>	<b>Ponto de Inflexão</b>
<b>M02.</b> Quantidade de incidentes de segurança recorrentes	Agrupamento dos registos de incidentes de segurança recorrentes classificados como críticos	<ul style="list-style-type: none"> <li>• Registos de incidentes de segurança classificados como críticos e que foram recorrentes nos últimos 12 meses</li> <li>• Incidentes concentrados em um mesmo tipo de evento</li> <li>• Incidentes concentrados em um sistema ou recurso tecnológico</li> </ul>

**RTTI.08:** Fraudes e desfalques decorrentes de incidentes de segurança não detectados e tratados tempestivamente.

As métricas e as regras aplicadas para apuração dos indicadores relacionadas ao risco RITI.08 estão descritas na tabela 4.10.

Tabela 4. 10 – Métricas para incidentes de segurança não detectados

<b>Métricas</b>	<b>Cálculo</b>	<b>Ponto de Inflexão</b>
<b>M11.</b> Quantidade de incidentes de segurança não tratados adequadamente	<ul style="list-style-type: none"> <li>• Agrupamento dos registos de incidentes de segurança recorrentes classificados como críticos</li> <li>• Comparação dos registos de incidentes de segurança com o tempo máximo pré-estabelecido para resposta e conclusão.</li> </ul>	<ul style="list-style-type: none"> <li>• Registos de incidentes de segurança classificados como críticos e que foram recorrentes nos últimos 12 meses</li> <li>• Tempo gasto para tratamento e/ou solução do incidente maior que o previsto</li> <li>• Incidentes reabertos</li> </ul>



Métricas	Cálculo	Ponto de Inflexão
<b>M12.</b> Concentração de incidentes de segurança em um ou mais recursos tecnológicos	<ul style="list-style-type: none"> <li>• Agrupamento por recurso tecnológico dos registros de incidentes de segurança classificados como críticos, com o cálculo de desvio padrão, média e mediana.</li> <li>• Agrupamento por tipo de evento dos registros de incidentes de segurança classificados como críticos, com o cálculo de desvio padrão, média e mediana.</li> </ul>	<ul style="list-style-type: none"> <li>• Incidentes em um sistema ou recurso tecnológico, acima de 10% da média geral</li> <li>• Incidentes em um mesmo tipo de evento acima de 10% da média geral</li> </ul>

**RTTI.09:** Inadequada proteção das ferramentas (softwares, hardwares e documentação) utilizadas para Segurança da Informação, possibilitando que ações mal intencionadas sejam realizadas em configurações do ambiente tecnológico para burlar os mecanismos de controle.

As métricas e as regras aplicadas para apuração dos indicadores relacionadas ao risco RITI.09 estão descritas na tabela 4.11.

Tabela 4. 11 – Métricas para inadequada proteção das ferramentas de segurança

Métricas	Cálculo	Ponto de Inflexão
<p><b>M13.</b> Quantidade de senhas nos sistemas ou recursos tecnológicos que não possuem os requisitos mínimos de segurança para assegurar confidencialidade</p>	<ul style="list-style-type: none"> <li>• Comparação das parametrizações de senhas dos recursos tecnológicos (sistemas operacionais, banco de dados, aplicações, etc.) com a política de segurança definida pela companhia</li> <li>• Identificação dos registros de senhas que sejam idênticos no cadastro de contas de usuários.</li> <li>• Verificação através do cadastro de contas de usuários a data em que a senha foi trocada pela última vez</li> </ul>	<ul style="list-style-type: none"> <li>• Contas de usuário com senha padrão ou sem senha</li> <li>• Contas de usuário que nunca trocaram a senha ou que não trocam de acordo com a periodicidade estabelecida</li> <li>• Sistemas e recursos tecnológicos que não obrigam o uso de caracteres especiais, números e letras na elaboração da senha</li> <li>• Sistemas e recursos tecnológicos cujo tamanho requerido para a elaboração da senha é inferior ao estabelecido pela política de segurança, que não armazenam o histórico de senhas evitando a reutilização e bloqueiam após tentativas inválidas de acesso</li> </ul>
<p><b>M14.</b> Quantidade de senhas alteradas ou contas de usuários desbloqueadas indevidamente</p>	<ul style="list-style-type: none"> <li>• Verificação dos registros eletrônicos das operações de desbloqueio e alterações nas senhas das contas de usuários</li> </ul>	<ul style="list-style-type: none"> <li>• Alterações de senha realizada por um ID diferente do proprietário da conta sem o registro da autorização.</li> <li>• Alterações de senhas de contas de usuário efetuadas fora do horário de expediente</li> <li>• Desbloqueio da conta de usuário sem o registro da solicitação pelo responsável.</li> <li>• Acesso simultâneo de contas de usuários com endereçamento de IP que indicam localidades distintas</li> </ul>

Métricas	Cálculo	Ponto de Inflexão
<p><b>M15.</b> Quantidade de softwares maliciosos ou não homologados nas estações de trabalho dos usuários</p>	<ul style="list-style-type: none"> <li>• Confronto da relação de softwares homologados pela área de Segurança da Informação com os instalados nas estações de trabalho dos usuários e servidores</li> <li>• Confronto da relação de softwares maliciosos com os instalados nas estações de trabalho dos usuários e servidores</li> <li>• Confronto da relação de softwares de análises de vulnerabilidades e tráfego de rede instalados nas estações de trabalho dos usuários e servidores, com a relação de estação de trabalho e servidores autorizadas.</li> </ul>	<ul style="list-style-type: none"> <li>• Softwares não homologados pela Segurança da Informação</li> <li>• Softwares maliciosos instalados nas estações de trabalho pela Segurança da Informação</li> <li>• Softwares de análise de vulnerabilidade e tráfego de rede instalados em estações de trabalho não autorizadas</li> </ul>

**RTTI.10:** Comprometimento dos mecanismos de controle que evitam o não-repúdio de operações críticas realizadas no ambiente tecnológico, decorrente da perda da confidencialidade e integridade de chaves criptográficas.

As métricas e as regras aplicadas para apuração dos indicadores relacionadas ao risco RITI.10 estão descritas na tabela 4.12.

