Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Camila Kawakami Avila

ALCANÇANDO A CONFORMIDADE DE NORMAS E LEIS INTERNACIONAIS ATRAVÉS DA NORMA TÉCNICA ISO/IEC 27002

Uma relação de requisitos fundamentais que atendam às normas e leis de segurança da informação dos diversos setores no cenário mundial

Rio de Janeiro

2010

Camila Kawakami Avila

ALCANÇANDO A CONFORMIDADE DE NORMAS E LEIS INTERNACIONAIS ATRAVÉS DA NORMA TÉCNICA ISO/IEC 27002

Uma relação de requisitos fundamentais que atendam às normas e leis de segurança da informação dos diversos setores no cenário mundial

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Prof^{o}. Luiz Fernando Rust da Costa Carmo, Ph.D. - (LAAS/CNRS) - França - 1994

Rio de Janeiro
2010

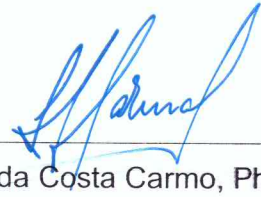
Camila Kawakami Avila

ALCANÇANDO A CONFORMIDADE DE NORMAS E LEIS INTERNACIONAIS ATRAVÉS DA NORMA TÉCNICA ISO/IEC 27002

Uma relação de requisitos fundamentais que atendam às normas e leis de segurança da informação dos diversos setores no cenário mundial

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em março de 2010.



Prof°. Luiz Fernando Rust da Costa Carmo, Ph.D. - (LAAS/CNRS) - França - 1994

Dedico este trabalho a minha família, especialmente à minha mãe, que sempre me incentivou a buscar por novos horizontes e oportunidades.

AGRADECIMENTOS

Gostaria de agradecer ao NCE que viabilizou a oportunidade de cursar o programa de treinamento MOT-CN, especialmente ao Nilson Theobald.

A todos os colegas de trabalho que conheci e que compartilharam comigo experiências e conhecimentos, principalmente à equipe do Suporte de Sistemas do NCE, onde aprendi grande parte do conhecimento que possuo hoje e conheci ótimas pessoas.

A todos os queridos amigos que de alguma forma me ensinaram com suas vivências e conhecimentos.

Ao Fernando Lima pelas sugestões e incentivo.

Ao meu noivo, Willer Junior, pela motivação e paciência.

À minha família pelo estímulo e apoio em todos os momentos.

E a todos aqueles que, de alguma forma, contribuíram para tornar tudo isso possível.

RESUMO

AVILA, Camila Kawakami. **ALCANÇANDO A CONFORMIDADE DE NORMAS E LEIS INTERNACIONAIS ATRAVÉS DA NORMA TÉCNICA ISO/IEC 27002:** uma relação de requisitos fundamentais que atendam às normas e leis de segurança da informação dos diversos setores no cenário mundial. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2009.

Com a grande evolução dos recursos tecnológicos e a crescente dependência desses recursos nos processos empresariais, as empresas tornam-se mais vulneráveis a crimes e fraudes digitais. Por esse motivo e por exigência de clientes e parceiros, a necessidade de conformidade normativa, especialmente no departamento de TI aumentou significativamente nos últimos anos. Tal necessidade abrange inúmeros setores, entre eles: financeiro/contábil, público, financeiro de pagamentos com cartões de crédito e sobre cuidados de saúde.

Neste trabalho foi realizada uma análise comparativa entre as normas e leis existentes no mercado, tais como as normas do setor financeiro/contábil (Basiléia II, *Gramm-Leach-Bliley Act* – GLBA, *Sarbanes Oxley - SOX*), do setor público (*Federal Information Security Management Act* - FISMA), do setor financeiro de pagamentos com cartões de crédito (*Payment Card Industry Data Security Standard* - PCI-DSS) e sobre cuidados de saúde (*Health Insurance Portability and Accountability Act* - HIPAA), ressaltando as exigências comuns entre elas e como essas exigências podem ser implementadas com o auxílio das boas práticas descritas pela ISO 27002. Essa análise gerou um compendio sobre as mais importantes normas e leis vigentes no mercado informatizado e tem como objetivo auxiliar a equipe de TI a identificar e implementar os requisitos necessários para alcançar a conformidade com mais de um regulamento.

ABSTRACT

AVILA, Camila Kawakami. **ALCANÇANDO A CONFORMIDADE DE NORMAS E LEIS INTERNACIONAIS ATRAVÉS DA NORMA TÉCNICA ISO/IEC 27002:** uma relação de requisitos fundamentais que atendam à normas e leis de segurança da informação dos diversos setores no cenário mundial. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2009.

As a result of technological resources evolution, as well as its dependency on companies' lawsuits, companies became more vulnerable to digital crimes and frauds. Due to this fact, in addiction to clients and partners demands, the demand to develop a normative conformity, especially on IT department, increased significantly the last years. It ranges various sectors, including financial/accountantship, public, credit card payments' financial and health care.

A comparative analysis between patterns and existing market laws was developed in this work. Financial/accountantship sector's standard *Basiléia II, Gramm-Leach-Bliley Act – GLBA, Sarbanes Oxley – SOX*, public sector's standard *Federal Information Security Management Act – FISMA*, credit card payments' financial sector's standard *Payment Card Industry Data Security Standard - PCI-DSS* and health care sector's standard *Health Insurance Portability and Accountability Act – HIPAA* were compared with ABNT ISO/IEC 27002, highlighting common demands between them and how these demands could be implemented by assuming good practices described in ISO 27002. This analysis leaded to a compendium about the most important patterns and available laws in the computerized market, and it targets to assist IT team to identify and implement necessary requirements to achieve conformity based on more than one regulation.

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
BIS	Bank of International Settlements
CoBIT	Control Objectives for Information and related Technology
ePHIs	Informações de Saúde Eletrônicas Protegidas
FISMA	Federal Information Security Management Act
FIPS	Federal Information Processing Standards
GLBA	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
ISMS	Information Security Management System
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
PCI	Payment Card Industry
PHI	Protected Health Information
SOX	Sarbaney-Oxley
UPS	Uninterruptible Power Supply

LISTA DE FIGURAS

Página
Figura 1 – ISO/IEC 27002 84

LISTA DE TABELAS

Página
Tabela 1 – Análise comparativa de requisitos 49

SUMÁRIO

1 INTRODUÇÃO 13
2 O QUE É SEGURANÇA DA INFORMAÇÃO? 15
2.1 INFORMAÇÃO 15
2.2 CICLO DE VIDA DA INFORMAÇÃO 15
2.3 SEGURANÇA DA INFORMAÇÃO 16
2.4 PRINCÍPIOS BÁSICOS DA SEGURANÇA DA INFORMAÇÃO 16
2.4.1 O Princípio da Integridade 16
2.4.2 O Princípio da Confidencialidade 16
2.4.3 O Princípio da Disponibilidade 17
2.5 INCIDENTE DE SEGURANÇA 17
2.6 POLÍTICA DE SEGURANÇA 17
3 NORMAS E REGULAMENTAÇÕES 19
3.1 REGULAMENTO TÉCNICO 19
3.2 NORMAS TÉCNICAS 19
3.3 PRINCIPAIS NORMAS E LEIS INTERNACIONAIS 20
3.3.1 Basileia II 20
3.3.2 Gramm-Leach-Bliley Act (GLBA) 20
3.3.3 Sarbanes-Oxley Act (SOX) 22
3.3.4 Federal Information Security Management Act (FISMA) 23
3.3.5 Payment Card Industry Data Security Standard (PCI - DSS) 24
3.3.6 Health Insurance Portability and Accountability Act (HIPAA) 24
3.3.7 Norma ISO 27002:2005 25
4 PRINCIPAIS CONTROLES DA NORMA ISO/IEC 27002 26
4.1 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO 26
4.2 GESTÃO DE ATIVOS 27
4.3 SEGURANÇA EM RECURSOS HUMANOS 28
4.4 SEGURANÇA FÍSICA E DO AMBIENTE 28
4.5 GESTÃO DAS OPERAÇÕES E COMUNICAÇÕES 29
4.5.1 Procedimentos e responsabilidades e controle de documentação 30
4.5.2 Procedimentos de *backups* 30
4.5.3 Controle e prevenção de vírus 31
4.5.4 Procedimentos para uso da internet 32
4.5.5 Segurança do serviço de correio eletrônico 33
4.5.6 Segurança de mídias de armazenamento 34
4.5.7 Controle de redes 35
4.5.8 Controle de acessos 35
4.5.9 Controle de acesso de usuários 35
4.5.10 Utilização de senhas 36
4.5.11 Controle de acesso ao sistema operacional 38
4.5.12 Acesso remoto 39
4.5.13 Roteamento de redes 41
4.6 GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO 41
4.7 CONFORMIDADE 41
4.7.1 Direito de propriedade intelectual 42
4.7.2 Conformidade com as políticas e normas de segurança da informação 42
5 ANÁLISE COMPARATIVA 44

6 CONCLUSÃO 52
7 REFERÊNCIAS BIBLIOGRÁFICAS 54
ANEXOS 60
I BASILEIA II – GLOBAL 60
II GRAMM-LEACH-BLILEY ACT (GLBA) 66
III SARBANES-OXLEY ACT (SOX) 69
IV FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) 71
V PAYMENT CARD INDUSTRY (PCI) SECURITY STANDARD – GLOBAL 74
VI HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) 76
VII NORMA ABNT NBR ISO/IEC 27002:2005 82

1 INTRODUÇÃO

“Contrariando a tendência a diminuir investimentos face à crise econômica mundial, a necessidade de garantir a Segurança da Informação segue crescente para a continuidade dos negócios, para a conformidade com os regulamentos vigentes e para a proteção aos dados da empresa e de parceiros de negócio.”

Michael Rasmussen

O advento da Informática na automação de processos empresariais trouxe novos riscos aliados a uma dependência inegável da tecnologia da informação para a agilidade, a continuidade e a perpetuidade dos mais variados tipos de negócios. À medida que essa dependência aumenta, as empresas tornam-se mais vulneráveis a crimes e fraudes cometidos através dos recursos computacionais que elas tanto necessitam. Além disso, a globalização e as fortes pressões econômicas, cada vez mais latentes introduziram e redesenharam os conceitos e práticas de transparência, equidade, prestação de contas e responsabilidade corporativa, que estão crescentemente aderindo ao mundo empresarial [10].

Ao longo dos últimos dez anos, houve um impacto significativo e crescente da necessidade de conformidade normativa, especialmente no departamento de TI [1]. Cumprir com essas leis e normas, é uma carga crescente para as empresas, que enfrentam um conjunto de desafios normativos, da diretoria ás bases de negócio. Os órgãos regulamentadores ao redor do mundo têm concentrado as normas em numerosas áreas: emprego/trabalho, comércio global, anticorrupção, controles financeiros/contábeis, entre outros adentrando setores como ciências biomédicas, bancos, seguradoras e serviços públicos. Essa pressão por cumprir a conformidade

não vem somente de órgãos reguladores, mas também dos clientes e parceiros de negócios [1].

A partir desse contexto, a preocupação de algumas empresas, integrantes dos mais diversos setores do mercado com o tema Segurança da Informação tem aumentado consideravelmente [10].

Com base nesse cenário, esta monografia tem como objetivo gerar um compendio sobre as mais importantes normas e padrões relacionados à Segurança da Informação nos diversos setores do mercado mundial que surgiram atualmente. Os principais aspectos e características de cada regulamento são apresentados para que de posse desses dados sejam definidos quais controles são necessários para cada setor. Tais controles serão definidos de acordo com o que sugere a norma técnica NBR ISO/IEC 27002:2005, que possui uma estrutura mais flexível para uma abordagem proativa de riscos e da conformidade.

O trabalho descrito a seguir estrutura-se da seguinte maneira: o capítulo um relata uma breve introdução da proposta e dos temas que serão abordados no decorrer dos demais capítulos. O segundo capítulo esclarece temas como segurança da informação e alguns de seus principais componentes. O conceito de normas e regulamentações, assim como a uma breve descrição das mesmas é apresentado no capítulo 3. No quarto capítulo são apresentadas as principais seções da norma ABNT ISO/IEC 27002. O quinto capítulo é a própria arquitetura de controles, uma análise comparativa entre os padrões e normas apresentados, enumerando os requisitos necessários para que uma instituição alcance a conformidade com tais regulamentos. O capítulo seis expõe a conclusão do trabalho e a seção de anexos contém uma descrição detalhada das principais normas e leis, assim como seus requisitos.

2 O QUE É SEGURANÇA DA INFORMAÇÃO?

2.1 INFORMAÇÃO

Informação é aquilo que sintetiza a natureza de tudo o que existe ou ocorre no mundo físico [2]. Segundo Laudon et al.[3], a informação pode se manifestar de várias maneiras, isto é, de forma escrita, eletrônica ou impressa. Ela representa um conjunto de dados dos quais são modificados e tomam forma útil e significativa. Por esse motivo, a informação necessita estar sempre protegida, seja qual for a sua forma de manifestação.

2.2 CICLO DE VIDA DA INFORMAÇÃO

De acordo com Sêmola [4], o ciclo de vida da informação é composto e identificado pelos momentos vividos pela informação e que a colocam vulnerável. Esses momentos acompanham os ativos físicos, humanos e tecnológicos que fazem uso, alteram ou descartam a informação.