Tabela 4. 12 – Métricas para mecanismos de não-repúdio

Métricas	Cálculo	Ponto de Inflexão
<p><b>M16.</b> Quantidade de agentes externos que realizam transações críticas com a companhia que estão com o certificado ou chave criptográfica expirada, revogada ou inválida</p>	<ul style="list-style-type: none"> <li>• Verificação dos certificados de autenticidade emitidos para a realização de transações eletrônicas entre a companhia e agentes externos</li> </ul>	<ul style="list-style-type: none"> <li>• Transações de criticidade alta utilizada para comunicação com agentes externos que não exigem certificados de autenticidade da contraparte</li> <li>• Transações críticas realizadas com agentes externos com o certificado expirado ou inválido</li> </ul>
<p><b>M17.</b> Quantidade de contas de usuário com acesso indevido a geração, alteração, revogação e consulta das chaves criptográficas</p>	<ul style="list-style-type: none"> <li>• Comparação das contas de usuários autorizadas a emitir, revogar e distribuir as chaves de criptografia</li> </ul>	<ul style="list-style-type: none"> <li>• Contas de usuários não autorizadas a acessar o local de armazenamento das chaves criptográficas utilizadas para realização de transações críticas.</li> </ul>

**RTTI.11:** Interrupção dos negócios, roubo de informações e/ou prejuízo a imagem da companhia decorrente de instalação e uso de softwares maliciosos (vírus, worms, spyware, spam) no ambiente tecnológico.

As métricas e as regras aplicadas para apuração dos indicadores relacionadas ao risco RITI.11 estão descritas na tabela 4.13.

Tabela 4. 13 – Métricas para instalação e uso de softwares maliciosos

Métricas	Cálculo	Ponto de Inflexão
<p><b>M18.</b> Quantidade de computadores e dispositivos de conectividade que estão em desacordo com a política de configuração segura dos equipamentos</p>	<ul style="list-style-type: none"> <li>• Comparação da configuração segura estabelecida para as estações de trabalho e servidores com o parametrizado</li> </ul>	<ul style="list-style-type: none"> <li>• Contas de usuários locais com perfil de administrador habilitados nas estações de trabalho</li> <li>• Estações de trabalho com pacotes de segurança (patches) desatualizados</li> <li>• Contas de usuários padrão habilitadas incorretamente nas estações de trabalho, servidores e dispositivos de conectividade</li> <li>• Portas de rede habilitadas incorretamente nas estações de trabalho, servidores e dispositivos de conectividade</li> <li>• Serviços habilitados indevidamente nas estações de trabalho, servidores e dispositivos de conectividade</li> </ul>
<p><b>M19.</b> Quantidade de computadores sem software antivírus instalados ou que estão desatualizados há mais de um mês</p>	<ul style="list-style-type: none"> <li>• Verificação se todas as estações de trabalho e servidores possuem softwares antivírus instalados</li> <li>• Comparação da versão dos softwares antivírus instalados nas estações de trabalho dos usuários e servidores com o divulgado pelo fabricante</li> </ul>	<ul style="list-style-type: none"> <li>• Computadores com software antivírus desatualizados</li> <li>• Softwares maliciosos instalados nas máquinas dos usuários</li> <li>• Computadores sem software de proteção instalados contra malwares (vírus e spyware).</li> </ul>

**RTTI.12:** Invasão do ambiente tecnológico da empresa por pessoas mal intencionadas (Ex:hackers, crackers, insiders.), comprometendo a confidencialidade, disponibilidade dos sistemas e a imagem da companhia.

As métricas e as regras aplicadas para apuração dos indicadores relacionadas ao risco RITI.12 estão descritas na tabela 4.14.

Tabela 4. 14 – Métricas para invasão do ambiente tecnológico por agentes externos

Métricas	Cálculo	Ponto de Inflexão
<b>M20.</b> Quantidade de regras de segurança implementadas indevidamente nos firewall, switch e roteadores	Confronto das regras implementadas nos firewalls, roteadores e switch com as respectivas autorizações e validações da área de Segurança da Informação	<ul style="list-style-type: none"> <li>Regras de firewall, switch e roteadores sem autorização</li> </ul>
<b>M21.</b> Quantidade de sites desbloqueados para acesso com conteúdo malicioso ou inapropriado	<ul style="list-style-type: none"> <li>Comparação de uma lista sites impróprios com os bloqueados pelas companhias</li> <li>Comparação de uma lista de sites impróprios com os acessados pelos usuários da companhia</li> </ul>	<ul style="list-style-type: none"> <li>Sites maliciosos não bloqueados (Pedofilia, pornografia, hackers, drogas, racismo.)</li> <li>Sites maliciosos acessados</li> </ul>

**RTTI.13:** Transações eletrônicas inválidas e/ou não autorizadas efetuadas com parceiros de negócio (fornecedores, clientes, instituições financeiras), podendo acarretar em penalidades legais, perdas financeiras, comprometimento da confiabilidade e imagem da companhia.

A métrica e as regras aplicadas para apuração dos indicadores relacionadas ao risco RITI.13 estão descritas na tabela 4.15.

Tabela 4. 15 – Métricas para transações inválidas com parceiros de negócio

Métricas	Cálculo	Ponto de Inflexão
<p><b>M22.</b> Quantidade de operações não autorizadas e/ou realizadas em desacordo com as políticas comerciais da companhia</p>	<ul style="list-style-type: none"> <li>• Comparação das operações realizadas nos sistemas que suportam os processos de vendas, compras, contas a pagar, contas a receber, cobrança e tesouraria com as regras estabelecidas nas políticas da companhia</li> <li>• Confronto do dia e hora em que a operação foi realizada com horário de expediente e calendário de feriados nacionais e regionais.</li> </ul>	<ul style="list-style-type: none"> <li>• Operações realizadas fora do horário de expediente, sábados, domingos e feriados.</li> <li>• transações realizadas em desacordo com a política de preços e descontos da companhia</li> <li>• notas fiscais de fornecedor com datas de emissão anterior ao da emissão do pedido de compra ou que não estejam associadas a pedidos</li> <li>• transações financeiras realizadas com fornecedores e instituições financeiras em desacordo com os limites de alçada de aprovação da companhia</li> <li>• ausência de aplicação de sanções definidas na política de cobrança para clientes inadimplentes</li> <li>• transações realizadas em desacordo com a política de cobrança da companhia (Ex: alteração de vencimento, exclusão do serviço de proteção ao crédito sem autorização, etc.</li> </ul>

#### 4.6. CRITÉRIOS PARA AVALIAÇÃO DOS CONTROLES

Para avaliação dos controles foram atribuídos critérios que permitissem classificar o nível de exposição ao risco, visando demonstrar a criticidade e urgência das ações que deviam ser tomadas. Na definição do modelo foram avaliadas 8 tipos de técnicas analíticas, para a seleção daquela que atenderia o processo de monitoramento contínuo com resultados adequados para tomada de decisão. A seguir segue um resumo de cada uma: (Jaquith, 2007)

- Média – método simples para entender a tendência central de um conjunto de dados. Calculado com a soma total dos itens dividindo pelo número total dos itens
- Mediana – identifica o ponto onde a metade dos elementos está acima e a outra metade abaixo
- Desvio Padrão – mede o grau de dispersão estatístico de um conjunto de dados a partir da média, permitindo identificar se os dados tendem a agrupar-se ou são altamente irregulares
- Agrupamento – agrupa os registros de dados a partir de um atributo comum entre eles.
- Agregação – consiste em consolidar os registros dentro de sumários estatísticos por grupos de atributos e apresentando resultados como a soma, média, desvio padrão, contagem, maiores e menores valores.
- Análise de séries de tempo - visa entender o comportamento dos dados ao longo de intervalos regulares de tempo.
- Análise transversal dos dados – consiste em analisar o comportamento dos dados, avaliando mais de um atributo, ou seja, como se comporta outros atributos de um conjunto de dados
- Análise de quartil, - representa a análise dos dados em um grupo de quatro quartis, visando identificar o comportamento dos dados entre eles.
- Matrizes de correlação – explora o relacionamento entre mais que um par de atributos no tempo. Prove uma forma compacta e estruturada para analisar muitos pares de atributos de uma vez.