O manuseio, o armazenamento, o transporte e o descarte das informações são etapas que constituem o ciclo de vida da informação. O manuseio é a etapa onde a informação é criada e manipulada. A etapa de armazenamento, como o próprio nome já diz, consiste no armazenamento da informação, seja em um banco de dados, em um papel, em um DVD, entre outros. A próxima etapa, de transporte, ocorre quando a informação é transportada para algum local, não importando o meio no qual a mesma está armazenada. A última parte do ciclo da informação é o momento de descarte da informação. Essa fase pode ser observada quando, por

exemplo, algum documento impresso é depositado na lixeira ou um arquivo eletrônico é eliminado ou até mesmo quando alguma mídia de armazenamento (CDs, DVDs, disquetes, *pen-drives*) é descartada por apresentar falha no acesso a seus dados. Todas as fases do ciclo da segurança da informação devem ser levadas em consideração no momento do planejamento da política de segurança da Organização para que os princípios da segurança da informação não sejam comprometidos [4].

2.3 SEGURANÇA DA INFORMAÇÃO

De acordo com a ISO/IEC 27002 [5] é a proteção da informação contra vários tipos de ameaças para garantir a continuidade do negócio, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidades de negócios.

2.4 PRINCÍPIOS BÁSICOS DA SEGURANÇA DA INFORMAÇÃO

2.4.1 **O Princípio da Integridade**

O primeiro dos três princípios da segurança da informação é a integridade**,** essa nos permite garantir que a informação não tenha sido alterada em seu conteúdo e, portanto, é íntegra. Uma informação íntegra é uma informação que não foi alterada de forma indevida ou não autorizada [6].

2.4.2 **O Princípio da Confidencialidade**

O princípio da confidencialidade tem como objetivo garantir que a informação não estará disponível ou divulgada a indivíduos, entidades ou processos sem

autorização. Em outras palavras, é a garantia do resguardo das informações dadas pessoalmente em confiança e proteção contra a sua revelação não autorizada [6].

2.4.3 **O Princípio da Disponibilidade**

Para que uma informação possa ser utilizada, ela deverá estar disponível. A disponibilidade da informação permite que a informação seja utilizada quando necessário, esteja ao alcance de seus usuários e destinatários e possa ser acessada no momento em que for necessário utilizá-la [6].

2.5 INCIDENTE DE SEGURANÇA

Um incidente de segurança é definido como qualquer evento adverso que promova alguma ação que comprometa a segurança da informação. Os principais tipos de incidentes de segurança podem ser: tentativas de acesso não autorizado a sistemas ou serviços, alteração de sistemas sem consentimento prévio do dono, o não cumprimento ou desrespeito à política de segurança [5].

2.6 POLÍTICA DE SEGURANÇA

A Política de Segurança consiste em um conjunto formal de normas, diretrizes, procedimentos e instruções que define os critérios que devem ser adotados e seguidos pela Organização a fim de minimizar possíveis ameaças na segurança da informação. Ela trata dos aspectos tecnológicos e humanos, e também determina as penalidades que devem ser aplicadas quando houver a violação de alguma de suas normas [7].

“A Política de Segurança é a base para a proteção das informações, tendo papel fundamental para as organizações” [8].

Ou ainda, segundo [2], por política de segurança entende-se política bem elaborada, implantada e em contínuo processo de revisão, válida para toda a organização, com regras mais claras e simples possíveis e estrutura gerencial e material de suporte a essa política, claramente sustentada pela alta hierarquia.

3 NORMAS E REGULAMENTAÇÕES

As normas e regulamentações criadas por diversas empresas podem ser classificadas de acordo com o setor à que a empresa presta serviços.

3.1 REGULAMENTO TÉCNICO

São documentos normativos de caráter compulsório que contém requisitos aplicáveis a tecnologias de produtos, processos ou serviços, relacionados principalmente à saúde, meio ambiente, defesa do consumidor e práticas enganosas de comércio. A tendência internacional atual da regulamentação é a de que esta se restrinja a requisitos essenciais do objeto regulamentado, adotando como referência as normas técnicas, especialmente as internacionais [9].

3.2 NORMAS TÉCNICAS

Segundo o Ministério da Ciência e Tecnologia, são documentos de caráter voluntário e com conteúdo técnico obtido por consenso envolvendo o conjunto das partes interessadas, que dispõem sobre tecnologias de projeto e fabricação de produtos, concepção e prestação de serviços, transferência de tecnologia e gestão. As normas técnicas referem-se em geral a classificação, especificação, método de ensaio, procedimento, padronização, simbologia e terminologia, sendo no Brasil, elaboradas e aprovadas pelo foro brasileiro de normalização, a Associação Brasileira de Normas Técnicas (ABNT) [9].

3.3 PRINCIPAIS NORMAS E LEIS INTERNACIONAIS

Esta seção tem como escopo apresentar uma breve descrição das principais normas do setor financeiro/contábil (Basiléia II, *Gramm-Leach-Bliley Act* – GLBA, *Sarbanes Oxley - SOX*), do setor público (*Federal Information Security Management Act* - FISMA), do setor financeiro de pagamentos com cartões de crédito (*Payment Card Industry Data Security Standard* - PCI-DSS), sobre cuidados de saúde (*Health Insurance Portability and Accountability Act* - HIPAA) e sobre a norma ABNT ISO/IEC 27002.

3.3.1 **Basileia II**

O acordo da Basileia II define as metodologias de gerenciamento de risco dos bancos visando garantir a segurança e confidencialidade dos dados dos clientes, na supervisão das autoridades bancárias e no fortalecimento da disciplina de mercado. A nova estrutura vem alinhar a avaliação da adequação de capital mais intimamente aos principais elementos dos riscos bancários e fornecer incentivos aos bancos para aumentar suas capacidades de mensuração e administração dos riscos. O Basiléia II fixa-se em três pilares (Capital Mínimo Requerido, Revisão no Processo de Supervisão e Disciplina de Mercado) e 25 princípios básicos sobre contabilidade e supervisão.

3.3.2 **Gramm-Leach-Bliley Act (GLBA)**

O Gramm-Leach-Bliley Act (GLBA) foi promulgado em 12 de novembro de 1999 e é uma lei do Congresso dos Estados Unidos que permitiu aos bancos

comerciais e de investimento se consolidarem. A lei foi aprovada para legalizar estas fusões de forma permanente [46].

Historicamente, a indústria é conhecida como a indústria de serviços financeiros. A principal mudança provocada pela Lei consiste no encorajamento aos indivíduos a aplicarem o dinheiro em poupanças e em investimentos na mesma instituição financeira e ela também será capaz de fazê-lo em tempos bons e ruins economicamente falando. A conformidade com a GLBA é obrigatória. Se uma instituição financeira divulga informações públicas ou não, deve haver uma política para proteger a informação de ameaças previsíveis em termos de segurança e integridade dos dados.

A conformidade com a GLBA é obrigatória. O Apêndice B do regulamento de execução (51) exige que cada instituição financeira possua documentado um programa de segurança da informação que inclua proteções administrativas, técnicas e físicas adequadas à complexidade da instituição e ao escopo de suas atividades. Para isso, é preciso primeiramente, realizar uma avaliação regular dos riscos, capaz de identificar possíveis ameaças e riscos à segurança da informação, avaliar a probabilidade de ocorrência e os principais danos potenciais destas ameaças, e avaliar também a suficiência de controles para mitigação de tais riscos [52]. As diretrizes descritas no programa devem garantir a confidencialidade das informações dos clientes, a proteção contra qualquer ameaça ou risco previsível à segurança ou integridade dos dados e a proteção contra acesso não autorizado [50].

O GLBA coloca em prática três regras para garantir a segurança e integridade dos dados financeiros, são elas: regra de privacidade financeira, regra de proteção e proteção *pretexting* (contra engenharia social) [47].

3.3.3 **Sarbanes-Oxley Act (SOX)**

Promulgada em 30 de julho de 2002, a Lei Sarbanes-Oxley Act de 2002, é uma lei federal norte-americana criada em decorrência a uma série de escândalos financeiros ocorridos em grandes empresas (Enron, Tyco International, Adelphia, Peregrine Systems e WorldCom) que acarretou o êxodo dos investimentos financeiros na Bolsa de Valores.

Segundo [39], *a* SOX objetiva promover melhor a Governança Corporativa através da eficácia dos controles internos que influenciam nos resultados financeiros das organizações*.* A análise e divulgação das informações financeiras também são exigências da lei. Para isso, os diretores e o Presidente passam a ser responsáveis por estabelecer, avaliar e monitorar a estrutura dos controles internos da corporação, onde o não cumprimento das normas exigidas implica no o pagamento de multas e no cumprimento de penas de reclusão.

Composta por 1107 seções, as mais conhecidas são as seções 302 e 404. Na seção 302 os diretores e o Presidente devem declarar pessoalmente serem responsáveis pelos controles internos e processos de divulgação da empresa e na seção 404 são exigidos a realização de uma avaliação anual dos controles e procedimentos internos para emissão de relatórios financeiros [43][44]. Por isso, têm-se a obrigatoriedade da observância de práticas de segurança de redes e critérios rígidos para uso de aplicações terceirizadas por companhias que se encontram ao alcance da presente lei. Além disso, a seção 404 exige a criação de um *framework* de controles internos, que pode ser feita segundo as recomendações de padrões como, por exemplo, o COSO (*Committee of Sponsoring Organizations of*

the Treadway Commission) [40] ou COBIT (Control Objectives of Information and Related Technology) [41].

3.3.4 **Federal Information Security Management Act (FISMA)**

O Federal Information Security Management Act de 2002 ("FISMA", 44 USC § 3541, et seq.) é uma lei federal dos Estados Unidos promulgada em 2002 com o Título III do E-Government Act de 2002 (Pub.L. 107-347 , 116 Stat. 2899) que declara obrigatória a conformidade de todas as agências governamentais com os padrões FIPS (Federal Information Processing Standards) [24] [23].

O FISMA impõe um conjunto de procedimentos obrigatórios, conhecidos como requisitos mínimos de segurança para informações federais, que devem ser seguidos por todos os sistemas de informação utilizados ou acionados pela agência governamental federal dos Estados Unidos da América (EUA) ou por outra organização em nome dessa agência [24]. De acordo com [22], esses requisitos devem seguir os controles de segurança do Special Publication 800-53, que foram desenvolvidos através de uma combinação de variadas fontes, que incluem o NIST Special Publication 800-26, a ISO/IEC 17799, entre outras. Tais requisitos englobam itens como avaliação de riscos, certificação, gerenciamento da configuração, planejamento da segurança, proteção do sistema e das comunicações, segurança do corpo de funcionários, treinamento, proteção física e ambiental, proteção de mídias, plano de Contingência, manutenção, integridade do sistema e da informação, resposta à incidentes, procedimentos de identificação e autenticação, controle de acesso e auditoria.

3.3.5 **Payment Card Industry Data Security Standard (PCI - DSS)**

Esta norma se aplica a toda e qualquer empresa que coleta, processa, armazena ou transmite informação de cartão de crédito, estando, portanto, obrigada a se adaptar ao padrão [19]. Todos os segmentos, que processam dados de cartão de crédito e estão ligados à rede da associação de cartões, provedores de serviços que hospedam *sites* ou coletam e processam dados de cartão de crédito, em nome de membros das redes Visa e Mastercard, etc., e tais como comerciantes e intermediadores estão sujeitos a esta norma [20].

O PCI - DSS é composto de seis principais áreas que contém doze requerimentos. O documento contém padrões de segurança que cobrem os seguintes temas: segregação e segurança de redes; criptografia para proteção de dados de cartão; gerenciamento de atualizações e auditoria de vulnerabilidades em sistemas; medidas de controle de acesso e integridade de arquivos; teste e monitoramento de redes, e ainda gestão de incidentes e manutenção da política de segurança da informação [18].

3.3.6 **Health Insurance Portability and Accountability Act (HIPAA)**

O HIPAA (*Health Insurance Portability and Accountability Act*) é um Ato abrangente que governa a privacidade, segurança e transações eletrônicas das informações de saúde de clientes e pacientes. A legislação, também, se aplica a empresas com registros de saúde dos funcionários. A transmissão de informações de saúde deve ter proteções físicas, eletrônicas e administrativas e estes dados devem ser isolados e inacessíveis ao acesso não autorizado de forma a assegurar a confidencialidade dessas informações.

3.3.7 **Norma ISO 27002:2005**

Anteriormente chamada de ISO/IEC 17799, devido a série ISO 27000, teve sua nomenclatura alterada para ISO 27002. Seu objetivo é estabelecer procedimentos para as organizações desenvolverem, implementarem e avaliarem a gestão da Segurança da Informação. É um conjunto de 11 seções de controle que descrevem as principais categorias de segurança da informação e que deve ser usada como um guia prático para implementação da norma ISO/IEC 27001 [6].

4 PRINCIPAIS CONTROLES DA NORMA ISO/IEC 27002

Esse capítulo tem como objetivo reunir os requisitos de maior relevância sugeridos pela norma técnica brasileira ISO/IEC 27002:2005 de forma que a implementação dessas diretrizes auxilie as organizações a estarem em conformidade com a maioria das leis, normas e regulamentações existentes.

A organização desses procedimentos foi distribuída de acordo com a maioria das seções de controle contidas na norma.

I. Política de Segurança da informação
II. Gestão de ativos
III. Segurança em Recursos Humanos
IV. Segurança Física e do Meio Ambiente
V. Gestão das Operações e Comunicações
VI. Controle de Acesso
VII. Gestão de Incidentes de Segurança da Informação
VIII. Conformidade

4.1 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A ISO/IEC 27002 recomenda a criação e implementação de uma política de segurança da Informação, um documento que tem como objetivo a conscientização e orientação de funcionários, parceiros, fornecedores e clientes para o uso seguro do ambiente informatizado. Esse documento deve conter o conceito de segurança da informação e da sua importância para a continuidade do negócio, além de

explanar de forma clara e concisa as políticas de segurança da informação específicas para a organização. Deve ser descrito também os requisitos para conscientização e treinamento em segurança da informação, assim como as ações que serão tomadas para a continuidade do negócio e também as sanções aplicadas no caso de seu descumprimento. É importante destacar que sua revisão deve ser realizada periodicamente e que o documento necessita de aprovação da direção e deve ser de conhecimento de todos os envolvidos com a segurança da informação.

4.2 GESTÃO DE ATIVOS

A gestão dos ativos é importante, pois pode ser requisitado em outras áreas do negócio, como no processo de avaliação e tratamento dos riscos e tem como objetivo a identificação, proteção efetiva e gestão dos ativos. Para isso, convém que esses ativos sejam claros e suas características documentadas, dentre elas estão: o tipo de ativo, sua localização e formato (caso possua), informações sobre licenças e cópias de segurança e a importância do ativo para o negócio. Todos os ativos devem fazer parte do inventário, como por exemplo: ativos de informação, de software, físicos, serviços, recursos humanos e ativos intangíveis. O controle dos ativos pode ser delegado a um profissional que ficará responsável pela manutenção do inventário.

Essa seção contempla também a classificação do ativo mais importante para o negócio: a informação. A classificação e rotulação da informação têm como finalidade assegurar que a informação receba um nível adequado de proteção.

A classificação da informação estabelece a maneira como a informação deverá ser tratada com segurança física e lógica de acordo com o seu grau de sigilo. O nível de proteção pode ser calculado através dos três pilares da segurança da

informação: a confidencialidade, a integridade e a disponibilidade da informação; como também através de outros elementos.

Após as informações terem sido classificadas estas devem ser rotuladas apropriadamente e o rótulo deve reproduzir tal classificação. Para cada grau de sigilo, as ações a serem tomadas em cada fase do ciclo de vida da informação devem ser documentadas.

4.3 SEGURANÇA EM RECURSOS HUMANOS

A segurança em recursos humanos tem como objetivo a redução dos riscos de furto ou roubo, fraude ou mau uso de recursos. Ela envolve a seleção, treinamento e conscientização de todos os funcionários para que eles estejam cientes e aptos a apoiar a Política de Segurança da Informação durante a execução de suas funções.

As responsabilidades de cada funcionário pela segurança da informação devem ser atribuídas antes da contratação, de acordo com o cargo a ser ocupado.

4.4 SEGURANÇA FÍSICA E DO AMBIENTE

A segurança física e do ambiente tem como objetivo a prevenção do acesso físico não autorizado, danos e interferências às instalações de processamento de informações.

A segurança do perímetro das instalações da Organização pode ser alcançada com a utilização de barreiras físicas, instalando-se, por exemplo, portas de entrada controladas por cartão ou criação de uma área de recepção com

recepcionistas, além do uso e monitoramento de sistemas de detecção de intrusos e alarmes. O controle de entrada na Organização pode ser feito exigindo que todos os funcionários estejam devidamente identificados ao adentrar as instalações, assim como os visitantes, que devem ter sua estadia supervisionada e registrada. Outra boa prática é manter os equipamentos gerenciados pela Organização e os gerenciados por terceiros em ambientes fisicamente distintos, separados. Tais locais devem ainda possuir controle de condições ambientais como temperatura e umidade através do uso de termômetros e hidrômetros, respectivamente; ou até mesmo integrados ao sistema de alarmes, a fim de evitar que os equipamentos sejam afetados. Recomenda-se também a utilização de *UPS* (Uninterruptible Power Supply) para manter o funcionamento contínuo de equipamentos críticos e geradores ou múltiplas fontes de energia para o caso de falha do UPS.

A segurança do cabeamento é outro item que requer atenção. A elaboração do projeto de redes locais deve basear-se nos princípios do cabeamento estruturado, como por exemplo: segregação de cabos de energia e de cabos de telecomunicações de modo a evitar interferências; instalação de cabeamento de redes em canaletas; identificação de cabos e equipamentos, manutenção de uma documentação atualizada das conexões minimizando erros de manutenção e se possível, prover a instalação subterrânea dos cabos que entram nas salas de processamento de dados (CPD).

4.5 GESTÃO DAS OPERAÇÕES E COMUNICAÇÕES

Essa seção aborda as principais áreas que devem ser tratadas com atenção especial, com o objetivo de garantir a operação segura dos recursos de

processamento da informação. Questões referentes a procedimentos e responsabilidades, controle de documentação, procedimentos de *backups*, controle e prevenção de vírus, procedimentos para acesso à Internet, segurança do serviço de correio eletrônico, segurança de mídias de armazenamento, controle de redes, entre outras são explanadas com a gestão das operações e comunicações.

4.5.1 **Procedimentos e responsabilidades e controle de documentação**

É conveniente, em primeiro lugar, definir todos os procedimentos e responsabilidades pela gestão e operação dos recursos de processamento de informações através do desenvolvimento da documentação dos procedimentos operacionais que devem ser sempre mantidos atualizados.

4.5.2 **Procedimentos de *backups***

Os procedimentos de cópias de segurança ou *backups* e recuperação ou *restore* de dados devem estar descritos na Política de Segurança de tal forma que seja capaz de prover orientações de realização e recuperação das informações. Registros das cópias realizadas como por exemplo hora de início e término, o conteúdo e o tipo de cópia realizado, devem ser documentados.

De acordo com a aplicação, sua importância para o negócio e os meios de armazenamento disponíveis, pode-se utilizar como métodos de cópia os *backups* do tipo normal, incremental ou diferencial. O armazenamento das cópias pode ser realizado em fitas ou discos e pode ser local ou remoto (através da rede), além disso, pode-se também utilizar em conjunto um servidor de *backups* para armazenamento dos mesmos. Deve-se ainda levar em consideração duas situações a respeito da restauração dos dados:

- pedidos pequenos e rápidos de restauração;
- restauração para recuperação de desastres;

Como exemplo para o primeiro caso, podemos citar um usuário que apaga um arquivo por acidente e precisa de sua recuperação imediata. Para a recuperação do arquivo é necessário que a mídia de armazenamento do *backup* esteja próxima do sistema para onde os dados serão restaurados. Para exemplificar o segundo caso, pode ter ocorrido um desastre de natureza física, nesse caso, é preciso manter uma cópia do backup em local externo ao site. Para atender ambos os casos o ideal seria manter *backups* de um conjunto de dados mantidos mais próximos, para pedidos imediatos, que são casos mais frequentes de restauração e outro armazenado externamente à empresa para a recuperação de desastres. Devem ser realizados testes nas mídias de armazenamento para assegurar qure os backups mantidos nos ambientes interno e externo estejam em perfeito estado para serem utilizados e testes de restauração com a finalidade de avaliar a funcionalidade dos procedimentos, verificar a integridade da informação armazenada, identificar procedimentos ineficazes ou desatualizados e por fim identificar falhas ou defeitos.

4.5.3 **Controle e prevenção de vírus**

Para o controle e a prevenção contra códigos maliciosos devem ser estabelecidas políticas formais que considerem diretrizes como: a proibição do uso de softwares não-autorizados e quando necessário a aquisição e instalação de novos softwares deve ser solicitada à equipe de TI (Tecnologia da Informação), que deve ser responsável pela obtenção da licença de uso e homologação do software.

A prevenção, detecção e remoção de códigos maliciosos (como por exemplo, vírus, cavalos de Tróia, *worms, spyware, adware e rootkits*) podem ser feitas através

da utilização de programas antivírus que devem ter suas bases de definições de vírus atualizadas constantemente e independente da ação do usuário, preferencialmente. O exame dos sistemas deve ser executado periodicamente e estas verificações devem incluir: a verificação, antes do uso, da existência de algum código malicioso em mídias removíveis, em páginas web e em arquivos recebidos por meio do serviço de correio eletrônico (recomenda-se que essa verificação seja feita em mais de um local, como nos computadores pessoais, nos servidores de correio ou ao entrar na rede). Faz-se necessário ainda manter todos os sistemas e softwares com os *patches* de segurança mais recentes, e estes devem ser instalados com o prazo máximo de 30 dias após seu lançamento.

4.5.4 **Procedimentos para uso da internet**

O uso da internet deve ser descrito formalmente visando a proteção da propriedade intelectual, a privacidade das informações e qualquer tipo de discriminação. Esse documento deve ser de conhecimento de todos os usuários e deve esclarecer quais são os principais processos que podem vir a causar danos quando utilizados de forma inadequada. Por esse motivo, a monitoração do uso da internet é muito importante para registrar os acessos e verificar se o uso do serviço está sendo realizado adequadamente. Dados que podem ser monitorados são: a identidade do usuário, data e hora da conexão, endereço *IP* de origem, quais os protocolos utilizados e a quantidade de dados que foram transmitidos ou recebidos.

O Departamento Jurídico da empresa deve ser consultado para analisar aspectos como por exemplo:

- a permissão do uso da internet para uso pessoal e/ou fins comerciais pelos funcionários e em qual período esse acesso poderá ser realizado;

- como será realizada a monitoração do uso da Internet e a qual nível de privacidade os funcionários estão sujeitos;
- definição de acessos não permitidos, determinando quais tipos de sites não serão aceitos;

As sanções que serão aplicadas no caso de descumprimento do procedimento também devem estar descritas no documento.

4.5.5 **Segurança do serviço de correio eletrônico**

Tratando-se de segurança da informação, outro item que oferece diversos riscos para a empresa é o serviço de correio eletrônico. Por ser muito utilizado para troca de informações rápida e garantia de documentação. Inúmeras maneiras de fraudar as mensagens do correio eletrônico têm surgido; sem desconsiderar a sua utilização por funcionários mal intencionados. Por esse motivo, a segurança do correio eletrônico deve ser tratada com muita cautela buscando a avaliação de normas legais para evitar a invasão de privacidade e ao mesmo tempo proteger as mensagens eletrônicas. É conveniente que as considerações de segurança a seguir sejam integrantes da Política de Segurança:

- proteção das mensagens contra acesso não autorizado, modificação ou negação de serviço;
- assegurar que o endereçamento e o transporte da mensagem estejam corretos;
- confiabilidade e disponibilidade geral do serviço;
- aspectos legais, como por exemplo, requisitos de assinaturas eletrônicas.

4.5.6 **Segurança de mídias de armazenamento**

A preocupação com a segurança e o tratamento de mídias é outro fator importantíssimo para assegurar que as informações contidas em discos ou outros meios de armazenamento sejam descartadas de forma segura e protegida quando estas não forem mais necessárias; prevenindo contra a divulgação não autorizada ou modificação das mesmas . A remoção ou transporte de qualquer mídia de armazenamento, seja ela removível ou não, deve ser previamente autorizada e registrada. Recomenda-se verificar o nível de confiabilidade do meio de transporte ou serviço de entregas utilizado, além de se definir uma lista de portadores que estejam autorizados a transportar as mídias e por fim sugere-se embalar a mídia em recipientes lacrados e entregá-la em mãos. Excepcionalmente, pode-se enviar mais de uma remessa por rotas distintas.

Não sendo mais necessária a utilização da mídia ou sendo encontrado algum problema em seu funcionamento o seu descarte deve ser imediato e realizado através de aparelhos trituradores ou incineradores ou a partir da contratação de empresas que ofereçam serviços de coleta e descarte. Para o registro dessas informações pode-se utilizar um sistema de controle, o qual pode conter o inventário de todos os recursos de tecnologia da informação da Organização, como por exemplo, a documentação de todos os elementos da rede, dos recursos de hardware e software, entre outros.

O manuseio e descarte das mídias de armazenamento devem ser descritos formalmente, podendo ser parte da Política de Segurança da Informação.

4.5.7 **Controle de redes**

Controles devem ser implementados de forma a possibilitar a gerência das redes garantindo a proteção de acesso não autorizado dos serviços e aplicações a elas conectadas. Responsabilidades e procedimentos devem ser definidos para o gerenciamento de equipamentos remotos e controles especiais devem ser estabelecidos para garantir a confidencialidade, integridade e disponibilidade dos dados que trafegam sobre as redes públicas ou sobre as redes sem fio (*wireless*)

4.5.8 **Controle de acessos**

Este tópico tem como escopo o controle de acesso a sistemas, a utilização de senhas, acesso remoto, entre outros.

O acesso à informação e aos recursos da rede precisa ser controlado com base na segurança da informação e nos requisitos do negócio. Para garantir o acesso somente de usuários autorizados e prevenir o acesso não autorizado aos recursos de TI recomenda-se as boas práticas descritas no decorrer desta seção.

4.5.9 **Controle de acesso de usuários**

Para cada usuário deve ser implementado procedimentos formais que controlem a distribuição de direitos de acesso aos sistemas de informação e serviços, como por exemplo:

- existência de um procedimento formal de criação e registro de usuário de forma a garantir e revogar acessos;
- para cada usuário, utilizar um identificador único, assegurando a responsabilidade de cada usuário por suas ações;

- conceder aos usuários um documento por escrito informando-o dos seus direitos de acesso e requerer dos usuários um registro declarando o recebimento e entendimento do documento;
- bloquear ou remover configurações de acesso dos usuários que não fazem mais parte da Organização ou que tiveram seus cargos ou funções alteradas;
- deve ser concedido a cada usuário somente os privilégios de acesso necessários para a execução de suas atividades;
- a concessão dos direitos de acesso deve ser devidamente autorizada e registrada;
- incentivar o uso e/ou desenvolvimento de programas que funcionem sem a necessidade de contas com permissões privilegiadas.

4.5.10 **Utilização de senhas**

O estabelecimento de diretrizes que auxiliem os usuários a criarem e utilizarem senhas seguras é uma boa prática recomendada e a seguir são descritas recomendações importantes para a criação de senhas.