Para critérios de avaliação dos controles e conseqüentemente dos riscos residuais, será utilizada a técnica analítica de desvio padrão, pelo fato de que para cada risco há vários sistemas e infraestruturas relacionados, permitindo assim identificar possíveis comportamentos discrepantes entre eles. Além disso, a análise de série de tempo será considerada em todos, visando identificar e monitorar o comportamento durante períodos e sazonalidade. Durante a evolução da implementação da solução, caso seja necessário, outras técnicas poderão ser aplicadas.

#### **4.7. PROPOSTA DO MODELO DE MONITORAMENTO CONTÍNUO**

Para elaboração do modelo foram consideradas pesquisas em implementações do processo de monitoramento contínuo por outras empresas (ERNST & YOUNG, 2009) e as recomendações descritas do Global Technology Audit Guide (GTAG) (Coderre, 2005).

A estrutura do modelo baseou-se nos pontos chaves:

1. Definição do objetivo e indicadores de risco – os indicadores foram baseados na matriz unificada de Segurança da Informação, desenvolvida para proporcionar a administração uma visão da exposição aos riscos para tomada de decisões. A matriz foi elaborada, a partir de um estudo comparativo entre estruturas de trabalhos e normas reconhecidas internacionalmente, visando identificar os riscos e controles associados.
2. Cálculo e métricas para medição dos indicadores – as métricas foram desenvolvidas, adotando como base os controles classificados como chaves para mitigação dos riscos associados na matriz unificada. O escopo da avaliação dos controles, foi definido com base na identificação de processos críticos e dos sistemas aplicativos, considerando a infraestrutura tecnológica que suportavam cada um deles.
3. Método para extração e análise dos dados – A ferramenta utilizada, para análise dos dados foi o software ACL (Audit Command Language) pela capacidade que tem para trabalhar com vários formatos de arquivos (Ex: PDF, texto, relatório, dbf,

xls, sequencial, etc.) e por possibilitar a conexão em banco de dados diversos e conectividade inclusive com o sistema ERP SAP R/3. Também influenciou na decisão da ferramenta, além do conhecimento prévio da ferramenta, o fato ser uma das mais utilizadas por auditorias possibilitando inclusive o compartilhamento de informação e melhoria contínua da solução (Deloitte, 2007). O método para obtenção dos dados foi uma mescla de conexão direta ao banco de dados com a importação de arquivos texto.

4. Forma de apresentação dos resultados – Devido a limitação da ferramenta ACL, para apresentação dos resultados, a qual dependia de outros aplicativos como o Cristal Reports, foi utilizada uma ferramenta de BI (Business Intelligence) chamada Qlikview, para divulgação gráfica dos resultados obtidos. Uma vez que, conforme já comentado anteriormente, a apresentação precisa ser, dentre outros aspectos, clara, concisa e transparente.

Conforme apresentado na Figura 4.9, a arquitetura da solução busca extrair dados dos diversos recursos tecnológicos da empresa (Ex: sistema operacional, banco de dados, arquivos de configuração, etc.) de forma sistemática, automatizada e periódica e comparar as informações com as regras de negócio (Ex: Políticas, normas, procedimentos, leis, regulamentos, etc.). Caso fossem identificadas exceções, eram calculadas as métricas de volume e desvio padrão, para apresentação dos resultados em um módulo gráfico que permitisse a alta administração identificar desvios nos processos e exposição aos riscos, bem como o comportamento ao longo do tempo para responder adequadamente as situações identificadas.

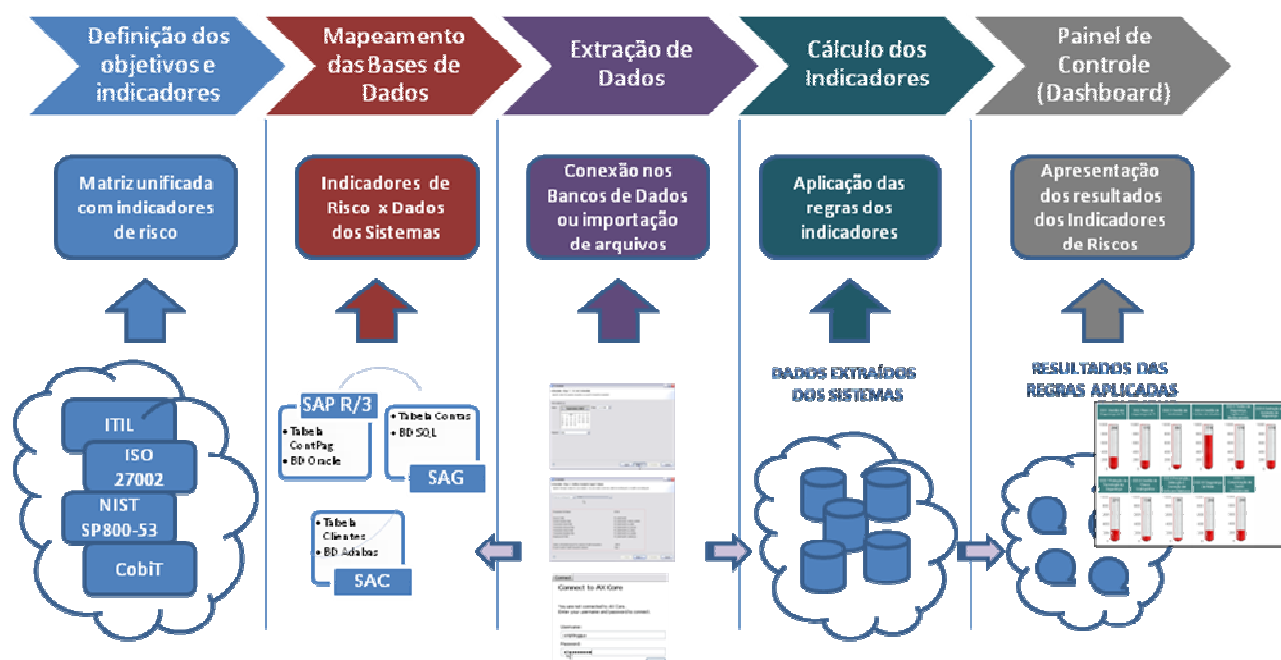






Figura 4. 9 – Solução proposta de monitoramento contínuo

A descrição das atividades necessárias para definição e implementação da solução apresentada na Figura 4.9 são detalhadas na tabela 4.16.