- Tamanho mínimo e Complexidade da senha: esse item tem como principal objetivo evitar ataques de força bruta e de dicionário. As senhas devem ser compostas por um número mínimo de 6 caracteres e ser formada por caracteres alfanuméricos maiúsculos e minúsculos. Esses dois itens garantem um nível de entropia que torna um ataque de força bruta inviável. Deve-se evitar também o uso de caracteres repetidos ou em sequências e o uso de palavras contidas nos dicionários em qualquer idioma, assim como usar apenas caracteres semelhantes para substituição de letras, isto é, utilizar substituições de

caracteres semelhantes como, por exemplo, o uso de ‘1’ no lugar de ‘i’ ou ‘&’ no lugar de ´e´ ou ‘@’ no lugar de 'a', como em "m1cr0$0ft" ou "c@mil@". Esse tipo de técnica tornou-se muito conhecida, facilitando os ataques, entretanto, tais substituições podem ser usadas combinadas com outras técnicas, visando aumentar a força da senha.

- Memorização de senhas: Uma maneira de minimizar a dificuldade de memorizar senhas complexas seria orientar os usuários a fazerem uso de frases secretas ao invés de senhas ininteligíveis, como por exemplo: “Meu cãozinho Totó tem 2 anos.”, gerando a senha: mcTt2a.
- Troca periódica da senha**:** a alteração das senhas periodicamente deve ser obrigatória para todos os usuários e essa alteração pode ser feita a cada 3 ou 4 meses. Além de evitar que a senha seja descoberta por pessoas mal intencionadas, esse item auxilia o administrador da rede a encontrar contas de usuário que não são mais utilizadas e que deveriam ter sido excluídas ou desabilitadas.
- Repetição de senhas: a utilização das últimas 5 senhas deve ser proibida. Isso impede que o usuário realize a alteração da senha, mas permaneça com a mesma. A plataforma Microsoft, por exemplo, utiliza por padrão a não utilização das últimas 24 senhas, no entanto, um valor mais baixo pode ser definido.
- Quantidade de tentativas inválidas de acesso: definir um limite de tentativas de acesso inválidas, bloqueando o acesso de forma a evitar a descoberta das senhas. Sugere-se o bloqueio após três tentativas falhas.
- Troca de senhas iniciais (padrão): senhas iniciais de sistemas, banco de dados ou outras aplicações, devem ser alteradas imediatamente após o seu recebimento em ambiente seguro, antes de sua utilização.

- Bloqueio automático por período de inatividade (*time out*): todos os sistemas devem possuir definido um período de tempo máximo para realizar o encerramento de um acesso por inatividade.
- A senha é pessoal, intransferível e confidencial.

4.5.11 **Controle de acesso ao sistema operacional**

O controle de acesso ao sistema operacional tem como finalidade a implementação de políticas para a prevenção de acesso não autorizado aos sistemas operacionais. Para isso, o procedimento de entrada no sistema (log-on) deve exibir somente o mínimo de informações necessárias ao usuário.

Um procedimento de “log-on” seguro deve seguir as seguintes diretrizes:

- até que o processo tenha sido finalizado com sucesso, o procedimento não deve exibir nenhum tipo de identificação do sistema;
- uma mensagem alertando que o computador deve ser utilizado somente por usuários permitidos deve ser sempre exibida;
- mensagens de ajuda que possam facilitar o “log-on’ de usuários não autorizados não devem ser exibidas;
- as informações de entrada devem ser validadas somente quando todos os dados solicitados forem preenchidos e caso haja uma condição de erro, apenas este deve ser informado e não a parte do dado que estaria inconsistente;
- o número de tentativas de entrada no sistema com e sem sucesso devem ser registradas, tendo ainda essa última o número de tentativas limitadas. Caso esse número máximo de tentativas de entrada no sistema seja atingido, uma mensagem de alerta deve ser enviada ao administrador do sistema e um período de tempo de espera deve ser configurado antes de permitir que novas tentativas

de acesso sejam realizadas;

- configuração de um período de tempo de espera de maneira a impedir tentativas posteriores de acesso;
- limitar o tempo máximo e mínimo para que o procedimento de entrada seja realizado, ultrapassado esse período, o sistema deve encerrá-lo;
- mostrar ao término do procedimento de entrada com sucesso:a data e hora da última entrada no sistema e detalhes de tentativas falhas desde o último acesso com sucesso;
- a entrada da senha deve ser feita através do uso de símbolos, ocultando-a;
- a transmissão da senha pela rede deve ser realizada somente com o uso de técnicas criptográficas.

4.5.12 **Acesso remoto**

Para que o acesso remoto seguro a aplicações, documentos e dados da organização sejam oferecidos de forma segura é indicado que algum método de autenticação seja utilizado, como o uso algoritmos criptográficos, de *tokens* ou uso de um protocolo de autenticação baseados em desafio-resposta. Se a escolha for utilizar criptografia, pode-se optar por um dos três tipos principais, dependendo do tipo de garantia desejado (autenticação, integridade, não-repúdio e confiabilidade): funções hash, criptografia simétrica e criptografia assimétrica. Os *tokens* são dispositivos que possuem um chip que geram senhas automaticamente. Nos protocolos que baseiam-se no princípio desafio-resposta, o emissor envia um número aleatório para o receptor e este, ao receber a mensagem transforma o número recebido em uma forma especial e o envia para o emissor. No entanto, esse último método pode ser facilmente quebrado devido a possibilidade de um ataque

man-in-the-middle, onde uma pessoa má-intencionada no meio dessa comunicação pode receber o desafio, criar uma nova conexão para obter a resposta do desafio e ao obtê-la, utilizá-la para autenticar-se com o emissor.

O acesso remoto pode ser viabilizado através da rede pública, por exemplo, através do uso de uma VPN (Virtual Private Network), ou rede privada virtual, que permite a interligação de dois ou mais locais remotos de forma segura e de baixo custo permitindo a troca de informações. As técnicas de autenticação descritas acima podem ser facilmente combinadas com a solução de VPN.

Outra maneira de proporcionar esse acesso seria com o uso de linhas privadas dedicadas, as quais garantem a origem das conexões.

Não é indicado o uso de controles de discagem reversa ou *dial-back* através de modens que possuam tal mecanismo. Tais equipamentos podem permitir conexões não autorizadas, autenticando os usuários remotos que tentam estabelecer uma conexão com a rede da Organização. Ao utilizar esse controle, o serviço de rede que inclua transferências de chamadas (*forward*) deve ser desabilitado visando evitar vulnerabilidades associadas ao *call forward*, ou discagem reversa. O processo de discagem reversa deve assegurar que realmente houve a desconexão no lado da organização, caso contrário, o usuário remoto poderia reter a linha aberta simulando a ocorrência de uma confirmação de retorno de chamada (*call back*). Por esses motivos, os controles da discagem reversa devem ser cuidadosamente testados quanto a esta possibilidade.

4.5.13 **Roteamento de redes**

Em situações onde a técnica de tradução de endereços é empregada, recomenda-se o uso de gateways de segurança nos pontos de controle da rede interna ou externa para verificar a veracidade dos endereços de origem e destino.

4.6 GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Procedimentos para o gerenciamento de incidentes devem ser estabelecidos de forma a garantir respostas rápidas e efetivas aos incidentes de segurança. Devem ser definidos procedimentos que cubram os diferentes tipos de incidentes, incluindo falha nos sistemas de informação e indisponibilidade de serviços. Um ponto de contato para receber tais notificações e tratá-las com mais rapidez possível deve ser definido e de conhecimento de toda a força de trabalho.

Os planos de contingência devem estabelecer procedimentos que contemplem a análise e a identificação das causas do incidente, planejamento e implementação de uma ação corretiva que previna a repetição do incidente, comunicação com os afetados ou envolvidos com a recuperação do incidente e notificação da ação tomada à autoridade apropriada.

4.7 CONFORMIDADE

Esta última seção apresenta a necessidade de observação das obrigações legais com o objetivo de evitar a violação de qualquer lei, regulamentos ou obrigações contratuais e de quaisquer requisitos de segurança da informação que possam estar sujeitos aos sistemas de informação.

4.7.1 **Direito de propriedade intelectual**

Para proteger qualquer material que possa ser considerado como propriedade intelectual é conveniente que as diretrizes a seguir sejam consideradas:

- divulgação de uma política de conformidade com os direitos de propriedade intelectual que defina o uso legal de *softwares* e de informação;
- a aquisição de softwares deve ser realizada somente através de fontes conhecidas e de boa reputação;
- manter a constante conscientização das políticas para proteger direitos de propriedade intelectual e notificar a respeito das ações disciplinares tomadas em caso de violação dessas políticas;
- manter documentação atualizada de licenças, discos-mestres, manuais, etc;
- Implementação de controles que assegurem que o número máximo de usuários permitidos não exceda o número de licenças adquiridas;
- cumprir termos e condições para *software* e informação obtidos a partir de redes públicas.

4.7.2 **Conformidade com as políticas e normas de segurança da informação**

Faz-se necessário garantir que todos os procedimentos de segurança da informação contidos na política de segurança da informação ou em qualquer outro documento formal estejam sendo executados corretamente atendendo a conformidade com as leis, normas e regulamentações. Para tal verificação convém que a segurança dos sistemas de informação passe por auditorias regulares. Em caso de não-conformidade como resultado da análise, recomenda-se que os gestores determinem o que causou a não-conformidade, definam ações para assegurar que não ocorram reincidências; determinem, implementem e realizem

uma análise das ações corretivas. O resultado e as ações corretivas oriundas das auditorias devem ser registradas para posteriormente serem analisados novamente, caso necessário.

5 ANÁLISE COMPARATIVA

Nesta seção é realizada uma análise comparativa entre as normas e leis apresentadas, ressaltando as exigências comuns entre elas (tabela 01) e como essas exigências podem ser implementadas com o auxílio das boas práticas descritas pela ISO 27002. Essa análise tem como objetivo auxiliar a equipe de TI a identificar e implementar os requisitos necessários para alcançar a conformidade com mais de um regulamento.

As normas e padrões do setor financeiro/contábil − a Basiléia II, o GLBA e o SOX − tem como foco principal a governança corporativa e transparência dos dados.

O Basiléia II tem como exigências a adoção de um framework de melhores práticas para implementação de novos processos, criação de procedimentos para identificar, analisar e integrar os ativos de TI, a implementação de processos operacionais e controles para o gerenciamento de riscos de TI e a garantia de rastreabilidade de mudanças e auditorias dos dados. Além da avaliação de riscos, o Basiléia tem como principais exigências a existência de controles nas seguintes áreas: controles de acesso de acordo com a segregação de funções, segurança dos sistemas e comunicação, monitoramento para melhoria contínua de procedimentos e comprometimento da alta administração com a segurança da informação.

O GLBA, assim como o Basiléia II, também tem como exigência a realização de uma avaliação regular capaz de identificar possíveis ameaças e riscos à segurança da informação, avaliar a probabilidade de ocorrência e os principais danos potenciais destas ameaças; além de avaliar também a suficiência de controles para mitigação de tais riscos. Esses procedimentos de gerenciamento de riscos devem também estar descritos em um programa de segurança da informação

que inclua principalmente procedimentos nas áreas de autenticação e controle de acesso, controle de acesso físico, planos de contingência e processos de auditorias [50]. Esse programa deve ainda, incluir a atribuição de responsabilidade de gerenciamento das salvaguardas de segurança a um funcionário específico e um programa de conscientização e treinamento do corpo de funcionários.

Por último, para alcançar a conformidade com o SOX é preciso atender às exigências da seção 404 da lei, que exige a criação de um framework de controles internos para as atividades relacionadas à emissão de relatórios financeiros. E este framework deve ser avaliado, monitorado e anualmente revisado. Para isso, a área de TI deve cobrir todos os aspectos de segurança e controle das informações digitais da empresa, devendo assegurar a confiabilidade do sistema operacional, a veracidade dos dados de saída e a proteção de equipamentos e arquivos. Para cumprir essas exigências todos os processos internos que abrangem desde as metodologias de desenvolvimento de sistemas até as áreas de operações de computadores devem ser revistas. Além disso, as áreas usuárias de tais recursos devem ser conscientizadas sobre os aspectos de segurança e cuidados na manipulação das informações, tais como: e-mails, compartilhamento de diretórios nos microcomputadores, compartilhamento de senhas de acesso aos aplicativos, entre outros. Aspectos de engenharia social também devem considerados.

Logo, para a criação do framework, presente tanto na lei SOX quanto no Basiléia, podem ser utilizadas as recomendações do COSO, CoBIT, as boas práticas do ITIL e da norma ABNT ISO/IEC 27002.

Para estar conforme com os requisitos exigidos pela lei aplicada ao setor público dos EUA, o FISMA, é preciso que seja desenvolvido, implementado e mantido um programa de segurança, onde responsabilidades específicas devem ser

atribuídas para sua implementação e gerenciamento. Uma avaliação de riscos deve ser realizada para que ameaças internas e externas possam ser identificadas e controladas. Controles de acesso, incluindo autenticação de usuários devem ser implementados para que pessoas não autorizadas não obtenham acesso aos sistemas e as informações. O acesso físico aos locais de armazenamento de informações e sistemas deve ser permitido somente pessoas autorizadas. As informações eletrônicas que estejam sendo transmitidas ou armazenadas em meios eletrônicos onde pessoas que não possuam autorização de uso tenham acesso devem estar protegidas com algum tipo de criptografia e possuir algum mecanismo que garanta a sua integridade. A monitoração dos sistemas deve ser realizada constantemente de maneira a identificar possíveis ataques ou intrusões e para esses casos, a instituição deve manter um programa de resposta a incidentes. Outra exigência é a existência de planos de continuidade ou de emergência, que descrevem procedimentos de como a instituição deve proceder caso ocorra algum desastre natural ou falha tecnológica. O comprometimento e conhecimento do programa de segurança pelos empregados podem ser alcançados através de treinamentos. Por fim, testes nos sistemas e revisões devem ser realizados periodicamente para verificar a necessidade de modificações nos procedimentos contidos no programa de segurança.

No setor financeiro de pagamentos, mais precisamente na indústria de cartões de crédito, o PCI-DSS define os seguintes controles: soluções de segurança para restringir ao máximo o acesso físico e lógico aos dados do portador do cartão devem ser implementadas. Para cada usuário, deve ser atribuído um identificador único e restrições de acesso aos sistemas devem ser configuradas, autorizando apenas os que necessitam utilizá-los para execução de suas atividades.

Todos os sistemas e equipamentos devem ser verificados, de forma a certificar que as senhas padrões ou parâmetros de segurança utilizados não sejam os fornecidos pelos fabricantes. A transmissão de dados do portador do cartão em rede pública deve ser codificada. Além disso, a instituição deve manter um programa de vulnerabilidades que descreva procedimentos para manter os sistemas seguros e declare obrigatória a utilização de um software de antivírus atualizado e executado ativamente, capaz de gerar *logs* para auditorias. O PCI-DSS exige ainda que todo o acesso aos recursos de rede e aos dados do portador do cartão seja monitorado e armazenado permitindo o acompanhamento e análise futura, caso necessário. Tais procedimentos devem ser testados regularmente, a fim de testar sua eficácia ou encontrar alguma vulnerabilidade. E por fim, os procedimentos acima devem ser mantidos em uma política de segurança da informação.

Para as entidades do setor de saúde que necessitem estar em conformidade, as exigências a seguir descritas precisam ser atendidas. Semelhantemente às normas do setor financeiro, do governo e de cartões de crédito, procedimentos para identificação, análise e controle de riscos devem ser estabelecidos. Salvaguardas de controle de acesso lógico e físico aos recursos de rede e sistemas também devem ser implementados, assim como procedimentos de utilização e de segurança das estações de trabalho, nos quais devem ser utilizadas ferramentas de identificação e autenticação de usuários, onde uma identificação exclusiva deve ser atribuída a cada usuário. Procedimentos para uso, re-uso e descarte de mídias eletrônicas devem ser descritos. Além desses requisitos, deve ser atribuída a uma pessoa ou setor a responsabilidade pela segurança da informação. Periodicamente, tais procedimentos e controles internos devem ser avaliados de forma a verificar a sua eficácia e necessidade de alteração. Um programa de resposta a incidentes deve

ser elaborado, assim como um plano de contingência e a avaliação desses planos deve ser periódica. Instituições terceiras prestadoras de serviço, fornecedores e parceiros devem cumprir com as políticas de segurança adotadas pela entidade de saúde. O registro de atividades dos sistemas e dos controles implementados deve ser mantido para fins de auditoria. O HIPAA exige que todos esses procedimentos estejam descritos no documento de política de segurança da informação e que toda a força de trabalho esteja informada do seu conteúdo. Isso pode ser alcançado através de treinamentos e programas de conscientização.

Por fim, a norma ISO/IEC 27002 estabelece diretrizes para implementar e manter a gestão de segurança da informação e essas diretrizes podem ser utilizadas para auxiliar na implementação dos requisitos exigidos pelas normas citadas anteriormente. A norma ISO/IEC 27002 nada mais é do que um guia prático que auxilia o desenvolvimento de procedimentos e práticas para a gestão da segurança da informação.

As áreas de exigências comuns referentes a cada uma das normas e regulamentos apresentados foram agrupadas na tabela a seguir, que correlaciona o controle recomendado pelo padrão ABNT ISO/IEC 27002.

Tabela 1 – Análise comparativa de requisitos

TABELA COMPARATIVA							
Exigências	**Basiléia**	**GLBA**	**SOX**	**FISMA**	**PCI-DSS**	**HIPAA**	**Recomendação ISO 27001**
Criação de uma política de segurança	**X**	**X**	**X**	**X**	**X**	**X**	5.1 5.1.1
Gestão de riscos	**X**	**X**	**X**	**X**	**X**	**X**	4 4.1 4.2 6.2.1 12.5.1 12.6.1 14.1.1 14.1.2
Gestão de ativos	**X**			**X**		**X**	7.1 7.1.1 7.1.2 7.1.3 7.2 7.2.1 7.2.2
Atribuição de responsabilidades para segurança da informação		**X**				**X**	6.1.3
Cumprimento das normas de segurança por terceiros		**X**	**X**	**X**	**X**	**X**	6.2 6.2.3
Segurança de recursos humanos		**X**		**X**		**X**	6.1.5 8.1.1 8.1.2 8.1.3 8.3 8.3.1 8.3.3 11.2.1 15.1.1
Conscientização e Treinamento	**X**		**X**	**X**	**X**	**X**	5.1.1 8.2.2
Procedimentos de resposta a incidentes			**X**	**X**		**X**	6.1.6 10.4.1 13.1 13.1.1 13.2.1 14.1.5 15.1.1
Plano de contingência		**X**			**X**	**X**	10.3.2 10.4.1 10.8.5 14.1.3 14.1.4
Procedimentos para uso e segurança da estação de trabalho			**X**	**X**	**X**	**X**	11.3 11.3.2 11.3.3 11.5.4 11.5.5 11.5.6

TABELA COMPARATIVA							
Exigências	**Basiléia**	**GLBA**	**SOX**	**FISMA**	**PCI-DSS**	**HIPAA**	**Recomendação ISO 27001**
Controles/Segurança de mídias de armazenamento		**X**	**X**	**X**	**X**	**X**	6.2.2 6.2.3 8.3.3 11.2.1 11.2.2 11.2.4 11.7.2
Segurança física	**X**	**X**	**X**	**X**	**X**	**X**	9.1.1 9.1.2 9.1.5 9.1.6 10.5.1
Segurança Ambiental		**X**		**X**			9.1.4 9.2.1 10.5.1 10.7.1
Controle de acesso lógico	**X**	**X**	**X**	**X**	**X**	**X**	11.1. 11.11.1 11.4 11.4.1 11.4.2 11.4.3 11.4.4 11.4.5 11.4.6 11.4.7
Procedimentos de identificação e autenticação	**X**	**X**	**X**	**X**	**X**	**X**	11.2.1 11.2.2 11.2.3 11.2.3 11.2.4 11.4.2 11.4.3 11.5.2 11.5.3 11.7.1
Proteção do Sistema e das Comunicações	**X**	**X**	**X**	**X**	**X**	**X**	10.4.2 10.6.1 10.8.1 10.8.4 10.9.1 10.9.2 10.9.3 11.4.5 11.4.6 11.6 11.6.1 11.6.2 12.3.1 12.3.2
Programa de administração de vulnerabilidades		**X**	**X**	**X**	**X**	**X**	10.4 10.4.1 10.4.2
Implementação de controles para manter a rastreabilidade (registros, logs)	**X**	**X**	**X**	**X**	**X**	**X**	10.10.1 10.10.2 10.10.3 10.10.4 10.10.5 10.10.6

TABELA COMPARATIVA							
Exigências	**Basiléia**	**GLBA**	**SOX**	**FISMA**	**PCI-DSS**	**HIPAA**	**Recomendação ISO 27001**
Auditorias internas	**X**	**X**	**X**	**X**		**X**	15.3 15.3.1 15.3.2
Revisão periódica da política de segurança da informação		**X**	**X**	**X**	**X**	**X**	5.1.2
Certificação e Acreditação			**X**	**X**			6.1.4 10.3.2
Acesso remoto				**X**	**X**	**X**	11.4.2 11.5.5 11.5.6 11.7 11.7.1 11.7.2

6 **CONCLUSÃO**

Diante destas breves visões a respeito dos aspectos de segurança, pode-se observar a constante evolução da segurança com o passar do tempo. O que anteriormente consistia somente em proteger-se contra os crackers, vírus e worms, atualmente evoluiu para uma complexidade de processos de conformidade e gerenciamento de riscos. Garantir a segurança da informação nos dias de hoje envolve a proteção da propriedade intelectual e de vantagens comerciais, monitoração do risco, e principalmente gerenciar a conformidade com a TI e a validação dos controles nas relações de negócios. Se no passado, o gerente de segurança era um tecnólogo, o de hoje precisa ter competência legal e de negócios. [1].

Os ativos, os valores e os pilares que são a base dos processos de produção mudaram, a maneira como é tratado o patrimônio da empresa também mudou e continuará mudando em uma velocidade cada vez maior [4].

Vale ressaltar que várias políticas são comuns às diferentes leis, normas e regulamentações citadas neste trabalho, tais como a criação de uma política de segurança, a existência da gestão de riscos, o cumprimento de normas de segurança por terceiros, a conscientização e treinamento, os procedimentos para uso e segurança da estação de trabalho, controle de acesso lógico, procedimentos de identificação e autenticação, proteção dos sistemas e das comunicações, o programa de administração de vulnerabilidades, a realização de auditorias internas e a necessidade de revisão periódica da política de segurança da informação, entre outros. Estas políticas estão presentes como requisitos da norma ISO/IEC 27002:2005, norma técnica brasileira que auxilia as organizações a estarem em conformidade com a maioria das leis, normas e regulamentações existentes relativas

à Gestão da Segurança da Informação. E ainda assim, com essa diversidade de regulamentos em setores distintos, é possível estar conforme com mais de uma lei, norma ou regulamento devido à inexistência de controles conflitantes entre eles.

Atualmente para que uma empresa possa permanecer no mercado mundial e obter vantagens competitivas é indispensável o comprometimento com a gestão da segurança da informação alinhada aos objetivos do negócio. Além disso, com a implantação de controles de segurança que tenham como objetivo estar conformes com a maioria das leis e normas existentes diversos benefícios são alcançados pela organização, como por exemplo, maior segurança nos processos de negócio, retorno do investimento aplicado, por meio da redução de incidentes relacionados à segurança e solidificação da imagem associada a Segurança da Informação.

Por essa razão é importante estar sempre atento ao surgimento de novas normas e regulamentações, à forma e à tecnologia adotadas para promover o fluxo de dados da empresa de forma a estar sempre em conformidade com a TI.

7 REFERÊNCIAS BIBLIOGRÁFICAS

[1] RASMUSSEN, Michael. Desenvolvendo um programa sustentável e econômico de conformidade com TI, abril de 2008.
Disponível em http://www.rsa.com/solutions/compliance/wp/9767_DSCE_IT_Com_Prog_WP_0408_BR.pdf
Acessado em outubro de 2009.

[2] CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. Segurança em informática e de informações. 2ª. Ed., São Paulo: Senac, 1999, p21-25.

[3] LAUDON, Kenneth C, LAUDON, Jane Price. Sistemas de Informação com Internet. 4a. ed. Rio de Janeiro: LTC-Livros Técnicos e Científicos S. A, 1999.

[4] SÊMOLA, Marcos. Gestão da segurança da informação: visão executiva da segurança da informação. Rio de Janeiro: Campus, p.9 e p.153, 2003.

[5] ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão de segurança da informação". ABNT, p.ix, p.2, 2005

[6] MICROSOFT. Academia Latino Americana de Segurança da Informação. e-modulo, módulo 2, 2005.
Disponível em http://technet.microsoft.com/pt-br/events/cc752934.aspx#EAYAG
Acessado em março de 2009.

[7] MICROSOFT - Academia Latino Americana de Segurança da Informação . e-modulo, módulo 3, cap1, 2005.
Disponível em http://technet.microsoft.com/pt-br/events/cc752934.aspx#EAYAG
Acessado em março de 2009.

[8] GEUS, P.L.; NAKAMURA, E.T. Segurança de redes em ambientes cooperativos. 2a ed São Paulo: Futura, 2003, p 173.

[9] INMETRO, Definições de Regulamento Técnico, Norma e Procedimento de Avaliação da Conformidade.
Disponível em http://www.inmetro.gov.br/barreirastecnicas/definicoes.asp
Acessado em outubro de 2009.

[10] DUPONT, Alexandre. Segurança da Informação – Evitando riscos potenciais. Revista Anefac, número 12, p.7, janeiro 2005.

[11] BIS. BANK FOR INTERNATIONAL SETTLEMENTS. International Convergence of Capital Measurement and Capital Standards – A revised framework. Basel Committee on Banking Supervision. November 2005.
Disponível em http://www.bis.org.
Acessado em janeiro de 2008.

[12] BIS. BANK FOR INTERNATIONAL SETTLEMENTS. Sound Practices for the Management and Supervision of Operational Risk. Basel Committee on Banking Supervision. February 2003.
Disponível em http://www.bis.org.
Acessado em janeiro de 2008.

[13] CARVALHO, E. J. L de. Gerenciamento do risco operacional em organizações financeiras. In: DUARTE Jr., A.M., VARGA, G. (org.) Gestão de Riscos no Brasil. Rio de Janeiro, Financial Consultoria, 2003.

[14] FILHO, Lopes & ASSOCIADOS. O novo acordo de capital da Basiléia (Basiléia II). Boletim Risk Bank , 21/08/02
Disponível em http://www.riskbank.com.br/anexo/basileia2.pdf
Acessado em Janeiro de 2009.

[15] BOECHAT, Dalton e BERTOLOSSI, Flávio Motta. Basiléia II - uma avaliação do impacto das novas regras nas regulações vigentes e captações externas. Retrospectiva 2001, Andima, 2001.
Disponível em http://www.andima.com.br/publicacoes/arqs/2001_basileia.pdf
Acessado em Janeiro de 2009.

[16] BMC Software. Como as soluções BMC Software atendem aos requisitos do Acordo Basiléia II e da lei Sarbanes-0xley.
Disponível em
http://www.cscbrasil.com.br/folhetos/2005/Folheto_SBOX_BAISILEIA.pdf
Acessado em fevereiro de 2009.