Tabela 4. 16 – Atividades para definição e implementação do monitoramento contínuo

Etapa	Objetivo	Macro Atividades	Atividades específicas
	Definir os indicadores de riscos para o processo de segurança de informação.	Definição de escopo	Elaboração da Matriz de Riscos e controles para o processo de Segurança da Informação baseado no domínio DS 5 do CobiT
		Definição dos indicadores de riscos	Identificação e classificação dos riscos dos processos de segurança da informação através da análise e consolidação dos controles descritos no CobiT, ITIL, ISO 27002 e NIST SP800-53
		Avaliação dos riscos inerentes	Pesquisas com os gestores da companhia e análise do histórico de incidentes para avaliação de riscos.

Etapa	Objetivo	Macro Atividades	Atividades específicas
		Definição das métricas para monitoramento dos indicadores de risco	Identificação de controles chaves que mitigavam os riscos de segurança da informação através de critérios sugeridos pelo GAIT e PCAOB e definição de métricas baseadas em técnicas de auditoria utilizadas para avaliação da efetividade de controles.
	Identificar a origem e localização dos dados necessários para medição dos indicadores de riscos	Definição dos sistemas que serão objetos de monitoração	Identificação dos processos críticos baseados em critérios de materialidade e definição dos sistemas que suportavam os processos selecionados, através da avaliação de criticidade.
		Identificação das bases de dados e campos chaves	Levantamento junto aos desenvolvedores, administradores de banco de dados e especialistas de segurança de informação, a localização das bases de dados necessários para extração e automação do processo de monitoramento contínuo.
	Extrair os dados dos sistemas de origem para medição dos indicadores	Seleção da ferramenta para análise de dados.	Definição da ferramenta com base em especificação de negócio e comparativo das soluções apresentadas, levando em consideração custo x benefício
		Identificação da melhor alternativa para extração dos dados.	<p><b><u>Tabelas de banco de Dados</u></b></p> Estabelecimento de conexão com banco de dados via ODBC, com usuário cujo acesso seja somente de consulta.
			<p><b><u>Arquivos:</u></b></p> Mapeamento dos diretórios onde arquivos serão disponibilizados para importação dos dados pela ferramenta.

Etapa	Objetivo	Macro Atividades	Atividades específicas
		Automação da rotina de extração e importação dos dados para a ferramenta de análise de dados.	Definição da periodicidade de execução e implementação de rotinas para extração automática e rotineira dos dados, bem como monitoramento de erros de execução.
			Implementação de controles para teste de integridade da base de dados extraídas, tais como: header/trailer, algoritmo de validação, controle de acesso, etc.
	<p>Apurar os resultados dos indicadores de riscos baseado em métricas previamente definidas</p>	Desenvolvimento e implementação da lógica para análise dos dados de acordo com as métricas definidas.	Desenvolvimento da lógica e homologação dos resultados com os responsáveis pelos controles, visando a validação das regras.
		Automação do processo de importação dos dados extraídos dos sistemas de origem e cálculo dos indicadores	Implementação de rotina automatizada e periódica dos cálculos dos indicadores, com controles de verificação de erros.
	<p>Definir modo de apresentação dos indicadores de riscos</p>	Definição dos gráficos para apresentação dos indicadores entre 3 e 6 níveis de visão.	Consolidação dos resultados de cada controle ao indicador de risco relacionado.
			Definição da visão de acordo com a tolerância aos riscos da administração.
		Definição do período de retenção dos dados, visando propiciar comparativo e a evolução ao longo do tempo.	Definição de política de retenção de dados de acordo com o período previamente definido pela administração de 24 meses.

#### **4.7.1. VISÃO GRÁFICA DOS INDICADORES DO MONITORAMENTO CONTÍNUO**

Para divulgação dos resultados do monitoramento contínuo foram elaboradas 03 visões gráficas, visando atingir mais de um público dentro da organização e permitindo obter o nível de detalhamento suficiente para compreensão e correção da situação identificada.

A apresentação inicial parte de uma visão macro dos processos de segurança da informação conforme demonstra a Figura 4.10, onde a seta verde representa que o nível de controle está adequado para o processo relacionado, a exclamação os que merecem atenção e ações para que não atinjam níveis indesejáveis e a seta vermelha aqueles que necessitam de uma intervenção o mais rápido possível, uma vez que estão abaixo da expectativa da companhia. A apuração dos indicadores são realizadas através dos cálculos e comparações definidos nas métricas, as quais estão associadas aos riscos e processos de segurança da informação.

A definição dos níveis de controle por processo está associada a tolerância da administração aos riscos e por este motivo a solução estabelecida deve ser flexível o suficiente para adequação a qualquer momento. Para empresa analisada, definiu-se inicialmente que se o processo tiver qualquer ocorrência associada a risco alto ou se a quantidade total de ocorrências dos indicadores associados for superior a 5% do total para risco médio e 10% para baixo, deverá ser classificado como insatisfatório.

A classificação de “atenção” será aplicada se o processo tiver qualquer ocorrência associada a risco médio ou se a quantidade total de ocorrências dos indicadores associados for superior a 5% do total para risco baixo. Importante ressaltar, que os níveis poderão ser ajustados por quantidade de ocorrências ou até classificação dos riscos conforme for obtido os primeiros resultados ou alterada a tolerância aos riscos da administração.