[17] GARCIA, Lucio Fabio Tavares; DUARTE, Rodrigo Mendes. Adequações Finais ao Acordo Basiléia II. Estudo da área ERS – Enterprise Risk Services da empresa Deloitte, São Paulo, novembro de 2004.
Disponível em:
http://www4.bcb.gov.br/pre/inscricaoContaB/trabalhos/Apresentacao_Basileia%20II%20BACEN_Deloitte.pdf.
Acessado em fevereiro de 2009.

[18] Setor de cartões de pagamento (PCI). Padrão de segurança de dados Requisitos e procedimentos de avaliação da segurança. Versão 1.2 -Outubro de 2008 Disponível em
https://www.pcisecuritystandards.org/pdfs/pci_dss_portuguese.pdf
Acessado em março de 2009

[19] NEVES, Eduardo Vianna de Camargo. Entendendo o PCI. 2008
Disponível em http://www.netcentrics.com.br/_downloads/Entendendo_o_PCI-DSS.pdf
Acessado em março de 2009

[20] WIKIPEDIA. Payment Card Industry Data Security Standard.
Disponível em http://en.wikipedia.org/wiki/PCI_DSS .
Acessado em março de 2009.

[21] BSAFE INFORMATION SYSTEMS. Fisma. Maio 2008.
Disponível em www.bsafesolutions.com/FISMA%20Bsafe%20Road%20Map.pdf
Acessado em fevereiro de 2009.

[22] FIPS PUBLICATION 200. Minimum Security Requirements for Federal Information and Information Systems. 2006.
Disponível em http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
Acessado em fevereiro de 2009.

[23] BARKER, William C. NIST Special Publication 800-53 Revision 2 - Recommended Security Controls for Federal Information Systems.
http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf
Acessado em fevereiro de 2009.

[24] WIKIPEDIA. Federal Information Security Management Act of 2002.
Disponível em
http://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002
Acessado em fevereiro de 2009.

[25] NIST- Computer Security Division. FISMA Overview.
Disponível em http://csrc.nist.gov/groups/SMA/fisma/overview.html
Acessado em fevereiro de 2009.

[26] WIKIPEDIA. Health Insurance Portability and Accountability Act.
Disponível em
http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act
Acessado em novembro 2008.

[27] MICROSOFT CORPORATION. Regulatory Compliance Demystified: An Introduction to Compliance for Developers, 2008.
Disponível em http://msdn.microsoft.com/en-us/library/aa480484.aspx
Acessado em dezembro 2008.

[28] US-HHS. Adminstrative Simplification - Administrative Procedures. 2002.
Disponível em http://aspe.os.dhhs.gov/admnsimp/nprm/sec06.htm
Acessado em dezembro 2008.

[29] US-HHS. Adminstrative Simplification - Physical Safeguards. 2002
Disponível em http://aspe.os.dhhs.gov/admnsimp/nprm/sec07.htm
Acessado em dezembro 2008.

[30] US-HHS. Adminstrative Simplification - Technical Security Services to Guard Data Integrity, Confidentiality, and Availability. 2002.
Disponível em http://aspe.os.dhhs.gov/admnsimp/nprm/sec08.htm
Acessado em dezembro 2008.

[31] US-HHS. Adminstrative Simplification - Technical Security Mechanisms. 2002.
Disponível em http://aspe.os.dhhs.gov/admnsimp/nprm/sec09.htm
Acessado em dezembro 2008.

[32] US-HHS, HIPAA Administrative Simplification Regulation Text; United States Dept. of Health and Human services.
Disponível em http://www.hhs.gov/ocr/AdminSimpRegText.pdf
Acessado em dezembro de 2008.

[33] ROIWEBED. RoiAdvise Security Matrix. 2002.
Disponível em: www.roiwebed.com/secure/docs/HIPAAsecuritymatrix.pdf
Acessado em janeiro de 2009.

[34] NYS OFFICE FOR TECHONOLOGY (OFT). New York State HIPAA Security Matrix Administrative Safeguards. 2003.
Disponível em:
http://www.cumc.columbia.edu/it/about/security/docs/NYStateHIPAASecurity.pdf
Acessado em janeiro de 2009.

[35] HHS. 45 CFR Parts 160 and 164 HIPAA Administrative Simplification: Enforcement; Final Rule. Vol 71, nº 32, 2006.
Disponível em http://privacyruleandresearch.nih.gov/pdf/FinalEnforcementRule06.pdf
Acessado em janeiro de 2009.

[36] American Optometric Association. HIPAA security guidance for health care information in portable computers.
Disponível em http://www.optometryjaoa.com/article/S1529-1839(07)00156-X/ppt
Acessado em dezembro de 2008.

[37] HHS. Security 101 for Covered Entities.Volume 2, paper 1, 2007.
Disponível em
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf
Acessado em fevereiro de 2009.

[38] BORGERTH, Vânia Maria da Costa. SOX: Entendendo a Lei Sarbanes-Oxley – um caminho para a informação transparente. São Paulo: Thompson Learning, 2007.

[39] HAHN, Roberto Carlos. Doutrina: A Lei Sarbanes-Oxley. 2006.
Disponível em http://www.uj.com.br/publicacoes/doutrinas/4161/A_LEI_SARBANES-OXLEY
Acessado em fevereiro de 2009.

[40] BMC Software. Como as soluções BMC Software atendem aos requisitos do Acordo Basiléia II e da lei Sarbanes-0xley. 2005.
Disponível em
http://www.cscbrasil.com.br/folhetos/2005/Folheto_SBOX_BAISILEIA.pdf
Acessado em fevereiro de 2009.

[41] DELOITTE. Lei Sarbanes-Oxley: Guia para melhorar a governança corporativa através de eficazes controles internos. 2003.
Disponível em http://www.deloitte.com/assets/Dcom-Brazil/Local%20Assets/Documents/guia_sarbanes_oxley%281%29.pdf
Acessado em fevereiro de 2009.

[42] COSME, J., WILSON, J. e NEVES, R. Sarbanes-Oxley: Impactos para a Segurança da Informação.
Disponível em http://colab.interlegis.gov.br/attachment/wiki/Trabalhos/Sarbanes-Oxley.pdf
Acessado em fevereiro de 2009.

[43] Oliveira, Tatiane Carla e Campos, Jonas Comin de. Lei Sarbanex Oxley de 2002. 2006.
Disponível em www.inicepg.univap.br/INIC_2006/inic/inic/06/INIC0001037ok.pdf
Acessado em fevereiro de 2009.

[44] PINHEIRO, José Mauricio Santos. Sarbanes-Oxley e o Impacto Sobre a Governança de TI. 2007.
Disponível em http://www.projetoderedes.com.br/artigos/artigo_sarbanes_oxley.php
Acessado em fevereiro de 2009.

[45] WIKIPEDIA, Information Techonology Controls.
Disponível em http://en.wikipedia.org/wiki/Information_technology_controls.
Acessado em fevereiro de 2009.

[46] Vijay Gondhalekar, C.R. Narayanaswamy and
Sridhar Sundaram. The long-term risk effects of the Gramm-Leach-Bliley Act (GLBA) on the financial services industry. Emerald Group Publishing Limited, volume 12, 2007
Disponível em
http://www.emeraldinsight.com/Insight/viewContentItem.do;jsessionid=DA93C01013A2D9C736AA17BDEF258FE3?contentType=Book&contentId=1761412
Acessado em março de 2009.

[47] Security Brigade. Gramm-Leach-Bliley Act Compliance. 2008.
Disponível em http://www.securitybrigade.it/compliance/gramm-leach-bliley_act.php
Acessado em abril de 2009.

[48] WIKIPEDIA. Gramm-Leach-Bliley Act.
http://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act
Acessado em abril de 2009.

[49] Eletronic Privacy Information Center. The Gramm-Leach-Bliley Act — “History of the GLBA. 2009
http://epic.org/privacy/glba/#reduce
Acessado em julho de 2009.

[50] FORTINET. Simplified GLBA Compliance for Community Banks using Fortinet Hardware, Software and Partner Services. WhitePaper. 2006.
Disponível em www.fortinet.com/doc/whitepaper/GLBA-Compliance.pdf
Acessado em abril de 2009.

[51] FEDERAL Interagency Guidelines Establishing Standards for Safeguarding Customer Information. February 1, 2001.

http://www.ffiec.gov/exam/InfoBase/documents/02-joisafeguard_customer_info_final_rule-010201.pdf
Acessado em janeiro de 2009.

[52] BONG, Kevin M. Conducting an electronic information risk assessment for Gramm-Leach-Bliley Act compliance. SANS Institute. 2003.
Disponível em http://www.sans.org/reading_room/whitepapers/auditing/conducting_an_electronic_information_risk_assessment_for_grammleachbliley_act_compliance_1053
Acessado em março de 2010.

[53] ISO27001 SECURITY. ISO/IEC 27002.
Disponível em http://www.iso27001security.com/html/27002.html.
Acessado em outubro de 2009.

ANEXOS

I BASILEIA II – GLOBAL

O Comitê da Basiléia (subordinado ao BIS – Bank of International Settlements), em 1988, introduziu um padrão uniforme para cálculo do capital regulatório mínimo requerido para os bancos internacionalmente ativos denominado de Basiléia I [17] .

Para incluir uma abordagem de gerenciamento de riscos mais completa e sofisticada, o Comitê da Basiléia, em 2004, fez um novo acordo de capital denominado “Convergência Internacional de Mensuração e Padrões de Capital: Uma Estrutura Revisada”, mais conhecido por ‘Basiléia II’[11].

O Basiléia II define os padrões mínimos que as instituições financeiras terão de cumprir para modelar, gerir e reportar os requisitos mínimos de capital transversais às múltiplas dimensões de risco [11]. Ele fixa-se em três pilares (Capital Mínimo Requerido, Revisão no Processo de Supervisão e Disciplina de Mercado) e 25 princípios básicos sobre contabilidade e supervisão. Os três pilares, estabelecidos pelo Comitê da Basiléia, são atos que devem funcionar em conjunto e podem ser adequados a todo o setor, não apenas ao setor bancário internacional[15].

Pilar 1 – Capital Mínimo Requerido

Nesse pilar as entidades devem manter o requisito mínimo de capital para enfrentar os riscos de [14]:

a) Crédito – como as possíveis perdas devido à impossibilidade de o contratante liquidar uma obrigação no momento esperado ou de não fazê-lo a qualquer tempo;
b) Mercado – perdas decorrentes de movimentos adversos nos preços de mercado dos ativos dos bancos que afetam as posições no Balanço Patrimonial;
c) Operacional – perdas diretas ou indiretas decorrente da ineficiência de sistemas, pessoas e controles internos ou por eventos externos.

Para atender a esses requisitos são necessárias ações na área de TI, como por exemplo [16]:

- gerenciamento de dados e rastreamento de processos;
- redução dos riscos, assim como identificação, análise e integração dos ativos de TI;
- realizar uma avaliação da capacidade e disponibilidade dos sistemas e processos para redução e gerenciamento dos riscos;
- definição de dados (*logs*) a serem coletados, armazenados e analisados.

Pilar 2 - Processo de Revisão Supervisora

O segundo pilar tem como finalidade garantir que cada banco tenha processos sólidos internos que permitam uma verificação da adequação do seu capital, com base em uma avaliação completa de seus riscos pelas autoridades de fiscalização. Para este fim, o Comitê estabeleceu quatro princípios fundamentais que devem orientar a fiscalização dos reguladores através das instituições [15]:

a) os bancos devem dispor de processos para avaliar seu capital global em relação ao perfil de risco das suas posições;

b) as autoridades de fiscalização devem examinar as avaliações e estratégias da adequação do capital das instituições;

c) os bancos devem operar acima dos índices mínimos de capital regulador, estabelecendo, se necessário, índices iniciadores e definidores de capital;

d) as autoridades de fiscalização devem procurar intervir em um estágio inicial, para prevenir que o capital caia abaixo dos níveis mínimos exigidos.

O plano de ação para cumprir com os requisitos do segundo pilar deve incluir [16]:

- A adoção de um *framework* de melhores práticas para implementação de novos processos operacionais e de controles para o gerenciamento de riscos;
- Garantir a rastreabilidade dos dados para que possam ser auditados e mapeamento das mudanças passíveis de riscos.

Pilar 3 - Disciplina de Mercado

O terceiro pilar incentiva a evidenciação crescente das informações dos bancos, ou seja, que as instituições financeiras divulguem suas metodologias e procedimentos utilizados, acerca do grau de risco, de modo a assegurar maior transparência sobre a situação financeira e a solidez de uma instituição[14]. Ainda que não seja obrigatória a divulgação de grande parte das informações, se os métodos utilizados pelos bancos forem complexos, os padrões de supervisão exigidos também serão mais rigorosos. Essa exigência possibilita que os clientes entendam melhor o perfil de risco dos bancos promovendo a disciplina de mercado de maneira a beneficiar as instituições bancárias que se mostrarem mais transparentes e melhor administradas [15].

Sound Practices for the Management and Supervision of Operational Risk

Em complementação ao Basiléia II foi publicado em fevereiro de 2003 pelo Comitê de Supervisão Bancária da Basiléia, o documento *Sound Practices for the Management and Supervision of Operational Risk (*Boas Práticas Para o Gerenciamento e Supervisão do Risco Operacional - BIS, 2003b) constituído de 10 princípios, onde dois destes são voltados aos órgãos superiores e o restante destina-se ao desenvolvimento de uma estrutura de gestão de risco operacional de instituições financeiras[12]. Pode ser observado que os princípios de números um, sete e dez convergem para a governança corporativa [13].