PROCESSOS DE SEGURANÇA DA INFORMAÇÃO		
DS5.1	Gestão da Segurança de TI	↑
DS5.2	Plano de segurança de TI	!
DS5.3	Gestão de Identidade	↓
DS5.4	Gestão de Contas de Usuário	↓
DS5.5	Testes de Segurança, Vigilância e Monitoramento	↑
DS5.6	Definição de Incidente de Segurança	↑
DS5.7	Proteção da Tecnologia de Segurança	↑
DS5.8	Gestão de Chave Criptográfica	↑
DS5.9	Prevenção, Detecção e Correção de Software Malicioso	!
DS5.10	Segurança de Rede	↑
DS5.11	Comunicação de Dados Confidenciais	↑

Legenda	
↑	nível de controles adequado
!	controles necessitam de atenção
↓	nível de controles inadequado

Figura 4. 10 – Monitoramento dos Processos de Segurança da Informação

Uma outra forma elaborada para acompanhamento, é a visão por riscos de segurança da informação, conforme apresentado na Figura 4.11. Este formato, apresenta a medição dos 13 riscos identificados e demonstra a quantidade de exceções às regras definidas em cada métrica. Inicialmente foi definida uma escala de até 1000 ocorrências, considerando o histórico de incidentes registrados em relatórios de auditoria, o qual indica que não será ultrapassada mensalmente, uma vez que não é cumulativo. Por exemplo, no risco “Contas de usuários inválidas ou fictícias”, o indicador está demonstrando que foram identificadas 484 contas de usuários nestas condições para o mês avaliado.

Esta visão adota a premissa que independente da quantidade de ocorrências, alguma regra de segurança foi violada e deve ser corrigida imediatamente, no entanto caso haja a

intenção da administração em atuar somente após x ocorrências, as cores poderão ser alteradas a qualquer momento.

Importante ressaltar, que como os riscos estão relacionados a processos e atividades de controles distintas não há uma relação direta entre eles, e desta forma as ocorrências identificadas em um deles podem ou não influenciar outros. Por exemplo, a impossibilidade de atribuição de responsabilidades, pode demonstrar que não há rastreabilidade das operações realizadas nos sistemas, o que não impede que mecanismos de não repúdio, como o controle de chaves criptográficas e validação da contraparte antes de estabelecer uma comunicação não esteja sendo realizada. Por outro lado, a falha de controles no cadastramento de contas de usuário pode fragilizar a capacidade de identificar o responsável pela operação mesmo que haja registros eletrônicos, uma vez que pode haver contas de usuários fictícias.

O nível de monitoramento por processos ou de riscos, possibilita que a alta administração tenha condições suficientes para decidir as estratégias e táticas da companhia de acordo com os resultados obtidos. No entanto, para correção dos controles e mitigação dos riscos são necessárias visões mais detalhadas, por isto foi elaborada uma visão por métrica, contendo o detalhamento das situações encontradas. Como exemplo, na Figura 4.12, são demonstradas as métricas do risco de impossibilidade de atribuição de responsabilidade, onde ao lado de cada uma está associada a relação de transações críticas que não tinham rastreabilidade e a de contas de usuários “genéricas”.



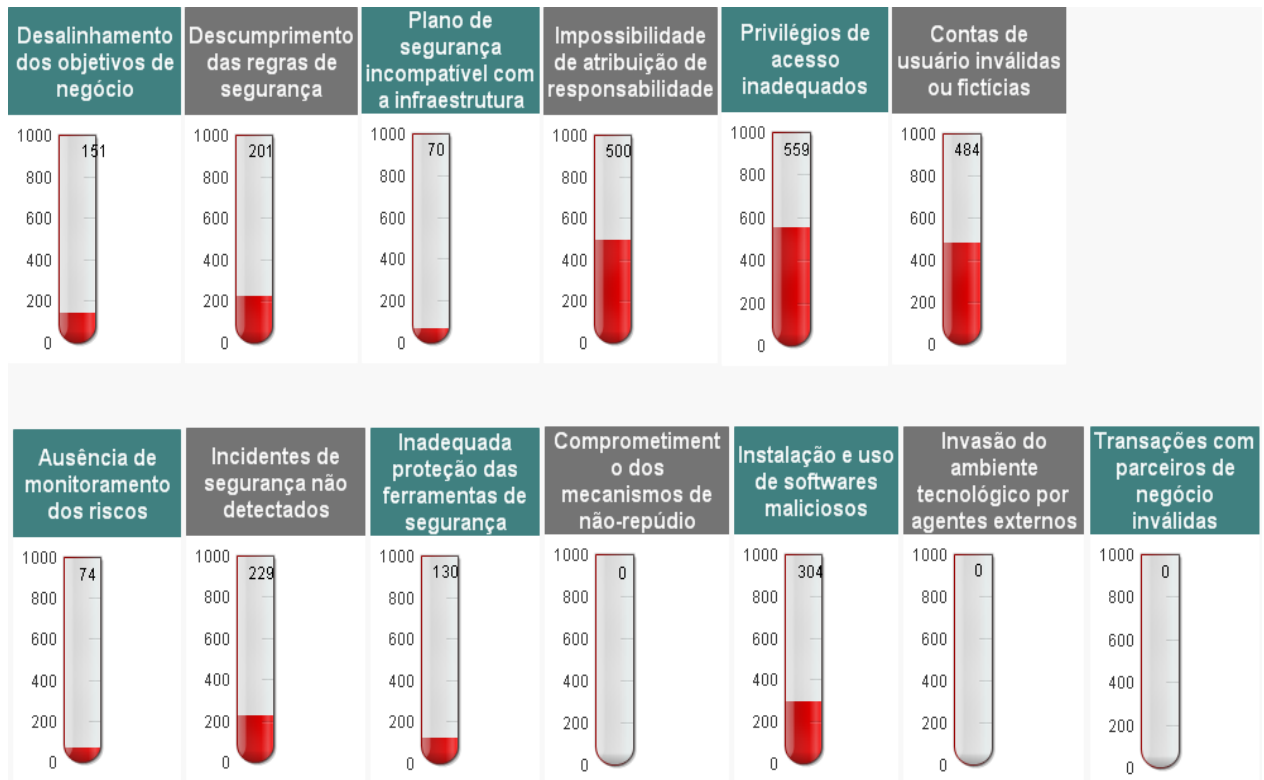


Figura 4. 11 – Monitoramento dos Riscos de Segurança da Informação

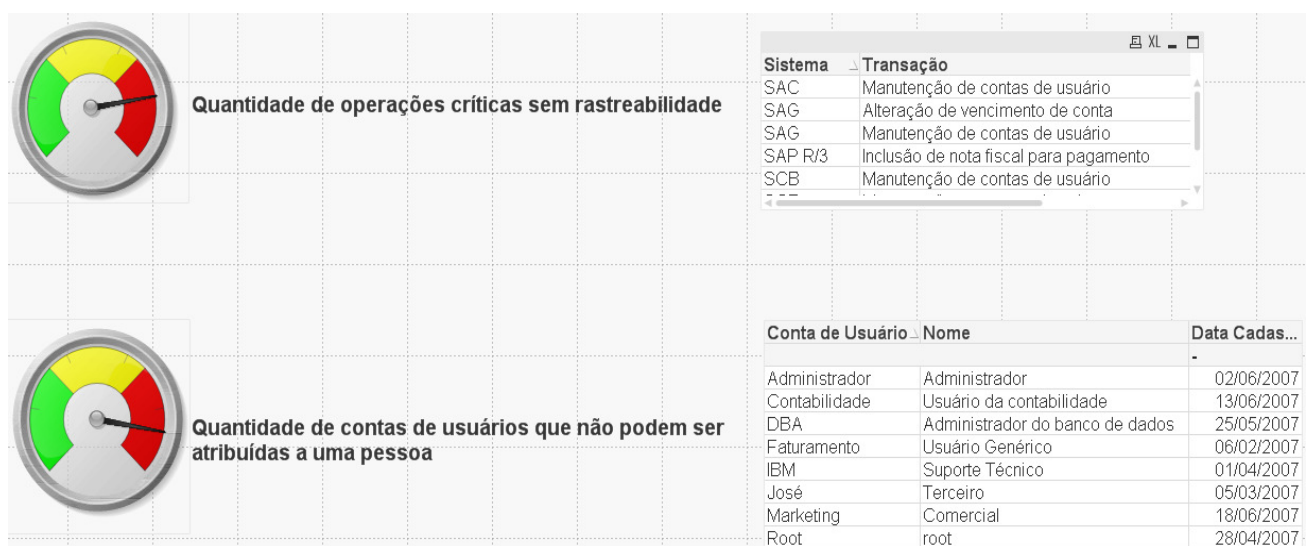


Figura 4. 12 – Métricas do Risco de Impossibilidade de atribuição de responsabilidades

Todos os indicadores foram construídos para permitir um comparativo com resultados de meses anteriores e programados para uma execução mensal através da própria ferramenta ACL, a qual permite o agendamento das rotinas. A periodicidade por ser parametrizável pode

ser alterada para execuções semanais e até diárias, mas para início do monitoramento foi adotado um intervalo que permite atingir a maturidade do processo, antes da realização de acompanhamentos diários. A título de exemplo, o gráfico da Figura 4.13 apresenta as quantidades de ocorrências identificadas para o processo de Gestão da Segurança de TI em determinado período. Neste caso, através da informação histórica é possível identificar a evolução dos controles ao longo do tempo e verificar que o motivo do decréscimo pode estar relacionado a ações mais efetivas de monitoramento dos riscos.

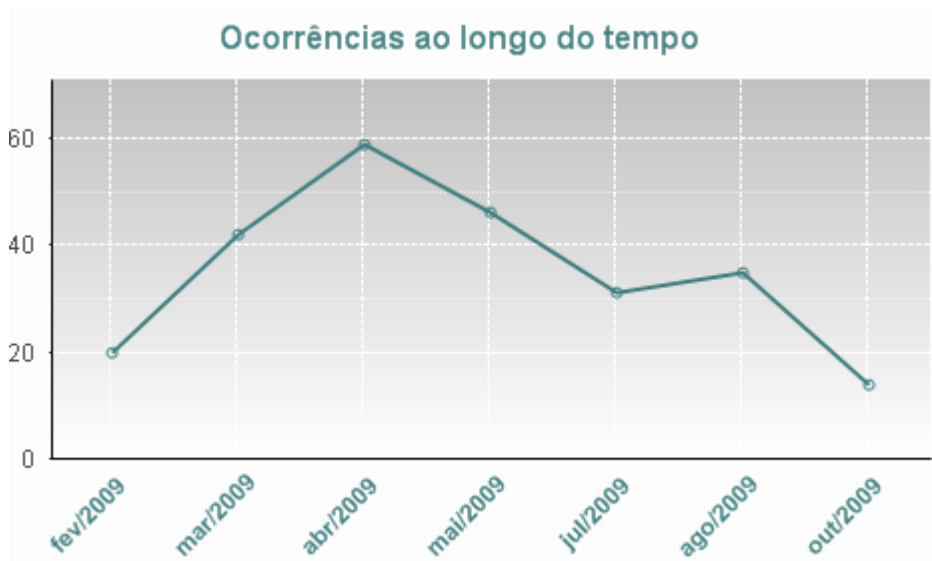


Figura 4. 13 – Gráfico das medições dos riscos ao longo do tempo

## 5. CONCLUSÃO

O gerenciamento dos riscos da segurança da informação, não deveria ser uma preocupação somente do executivo de tecnologia da informação, uma vez que suporta e visa proteger o bem mais valioso da organização contra ações mal intencionadas, como fraude, vazamento de informações, erros operacionais, indisponibilidade dos dados, dentre outros. No entanto, demonstrar a necessidade de investimento não é uma tarefa fácil, uma vez que os olhos dos acionistas estão focados no lucro e não em proteção e controle para evitar perdas e prejuízos.

Para convencer a alta administração sobre a necessidade de implementar ferramentas, criar programas de conscientização de segurança da informação, contratar serviços especializados, etc, é necessário inovar e quebrar paradigmas para demonstrar de forma clara, sucinta, transparente e rápida os riscos que podem causar interrupção dos negócios, impactos financeiros ou de receitas. Essa linguagem necessita ser de fácil compreensão para o nível de alçada que tem autonomia para a tomada de decisão.

A solução proposta neste trabalho tem como objetivo prover uma visão executiva, gráfica e interativa contendo a exposição dos riscos e deficiência nos processos de segurança da informação, através da medição periódica de indicadores associados.

Para suportar a definição dos indicadores de risco e proporcionar o diagnóstico claro e preciso da governança da segurança da informação foi elaborada uma matriz de riscos contendo mais de 150 práticas de controles recomendadas pelas estruturas de trabalho reconhecidas internacionalmente CobiT, ITIL e as normas ISO 27002 e NIST SP800-53, com a indicação daqueles controles que seriam chave para mitigação. Estudos individuais comparativos permitiram estabelecer um elo e intersecção entre eles, possibilitando identificar a complementaridade e duplicidade de controles. Para implantação e automação da solução foram utilizadas uma ferramenta de análise de dados e um software de BI (*Business Intelligence*) para demonstração gráfica dos resultados.

Visando classificar os riscos inerentes e direcionar os esforços na implantação dos indicadores o modelo contemplou um processo de pesquisa junto aos gestores da companhia, estabeleceu um método de correlação com histórico de incidentes e definiu um critério para seleção dos ativos de informação baseado em avaliação da criticidade, para que na ânsia de monitorar tudo, acabasse não monitorando nada.

Desta forma, a solução além de permitir verificar a exposição do risco residual, através da análise de 100% da base de dados relacionados a ativos de informação críticos para o negócio, possibilita que através da matriz sejam identificados quais controles necessitam ser revistos ou implementados quando os níveis estiverem em desacordo com a tolerância da organização.