Os 10 princípios do documento Boas Práticas Para o Gerenciamento e Supervisão do Risco Operacional

Desenvolvimento de um ambiente apropriado para o gerenciamento de risco

Princípio 1: O conselho de diretores deve ter conhecimentos dos principais aspectos dos riscos operacionais do banco como uma categoria distinta de risco que devem ser gerenciados. E deverá aprovar e rever periodicamente o framework de gerenciamento de risco operacional do banco. O framework deve prover uma definição sólida do risco operacional e estabelecer os princípios de como esse risco deve ser identificado, avaliado, monitorado e controlado/mitigado.

Princípio 2: O conselho de diretores deve assegurar que o framework de gerenciamento de risco operacional do banco está sujeita a uma auditoria interna realizada por pessoal devidamente treinado. A função de auditoria interna não deve ser diretamente responsável pela gestão do risco operacional.

Princípio 3: A administração sênior deve ter a responsabilidade de implementar o framework de gerenciamento de risco operacional aprovada pelo conselho de diretores. O framework deve ser consistentemente aplicado em toda a organização bancária e todo o corpo de funcionários deve compreender as suas responsabilidades no que diz respeito à gestão do risco operacional. A administração sênior também deve ter como responsabilidade o desenvolvimento de políticas, processos e procedimentos de gerenciamento de risco operacional em todos os produtos, atividades, processos e sistemas.

Identificação, avaliação, monitoramento e controle/mitigação (amenização) do risco

Princípio 4: Os bancos devem identificar e avaliar o risco operacional inerente a todos os produtos, atividades, processos e sistemas. Os bancos também devem garantir que, antes de novos produtos, atividades, processos e sistemas serem introduzidos ou realizados, o risco operacional inerente a elas é sujeita a avaliação.

Princípio 5: Os bancos devem implementar um processo para acompanhar regularmente perfis de risco operacional. Relatórios devem ser enviados regularmente à administração sênior e ao conselho de diretores que apóiam/suportam a gestão pró-ativa do risco operacional.

Princípio 6: Os bancos devem ter políticas e procedimentos para controlar e/ou amenizar os riscos operacionais. Os bancos devem rever periodicamente as suas estratégias de controle e ajustar seus perfis de risco de acordo com as estratégias apropriadas.

Princípio 7: Os bancos devem dispor de planos de contingência e continuidade do negócio a fim de assegurar a sua capacidade para operar regularmente e limitar as perdas em caso de interrupção/rompimento do negócio.

Função dos Supervisores

Princípio 8: Os supervisores bancários devem exigir que todos os bancos, independentemente da sua dimensão, possuam um *framework* eficaz a fim de identificar, avaliar, monitorar e controlar os potenciais riscos operacionais como parte de um enfoque geral para a gestão de riscos.

Princípio 9: Os supervisores devem realizar direta ou indiretamente avaliações regulares das políticas, procedimentos e práticas adotadas em avaliação independente de um banco de políticas, procedimentos e práticas relacionadas aos riscos operacionais. Eles também devem garantir a existência de mecanismos apropriados que lhes permitam manter-se informados do desenvolvimento do banco.

Função da Divulgação

Princípio 10: Os bancos devem tornar públicas suas informações a respeito do grau de exposição ao risco de modo a permitir que os participantes do mercado sejam capazes de realizar uma melhor avaliação de cada instituição.

II GRAMM-LEACH-BLILEY ACT (GLBA)

O Gramm-Leach-Bliley Act (GLBA) foi promulgado em 12 de novembro de 1999 e é uma lei do Congresso dos Estados Unidos que permitiu aos bancos comerciais e de investimento se consolidarem [46]. Por exemplo, o Citibank fundiu-se com a Travelers Group, uma companhia de seguros e em 1998 formou o conglomerado Citigroup, uma corporação combinando o banco e os serviços de seguro sob marcas tais como Smith Barney, Shearson, Primerica e Travelers Insurance Corporation. Esta combinação, anunciada em 1993 e finalizada em 1994, teria violado o Glass-Steagall Act e o Bank Holding Company Act, através da combinação de sociedades de seguros e valores mobiliários. A lei foi aprovada para legalizar estas fusões de forma permanente. Historicamente, a indústria é conhecida como a indústria de serviços financeiros. A principal mudança provocada pela Lei consiste no encorajamento aos indivíduos a aplicarem o dinheiro em poupanças e em investimentos na mesma instituição financeira e ela também será capaz de fazê-lo em tempos bons e ruins economicamente falando [47] [49].

Privacidade

A conformidade com a GLBA é obrigatória. O Apêndice B do regulamento de execução (51) exige que cada instituição financeira possua documentado um programa de segurança da informação que inclua proteções administrativas, técnicas e físicas adequadas à complexidade da instituição e ao escopo de suas atividades. Para isso, é preciso primeiramente, realizar uma avaliação regular dos riscos, capaz de identificar possíveis ameaças e riscos à segurança da informação, avaliar a probabilidade de ocorrência e os principais danos potenciais destas

ameaças, e avaliar também a suficiência de controles para mitigação de tais riscos [52]. As diretrizes descritas no programa devem garantir a confidencialidade das informações dos clientes, a proteção contra qualquer ameaça ou risco previsível à segurança ou integridade dos dados e a proteção contra acesso não autorizado [50]. O GLBA coloca em prática três regras para garantir a segurança e integridade dos dados financeiros, são elas: regra de privacidade financeira, regra de proteção e proteção pretexting (contra engenharia social) [47].

Regra de Privacidade Financeira

Essa regra, prevê uma política de privacidade entre a empresa e o consumidor e para isso, exige que as instituições financeiras enviem a cada consumidor um aviso particular no momento em que se estabelece a relação com o mesmo, anualmente. O anúncio particular deve explicar as informações recolhidas sobre o consumidor, onde a informação é compartilhada, como a informação é usada, e a forma como essa informação é protegida. O anúncio também deve identificar o direito do consumidor e optar pela exclusão da informação que é partilhada por entidade não afiliada através do Fair Credit Reporting Act. Caso haja alteração da política de privacidade, o consumidor deve ser notificado novamente, para aceitação [47].

Regra de Proteção

Tem como objetivo a proteção das informações do cliente e exige o desenvolvimento de um plano de segurança que descreve a forma como a empresa está preparada e pretende continuar a proteger as informações pessoais não públicas dos clientes. Este plano deve incluir [47]:

- a determinação, pelo menos, um funcionário para gerenciar as salvaguardas;

- a construção de uma gestão de risco, sobre cada movimentação de informações não públicas;
- o desenvolvimento, o acompanhamento e testes de um programa para garantir a segurança das informações;
- alterar as proteções que forem necessárias, caso sejam realizadas alterações na maneira como a informação é coletada, armazenada e utilizada.

Pretexting Protection (Proteção contra Engenharia Social)

Pretexting (às vezes chamado de "engenharia social") ocorre quando alguém tenta obter acesso a informações pessoais não públicas sem a devida autorização para fazê-lo. Isto poderá ser realizado tomando o lugar do titular da conta, por telefone, pelo correio, por e-mail, ou mesmo por "phishing" (isto é, utilizando um "falso" site ou e-mail para a coleta de dados). O GLBA incentiva as organizações abrangidas por ele a aplicar salvaguardas contra engenharia social, como por exemplo, a conscientização dos empregados através de treinamentos regulares [48].

III **SARBANES-OXLEY ACT (SOX)**

Promulgada em 30 de julho de 2002, a Lei Sarbanes-Oxley Act de 2002, também conhecida como o *Public Company Accounting Reform Act and Investor Protection Act* de 2002 ou apenas por SOX, é uma lei federal norte-americana criada em decorrência a uma série de escândalos financeiros corporativos ocorridos em grandes empresas (Enron, Tyco International, Adelphia, Peregrine Systems e WorldCom) que acarretou o êxodo dos investimentos financeiros na Bolsa de Valores.

Segundo [39], *a Lei Sarbanes-Oxley* objetiva promover melhor a Governança Corporativa através da eficácia dos controles internos que influenciam nos resultados financeiros das organizações. A análise e divulgação das informações financeiras também são exigências da lei. Para isso, os diretores e o Presidente passam a ser responsáveis por estabelecer, avaliar e monitorar a estrutura dos controles internos da corporação, onde o não cumprimento das normas exigidas implica no o pagamento de multas e no cumprimento de penas de reclusão, inclusive para firmas de auditoria e advocacia contratadas.

Dentre as 1107 seções que compõe a SOX, as mais conhecidas são as seções 302 e 404, onde na seção 302 os diretores e o Presidente devem declarar pessoalmente serem responsáveis pelos controles internos e processos de divulgação da empresa. Já a seção 404 exige a realização de uma avaliação anual dos controles e procedimentos internos para emissão de relatórios financeiros [43][44].

A Seção SOX 404 e Tecnologia da Informação

Os processos de informação financeira de muitas empresas dependem, em certa forma dos sistemas de TI. Portanto, os controles de tecnologia da informação que tratam especificamente de riscos financeiros podem estar dentro do escopo da seção SOX 404 [45].

A criação de um *framework* de controles internos, como exigido pela seção 404, pode ser feita segundo as recomendações de padrões como por exemplo, COSO (*Committee of Sponsoring Organizations of the Treadway Commission)* [40] ou COBIT(Control Objectives of Information and Related Technology) [41].

Para o processo de adequação ao SOX, utilizando-se os controles internos do COSO, cinco componentes são considerados: controle do ambiente, análise de risco, atividades de controle, informação e comunicação, monitoramento. Esses componentes, na TI, podem ser consolidados em três áreas: segurança de infra-estrutura, controle de acesso e plano de contingência [42].

IV **FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA)**

O *Federal Information Security Management Act* de 2002 ("FISMA", 44 USC § 3541, et seq.) é uma lei federal dos Estados Unidos promulgada em 2002 com o Título III do E-Government Act de 2002 (Pub.L. 107-347 , 116 Stat. 2899) que declara obrigatória a conformidade de todas as agências governamentais com os padrões FIPS (*Federal Information Processing Standards*) [24] [23].

A lei tem por objetivo reforçar a segurança dos computadores e da rede dentro do governo federal e entidades associadas (tais como contratantes do governo) pela obrigatoriedade de auditorias anuais.

A FISMA chamou a atenção dentro do Governo Federal à segurança cibernética, que já tinha sido muito negligenciada [25].

Processo de cumprimento do FISMA para um sistema de informação

O FISMA impõe um conjunto de procedimentos obrigatórios, conhecidos como requisitos mínimos de segurança para informações federais, que devem ser seguidos por todos os sistemas de informação utilizados ou acionados pela agência governamental federal dos Estados Unidos da América (EUA) ou por outra organização em nome de uma agência governamental dos EUA [24]. De acordo com [22] esses requisitos devem seguir os controles de segurança do *Special Publication 800-53*, que foram desenvolvidos através de uma combinação de variadas fontes, que incluem o *NIST Special Publication 800-26*, a Norma ISO/IEC 17799, o *General Accounting Office* (GAO), o *Federal Information System Controls Audit Manual (FISCAM) e* Saúde e Serviços Humanos (HHS) e Centros de Serviços *Medicare e*

Medicaid (CMS) *Core Security Requirements*. Tais requisitos de segurança abrangem as seguintes áreas:

- Avaliação de Riscos;
- Certificação, Reconhecimento/Credenciamento e Avaliação da Segurança;
- Gerenciamento da Configuração;
- Planejamento da Segurança;
- Proteção do Sistema e das Comunicações;
- Segurança do corpo de funcionários;
- Sensibilização e Formação/Treinamento;
- Proteção Física e Ambiental;
- Proteção das Mídias;
- Plano de Contingência;
- Manutenção;
- Integridade do Sistema e da Informação;;
- Resposta à Incidentes;
- Procedimentos de identificação e autenticação;
- Controle de acesso e
- Prestação de Contas e Auditoria.

O FISMA tem como visão promover o desenvolvimento das principais normas de segurança e orientações para apoiar a sua implementação e o seu cumprimento e para que isso ocorra são abordadas [21]:

- normas para categorizar a informação e sistemas de informação pelo impacto da missão;

- normas para requisitos mínimos de segurança da informação e sistemas de informação;
- orientações para selecionar controles de segurança adequados para os sistemas de informação;
- orientações para avaliar controles de segurança nos sistemas de informação e para determinação da eficácia desses controles;
- orientações para a certificação e reconhecimento/credenciamento dos sistemas de informação.

V PAYMENT CARD INDUSTRY (PCI) SECURITY STANDARD – GLOBAL

O Payment Card Industry Data Security Standard (PCI-DSS) é um padrão de segurança para proteção de dados de cartão de crédito introduzido em 2001 pela VISA dos Estados Unidos. [20] O principal objetivo do padrão foi reduzir as fraudes em larga escala com cartão de crédito em ambientes de pagamento eletrônico, tanto via Internet quanto em estabelecimentos comerciais tradicionais. Neste sentido, o mercado financeiro de pagamentos, mais especificamente de cartões de créditos tem que estar em conformidade com esta norma, principalmente devido ao crescimento rápido do dinheiro de plástico, o que certamente se tornará uma das principais formas de pagamento nos mercados mundiais [19].