Como pontos de atenção, a adoção do modelo proposto neste trabalho depende de fatores importantes, como a identificação adequada dos ativos críticos da companhia, uma vez que um grande desafio no monitoramento contínuo é o de estabelecer o que deve ser monitorado.

Além disso, por envolver infraestrutura, processos e aplicações, a solução de monitoramento contínuo deve estar integrada ao processo de gestão de mudança da companhia para que alterações significativas no ambiente tecnológico (Ex: sistema, software ou hardware) não impacte o resultado dos indicadores, acarretando em distorções e perda da credibilidade da informação apresentada.

Adicionalmente, deve-se treinar profissionais em análise forense, uma vez que poderão surgir indícios de fraude, exigindo dos profissionais técnicas de investigação e coleta de informações que não comprometam as análises.

Outro fator importante, é com relação à credibilidade das informações. A solução que apresenta resultados para gerenciamento dos riscos de segurança da informação, deve estar devidamente protegida contra acessos não autorizados, manipulações de dados, perda da integridade e confidencialidade. Uma vez que uma pessoa mal intencionada poderia explorar os pontos de maior exposição da companhia.

Por fim, há outros processos além da segurança da informação, que necessitam de um adequado gerenciamento dos riscos. A definição de modelos unificados em trabalhos futuros e criação de indicadores para processos como gestão de mudança, desastre e recuperação, segurança física, manutenção e desenvolvimento de sistemas aplicativos, gerenciamento do nível de serviço, dentre outros, proverá a organização um ambiente de governança corporativa cada vez mais confiável.

Outros aspectos, como atendimento às exigências da lei Sarbanes Oxley e requerimentos do setor bancário como os estabelecidos pelo Comitê de Supervisão Bancária, atualmente conhecido como Basileia III que dá ênfase ao gerenciamento de risco podem ser resolvidos através da definição de indicadores e avaliação de controles chaves da área de negócio por meio do conceito de monitoramento contínuo.

## REFERÊNCIAS BIBLIOGRÁFICAS

Rocha, Cláudio. **Segurança: Como tudo começou.** Disponível em: <<http://www.informabr.com.br/nbr.htm>>. Acesso em: 09 julho 2009.

ERNST & YOUNG. **Falha em segurança da informação pode ter impacto maior na reputação do que no faturamento das empresas.** Disponível em: <<http://www.ey.com/BR/pt/Issues/Managing-risk/Information-security-and-privacy>>. Acesso em: 09 julho 2009.

Horta, Joana. **Gartner: segurança da informação precisa amadurecer.** Disponível em: <<http://www.itweb.com.br/noticias/index.asp?cod=41702>>. Acesso em: 09 julho 2009.

IT WEB. **Mobilidade exige segurança.** Disponível em: <<http://www.itweb.com.br/hotsites/mobilidade/noticia.asp?cod=52072>>. Acesso em: 09 julho 2009.

Westerman, George; Hunter, Richard. **O Risco de TI: Convertendo ameaças aos negócios em vantagem competitiva.** São Paulo: Editora M Books do Brasil, 2008. 204p.

Mell, Peter; Scarfone, Karen; Romanosky, Sasha . **The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities.** Estados Unidos da América: National Institute of Standards and Technology Interagency Report 7435, Agosto.2009. 42p.

Bernstein, Terry; Bhimani, Anish B.,Schultz, Eugene; Siegek, Carol A. **Segurança na Internet.** São Paulo: Editora Campus, 1997. 461p.

Ross, Ron; Katzke, Stu; Johnson, Arnold; Swanson, Marianne; Stoneburner and Rogers, George. **Special Publication 800-53, Revision 2.** Estados Unidos da América: Estados Unidos da América: National Institute of Standards and Technology Interagency, Dez 2007. 188p.

NIST. **Guide to NIST Information Security Documents.** Estados Unidos da América: National Institute of Standards and Technology Interagency, Março 2007. 36p.

PROJECT MANAGEMENT INSTITUTE. A Guide to the Project Management Body of Knowledge: PMBOK Guide. 4. ed. Reino Unido: PMI, dezembro 2008. 459p.

DELOITTE. **Auditoria Interna no Brasil:** Um estudo inédito para retratar o atual cenário da auditoria interna no País e auxiliar as empresas a identificar as melhores práticas do segmento: Brasil: Deloitte, 2007. 20p.

KPMG. **A fraude no Brasil Relatório da Pesquisa 2004.** Brasil: KPMG, setembro 2009. 35p.

ERNST & YOUNG. **Muito Além de Compliance:** Pesquisa Global sobre Segurança da Informação da Ernst & Young 2008. Brasil: EYGM, 2008. 36p.

HP. **Fundamentos ITIL para o Gerenciamento de Serviços.** Brasil: HP, 2004. 330p.

COSO. **Gerenciamento de Riscos Corporativos:** Estrutura Integrada. **Tradução de Audibra; Price Waterhouse & Coopers.** Brasil: AICPA, 2007. 141 p. Tradução de: Enterprise Risk Management — Integrated Framework.

ABNT. **ABNT NBR ISO/IEC 17799:2005.** 2 ed., Rio de Janeiro: ABNT, 2005. 120p.

ABNT. **ABNT NBR ISO/IEC 27001:2006.** 1 ed., Rio de Janeiro: ABNT, 2006. 34p.

IT GOVERNANCE INSTITUTE. **CobiT 4.1.** Estados Unidos da América: ITGI, 2007. 212p.

IT GOVERNANCE INSTITUTE. **Aligning CobiT® 4.1, ITIL ® V3 and ISO/IEC 27002 for Business Benefit:** A Management Briefing from ITGI and OGC. Estados Unidos da América: ITGI, 2008. 131p

PCAOB. **Bylaws and Rules of the Public Company Accounting Oversight Board.** Estados Unidos: PACOB, Dezembro 2004. 360p.

Weill, Peter; Ross, Jeanne W. **Governança de TI:** Como as empresas com melhor desempenho administram os direitos decisórios de TI na busca por resultados superiores. São Paulo: Editora M Books do Brasil, 2006. 276p.

Calder, Alan; Watkins, Steve. **IT Governance** : A Manager's Guide to Data Security and ISO 27001/ ISO 27002. 4. ed. Estados Unidos da América: Kogan Page, 2008. 385p

IT GOVERNANCE INSTITUTE. **The Risk IT Framework**. Estados Unidos da América: ITGI, 2009. 107p

Instituto Brasileiro de Governança Corporativa. **Guia de Orientação para gerenciamento de Riscos Corporativos**. São Paulo: IBGC, 2007. 48p.

KPMG. **2º. Estudo sobre as Melhores Práticas de Governança Corporativa no Brasil e nos Estados Unidos – 2007 Base – Relatório Anual 20F**. Brasil: KPMG, 2007. 20p.