O PCI – DSS contempla 12 requerimentos básicos agrupados em 6 grupos, que são conhecidos como “objetivos de controle” [18]:

- Manter uma rede segura

Requisito1: Instalar e manter uma configuração de firewall para proteger os dados;

Requisito 2: Não usar senhas padrões de sistema e outros parâmetros de segurança fornecidos pelos prestadores de serviços;

- Proteger os dados do portador de cartão

Requisito 3: Proteger os dados armazenados;

Requisito 4: Codificar a transmissão dos dados do portador de cartão e as informações importantes que transitam nas redes públicas;

- Manter um programa de gerenciamento de vulnerabilidades

Requisito 5: Usar e atualizar regularmente o software antivírus;

Requisito 6: Desenvolver e manter seguros os sistemas e aplicativos;

- Implementar medidas rígidas de controle ao acesso

Requisito 7: Restringir o acesso a apenas aqueles que necessitam conhecê-los para a execução de suas funções;

Requisito 8: Atribuir um ID único para cada pessoa que possua acesso ao computador;

Requisito 9: Restringir ao máximo o acesso físico aos dados do portador de cartão;

- Testar e monitorar a rede regularmente

Requisito 10: Acompanhar e monitorar todo o acesso aos recursos da rede e dados do portador de cartão;

Requisito 11: Testar regularmente os sistemas e os processos de segurança;

- Manter uma política que atenda à segurança da informação

Requisito 12: Manter uma política que atenda a segurança da informação.

VI **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)**

O "Health Insurance Portability and Accountability Act" (HIPAA) foi promulgado no dia 26 de agosto de 1996 pelo Congresso do EUA e em abril de 2003 e esperáva-se a sua atuação completa em todos os Estados Unidos da América. O HIPAA estabelece regulamentações federais que determinam padrões mínimos onde médicos, planos de saúde, hospitais, provedores individuais de Serviços de Saúde e fornecedores de assistência médica são obrigados a cumprir. [26]. Esses padrões foram criados com a finalidade de assegurar a confidencialidade e integridade das informações de saúde eletrônicas protegidas (ePHIs) e do seu uso em transações eletrônicas, garantindo assim a segurança de sua portabilidade. Quando essas informações são armazenadas em meio digital elas passam (ePHIs), como por exemplo prontuários médicos e registros [27].

As informações pessoais e de saúde dos pacientes eram consideradas propriedade da instituição de saúde, devido ao fato de serem armazenadas em bancos de dados pertencentes à organização. Esse paradigma foi quebrado, porque de acordo com o conceito do HIPAA, as organizações proprietárias dos bancos de dados, em conformidade com a Lei são apenas intermediários, sendo assim responsáveis por assegurar a segurança dos proprietários dessas informações. Com isso, os pacientes passaram a ter controle sobre suas informações de saúde, o uso do prontuário foi limitado, a garantia da segurança das informações individuais passou a existir e penalidades foram criadas para punir aqueles que não cumprirem com essas determinações [27][26].

O HIPAA subdivide-se em duas seções. A primeira delas, denominada Denominação I assegura a portabilidade da cobertura do seguro de saúde para os

trabalhadores e suas famílias ao mudarem ou perderem seus empregos. A Denominação II trata de provisões sobre a Simplificação Administrativa (parte no. 164) e é composta por três subseções: as Regras de Privacidade, as Regras de Intercâmbio Eletrônico de Dados e as Regras de Segurança. A regra de Privacidade abrange todos os papéis e meios eletrônicos do Protected Health Information (PHI), a Regra de Segurança trata especificamente da Eletronic Protected Health Information (ePHI) [27]. Ela estabelece os três tipos de garantias de segurança exigidas para o cumprimento: proteções administrativas, físicas e técnicas para a manutenção da integridade da ePHI [32].

Como o objetivo deste trabalho é abordar os tópicos específicos de conformidade técnica, somente assuntos relacionados a requisitos de Segurança serão estudados.

Cada padrão técnico do HIPAA estabelece dois tipos de requisitos: os exigidos e os aplicáveis. Requisitos exigidos devem ser cumpridos por todas as organizações de saúde que busquem estar conforme com a legislação do HIPAA [34]. Itens considerados requisitos aplicáveis também são obrigatórios, mas eles oferecem às organizações a possibilidade de adequarem-se ou não para estar em conformidade. Para isso, a entidade coberta deve avaliar se é razoável e adequado o seu cumprimento. Se a entidade abrangida, com base na avaliação realizada, optar por não implementar os requisitos aplicáveis, então ela deve documentar o motivo e, se necessário, aplicar uma medida alternativa equivalente [37].

Proteções Administrativas

São políticas e procedimentos concebidos para mostrar claramente a forma como a entidade vai cumprir esta proteção. As entidades abrangidas (entidades que têm de cumprir os requisitos do HIPAA) [35] devem adotar um conjunto de

procedimentos de privacidade e designar um funcionário para ser responsável por desenvolver e implementar todas as políticas e os procedimentos exigidos [29].

- as políticas e procedimentos devem referenciar a visão da gestão organizacional em conformidade com o controle de segurança e documentada.
- os procedimentos devem identificar claramente os empregados ou classes de trabalhadores que terão acesso às informações eletrônicas de saúde protegidas (ePHI). Acesso à ePHI deve ser restrito aos empregados que necessitem tê-la para executar a sua função.
- os procedimentos devem abordar autorização de acesso, criação, modificação e finalização.
- entidades devem mostrar que um apropriado programa de treinamento no manuseio de PHI é fornecido para os empregados que exercem funções administrativas.
- entidades abrangidas que delegam parte do negócio a terceiros devem assegurar que os seus fornecedores também cumpram com os requisitos HIPAA. As empresas normalmente ganham esta garantia através das cláusulas contratuais que afirmam que o vendedor irá cumprir os mesmos requisitos de proteção de dados que se aplicam às entidades abrangidas.
- um plano de emergência deve ser posto em prática para responder a emergências. Entidades abrangidas são responsáveis por fazer o backup de seus dados e a recuperação de procedimentos. O plano deverá documentar a prioridade dos dados, a análise de falhas, a análise das atividades e alterar os procedimentos de controle.
- as auditorias internas desempenham um papel fundamental no HIPAA pela revisão de operações com o objetivo de identificar potenciais violações de

segurança. Políticas e procedimentos que devem documentar especificamente o escopo, freqüência, e os procedimentos de auditoria. As auditorias devem ser rotineiras e, também, pontuais.

- os procedimentos devem documentar instruções para enfrentar e responder às violações de segurança que são identificados, quer durante a auditoria ou no curso normal das operações [36].

Proteções Físicas

São proteções para controlar o acesso físico inadequado e proteger contra o acesso a dados protegidos.

- controles devem reger a introdução e remoção de hardware e software da rede. (Quando o equipamento é retirado, garantir que o PHI não seja comprometido.)
- o acesso aos equipamentos que contenham informação de saúde deve ser, cuidadosamente, controlada e vigiada.
- acesso a hardware e software deve ser limitado a pessoas devidamente autorizadas.
- controles de acesso consistem em planos de segurança das instalações, manutenção de registros e de visitas e acompanhantes.
- as políticas são necessárias para um uso adequado da estação de trabalho. As estações de trabalho devem ser removidas de áreas de alto tráfego e as telas dos monitores não devem ser vistas diretamente pelo público.
- se as entidades abrangidas utilizam contratantes ou agentes, eles também devem estar plenamente treinados nas responsabilidades de seu acesso físico [29] [33][36].

Proteções Técnicas

Estas proteções controlam o acesso aos sistemas e permitem que as entidades abrangidas protejam as comunicações contendo PHI que são transmitidas eletronicamente através de redes abertas de serem interceptadas por qualquer outra pessoa que não o destinatário.

- sistemas de informação de PHI devem ser protegidos contra intrusão. Quando as informações fluem através de redes abertas, estas devem estar criptografadas adequadamente. Se sistema fechado/redes são utilizados, o controle de acesso é suficiente e a criptografia é opcional;
- cada entidade abrangida é responsável por garantir que os dados dentro de seus sistemas não tenham sido alterados ou apagados de uma maneira não autorizada;
- corroboração de dados, incluindo o uso de check-sum, doble-keying, mensagem de autenticação e assinatura digital podem ser usados para garantir a integridade dos dados;
- entidades abrangidas também devem autenticar entidades, caso comunique-se com elas;
- entidades abrangidas devem apresentar documentação de suas práticas de acordo com o HIPAA à disposição do governo para demonstrar a conformidade;
- além de políticas e procedimentos de acesso a registros, a documentação de tecnologia da informação deve incluir, ainda, um registro por escrito de todas as configurações dos componentes da rede;
- análise de risco documentada e programas de gestão de risco são obrigatórios [36][30][33].

Os requisitos técnicos mandatórios do HIPAA, nos âmbitos administrativo, físico e técnico podem ser encontrados em [26] [34]. E embora o HIPAA não especifique quais são as soluções tecnológicas necessárias para cumprir esses requisitos, estas podem ser necessárias, tais como [35]:

- controles de autenticação, como nome de usuário exclusivo, senhas ou uso de dispositivos biométricos;
- sistema operacional, aplicação ou mesmo controle de acesso ao diretório de serviço para permitir ou negar o acesso baseado no usuário, em sua função ou departamento;
- dispositivos de segurança de rede como firewall ou um sistema de detecção de intruso (IDS);
- dispositivos de filtragem de conteúdo, como varredura de e-mail para detectar PHIs vulneráveis sendo enviadas através da rede e programas antivírus para detectar softwares mal-intencionados;
- software de criptografia para proteger PHIs, em repouso ou em trânsito;
- rede privada virtual (VPN) para garantir acesso a comunicação remota rede-rede;
- sistemas *Logging*, incluindo funções *built-in logging* do sistema operacional e aplicações para fins de rastreamento de auditoria;
- política de gestão de software para edição e gestão de políticas HIPAA e para auxiliar na conscientização do usuário final do HIPAA;
- software de gestão de *patchs* (programa criado para atualizar ou corrigir um software) e para facilitar a gestão em curso e implantação de atualizações críticas de software.

VII **NORMA ABNT NBR ISO/IEC 27002:2005**

A norma ISO 27002 foi publicada pela primeira vez no ano de 2005 com o nome de ISO 17799:2005. Sua antecessora, BS7799 originou-se de um código de prática publicado em 1993 pelo governo britânico (*Department of Trade and Industry* - DTI), que em 1995 foi publicado como padrão pelo BSI (*British Standard Institution*) como BS7799. Em 2000, foi novamente re-publicado, desta vez pela ISO, tornando-se a ISO 17799; e constituía a base atual da norma. Em 2007 uma versão atualizada da norma, a ISO 17799:2005, foi renomeada a fim de ser incorporada ao novo esquema de numeração ISO 27000, que iniciava uma nova série de padrões internacionais para segurança da informação [53].

Ela estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma Organização. Os objetivos de controle e os controles desta Norma têm como finalidade ser implementados para atender aos requisitos identificados por meio da análise/avaliação de riscos. Esta norma pode servir como um guia prático para desenvolver os procedimentos de segurança da informação da Organização e as eficientes práticas de gestão da segurança (ISO/IEC 27002) [6].

A ISO 27002 é constituída de 11 seções de controles de segurança da informação, cada seção contendo as principais categorias de segurança, onde cada categoria principal de segurança da informação possui um objetivo de controle que define o que deve ser alcançado e um ou mais controles que possam colocados em prática para atingir esse objetivo de controle. Tais seções e a quantidade de categorias são listadas abaixo [6]:

- Política de Segurança da informação - 1;

- Organizando a Segurança da informação - 2;
- Gestão de ativos - 2;
- Segurança em Recursos Humanos – 3;
- Segurança Física e do Meio Ambiente – 2;
- Gestão das Operações e Comunicações – 10;
- Controle de Acesso – 7;
- Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação – 6;
- Gestão de Incidentes de Segurança da Informação – 2;
- Gestão da Continuidade do Negócio – 1;
- Conformidade – 3.

A Relação entre ISO 27001 e ISO 27002

A ISO/IEC 27001, publicada em 2005, é uma norma que define os requisitos para estabelecimento de um Sistema de Gestão de Segurança da Informação (SGSI) utilizando a metodologia do PDCA (*Plan-Do-Check-Act*) por meio do estabelecimento de uma política de segurança, controles e gerenciamento de riscos. Por estar de acordo com tais requisitos, a implementação desse padrão pode ser realizada com base nas orientações da ISO 27002, fazendo com que dessa forma os dois documentos sejam utilizados em conjunto de forma que um complemente o outro.

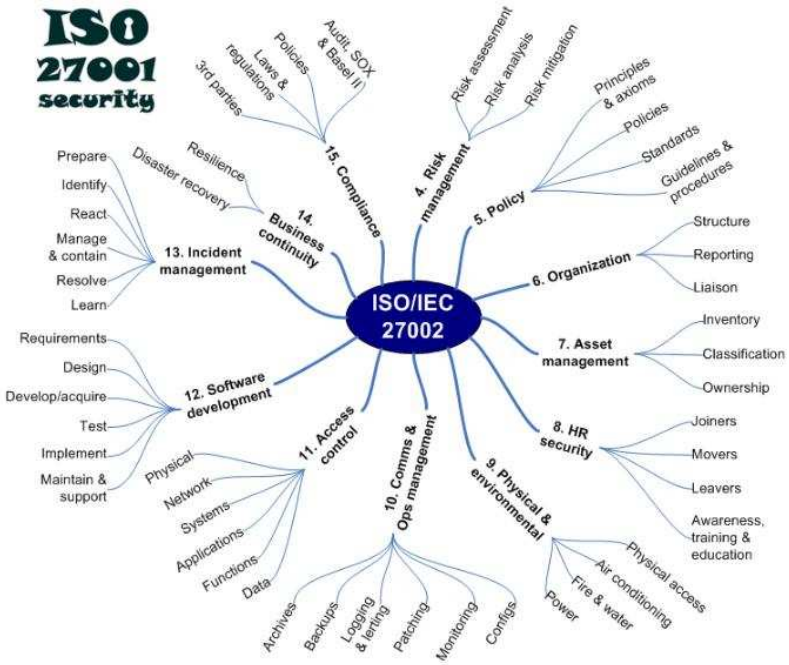


Figura 1 – ISO/IEC 27002