GONSALVEZ, Elisa Pereira. **Conversas sobre iniciação à pesquisa científica**. 4 ed. Campinas, São Paulo: Editora Alínea, 2005. 80p.

SEVERINO, Antônio Joaquim. **Metodologia do Trabalho Científico**. 22 ed. São Paulo: Editora Cortez, 2002

DELOITTE. **Taking Control**: A guide to compliance with section 404 of the Sarbanes Oxley Act of 2002. Brasil: Deloitte. 2004. 43p.

KPMG. **Sarbanes-Oxley Section 404**: Management's Assessment Process Frequently Asked Questions. Estados Unidos da América: KPMG, 2004. 20p.

One Hundred Seventh Congress of the United States of America. **Sarbanes Oxley Act 2002**. Estados Unidos da América. Disponível em: <<http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf>> . Acesso em: 10 de maio de 2010. 66p

THE INSTITUTE OF INTERNAL AUDITORS. **GAIT for Business and IT Risk**. Estados Unidos: THEIIA, mar 2008. 22p

THE INSTITUTE OF INTERNAL AUDITORS. **GAIT Methodology**: A risk-based approach to assessing the scope of IT general controls. Estados Unidos: THEIIA, ago 2007. 41p

David A. Richards, Alan S. Oliphant, Charles H. Le Grand. **Global Technology Audit Guide**: Information Technology Controls. Estados Unidos: THEIIA. Mar 2005, 62p.



Coderre, David. **Global Technology Audit Guide: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment.** Estados Unidos: THEIIA. 2005, 41p.

Bellino, Christine; Wells, Jefferson; Hunt, Steve. **Global Technology Audit Guide: Auditing Application Controls.** Estados Unidos: THEIIA, julho 2007, 34p.

IT GOVERNANCE INSTITUTE. **COBIT MAPPING: MAPPING OF ISO/IEC 17799:2005 WITH COBIT 4.0.** Estados Unidos da América: ITGI, 2006. 43p

IT GOVERNANCE INSTITUTE. **COBIT MAPPING: Mapping of ITIL v3 with COBIT® 4.1** Estados Unidos da América: ITGI, 2008. 65p

IT GOVERNANCE INSTITUTE. **COBIT MAPPING: Mapping of NIST SP800-53 Rev 1 With COBIT® 4.1.** Estados Unidos da América: ITGI, 2007. 58p

IT GOVERNANCE INSTITUTE. **Information Security Governance: Guidance for Boards of Directors and Executive Management 2<sup>nd</sup> Edition.** Estados Unidos da América: ITGI, 2006. 52p

IT GOVERNANCE INSTITUTE. **An Introduction to the Business Model for Information Security.** Estados Unidos da América: ITGI, 2009. 28p

IT GOVERNANCE INSTITUTE. **Implementing and Continually Improving IT Governance.** Estados Unidos da América: ITGI, 2009. 74p

Office Government Commerce. **ITIL V3 Service Operation Book.** Reino Unido: Stationery Office, Maio 2007. 263p.

Office Government Commerce. **ITIL V3 Service Design Book.** Reino Unido: The Stationery Office, Maio 2007. 334p.

Jaquith, Andrew. **Security Metrics Replacing Fear, Uncertainty, and Doubt.** Estados Unidos da América: Pearson Education, Março 2007. 335p.

DELOITTE. **Implementando Auditoria Contínua em Tesouraria de Bancos.** In: 6°. Congresso Internacional de Gestão de Tecnologia e Sistemas de Informação, São Paulo, Brasil, junho 2009.

ERNST & YOUNG. **Continuous Control Monitoring Metodologia de Implementação**. In: 6º. Congresso Internacional de Gestão de Tecnologia e Sistemas de Informação, São Paulo, Brasil, junho 2009.

ISO. **ISO/IEC 27005:2008. Information Technology - Security techniques – Information security risk management**. Suíça: ISO, Junho 2008. p61.

ISO. **ISO 31000:2009 Risk Management - Principles and guidelines on implementation**. Suíça: 2009. p24

ERNST & YOUNG. **À Frente da Mudança: 12ª Pesquisa Global sobre Segurança da Informação**. Brasil: EYGM, 2010. p28.

ISACA. CobiT Online. Apresenta os riscos dos processos e técnicas para testes de controles. Disponível em: <<http://www.cobitonline4.info/>>. Acesso em: 30 outubro 2009.

DELOITTE. **2007 Global Security Survey: The shifting security paradigm**. Estados Unidos da América: Deloitte, 2007. 48p.

Metrics Center. Serviço dedicado a fornecer métricas de segurança de informação. Disponível em: <<https://www.metricscenter.net/>>. Acesso em: 30 de maio 2010.

AUDINET. Apresenta técnicas de auditoria para testes de controles . Disponível em: <<http://www.auditnet.org/>>. Acesso em: 05 de maio 2010.

KPMG. **A fraude no Brasil Relatório da Pesquisa 2009**. Brasil: KPMG, 2009. 35p.

ISACA. Top Business / Technology Issues Survey Results. Estados Unidos da América: ITGI. 2008. 35p.

Price Waterhouse & Coopers. **Trial by fire what Global executives expect of information security – in the middle of the world’s worst economic downturn in thirty years**. Estados Unidos da América: PW&C, 2010. 50 p.

NIST. **Assessment of Access Control Systems – Interagency Report 7316**. Estados Unidos da América: National Institute of Standards and Technology Interagency, Setembro 2006. 60p.

NIST. **Risk Management Guide for Information Technology Systems – Special Publication 800-30**. Estados Unidos da América: National Institute of Standards and Technology Interagency, Julho 2002. 55p.

FEBRABAN. **O Setor Bancário em Números**. In: 20ª Congresso CIAB Febraban. São Paulo, Brasil, Junho 2010.

McKINSEY&COMPANY. **Global Investor Opinion Survey: Key Findings**. Disponível em:

<<http://www.mckinsey.com/clientservice/organizationleadership/service/corpgovernance/pdf/globalinvestoropinionsurvey2002.pdf>>. Acesso em: 19 junho 2010.

NIST. Apresenta informações institucionais do National Institute of Standards and Technology. Disponível em: <<http://www.nist.gov/index.html>>. Acesso em: 19 junho 2010.

Instituto Brasileiro de Governança Corporativa. **Código das Melhores Práticas de Governança Corporativa**. São Paulo: IBGC, 2009. 73p.

Office Government Commerce. **The Official Introduction to the ITIL Service Lifecycle**. Reino Unido: Stationery Office, Janeiro 2007. 238p.

Peotta, Laerte. **Proposta de Metodologia de Gestão de Risco em Ambientes Corporativos na área de TI**. Brasília: UnB, 2008. 181p.