Carlos Eduardo Ribas

**Sistema de gestão de segurança da informação
em organizações da área da saúde**

Dissertação apresentada à Faculdade de
Medicina da Universidade de São Paulo para
obtenção do título de Mestre em Ciências

Programa de: Fisiopatologia Experimental

Orientador: Prof. Dr. Marcelo Nascimento Burattini

São Paulo

2010

Dados Internacionais de Catalogação na Publicação (CIP)

Preparada pela Biblioteca da
Faculdade de Medicina da Universidade de São Paulo

©reprodução autorizada pelo autor

Ribas, Carlos Eduardo

Sistema de gestão de segurança da informação em organizações da área da
saúde / Carlos Eduardo Ribas. -- São Paulo, 2010.

Dissertação(mestrado)--Faculdade de Medicina da Universidade de São Paulo.
Programa de Fisiopatologia Experimental.

Orientador: Marcelo Nascimento Burattini.

Descritores: 1.Gerenciamento da informação 2.Segurança (computação)
3.Normas técnicas

USP/FM/DBD-353/10

DEDICATÓRIA

Dedico este trabalho ao meu pai Paulo Ribas (em memória) e a minha mãe Glacira Ribas como retribuição aos anos de dedicação, sacrifícios e renúncias em prol da minha formação e da minha educação.

Dedico também a minha esposa Laila Massad Ribas e a nossa filha que está por vir, Isabela Massad Ribas, por estarem sempre ao meu lado, me incentivando e ajudando em todos os momentos. Amo vocês!

AGRADECIMENTOS

Ao Prof. Dr. Marcelo Nascimento Burattini pela orientação, colaboração, apoio e incentivo.

Aos meus amigos Marcio Biczuk do Amaral, Jose Sergio Gonçalves Soares, Aurélio Jose Vitorino, Pedro Jose Pimentel, Newton George dos Santos Lima e Simone Bracalle Ambrogi Cunha pela ajuda na realização deste trabalho.

Aos funcionários da Divisão de Laboratório Central, local onde seria realizado este projeto, pelo apoio e compreensão.

Ao Prof. Dr. Eduardo Massad pelo incentivo, pela ajuda na revisão do artigo e pela ajuda com a análise estatística.

À Dra. Clarice Gameiro da Fonseca Pachi pela ajuda na avaliação dos resultados.

Ao Antonio João Ferreira Francisco e a Anna Paula Amadeu da Costa pela ajuda na elaboração do questionário.

À minha amiga Silvia Cruz pela ajuda com a língua inglesa.

Ao Prof. Dr. Jorge Futoshi Yamamoto pelo apoio e incentivo.

Aos meus irmãos, amigos e a todos que de alguma forma colaboraram para a realização deste projeto.

NORMALIZAÇÃO ADOTADA

Essa dissertação está de acordo com:

Referências: adaptado de *International Committee of Medical Journals Editors* (Vancouver)

Universidade de São Paulo, Faculdade de Medicina, Serviço de Biblioteca e Documentação. *Guia de apresentação de dissertações, teses e monografias*. Elaborado por Anneliese Carneiro da Cunha, Maria Julia de A. L. Freddi, Maria F. Crestana, Marinalva de Souza Aragão, Suely Campos Cardoso, Valéria Vilhena. 2ª ed. São Paulo: Serviço de Biblioteca e Documentação; 2005.

Abreviaturas dos títulos dos periódicos de acordo com *List of Journals Indexed in Index Medicus*.

SUMÁRIO

Lista de siglas

Lista de tabelas

Lista de figuras

Resumo

Summary

1 INTRODUÇÃO.....	1
1.1 Sistema de Gestão de Segurança da Informação.....	1
1.2 Justificativas	6
2 REVISÃO DA LITERATURA	7
2.1 Segurança da Informação	7
2.2 Segurança em Rede de Computadores	8
2.3 Segurança da informação na área da saúde.....	13
2.4 Os Componentes Básicos.....	14
2.4.1 Ativo	14
2.4.2 Ameaça.....	15
2.4.3 Vulnerabilidade	15
2.4.4 Risco.....	15
2.4.5 Impacto	16
2.4.6 Negócio.....	16
2.4.7 Interação entre os componentes	16
2.5 Normas de Segurança da Informação.....	17

2.5.1 ISO/IEC 27001	18
2.5.2 ISO/IEC 27002	19
2.5.3 ISO/IEC 27799	20
2.6 Ambiente Analisado	21
3 OBJETIVOS	22
3.1 Objetivo Geral	22
3.2 Objetivos Específicos	22
4 MÉTODO	23
4.1 Seleções das normas	23
4.2 Estruturação do projeto	23
4.3 Planejamento	25
4.3.1 Definição dos indicadores e avaliação de diagnóstico	25
4.3.1.1 ISO/IEC 27001:2006	26
4.3.1.2 Questionário	28
4.3.2 Criação do Comitê de Segurança	32
4.3.3 Definição do escopo	32
4.3.4 Inventário dos Ativos	33
4.3.5 Definição de Responsabilidades	34
4.3.6 Elaboração da Política de Segurança	34
4.3.7 Análise/Avaliação de Riscos	36
4.3.8 Definição dos controles	37
4.3.9 Plano de tratamento de risco	38
4.3.10 Declaração de aplicabilidade	38
4.4 Implantação	39

4.4.1 Executar o Plano de Tratamento de Risco.....	39
4.4.2 Implantação dos controles	39
4.4.3 Realizar treinamentos e implementar programas de conscientização	39
4.4.4 Controle de documentos.....	40
4.5 Avaliação	41
4.5.1 Auditoria interna	41
4.5.2 Análise crítica.....	41
4.5.3 Auditoria independente	42
4.5.4 Avaliação de diagnóstico	42
5 RESULTADOS	43
5.1 Documentos gerados	43
5.2 Indicadores.....	49
5.2.1 ISO/IEC 27001:2006.....	49
5.2.2 Questionário	54
6 DISCUSSÃO.....	61
7 CONCLUSÕES.....	66
8 ANEXOS	67
Anexo A – Amostra da planilha gerada com base nos controles do “Anexo A” da ISO 27001.....	67
Anexo B – Padrão de documento criado para o SGSI	68
Anexo C – Comitê de segurança da informação	69
Anexo D – Escopo do SGSI	71
Anexo E – Regulamento Interno de Segurança da Informação	73

Anexo F – Termo de Responsabilidade com a Segurança da Informação	78
Anexo G – Declaração de aplicabilidade.....	80
9 REFERÊNCIAS	81

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
COBIT	Control Objectives for Information and related Technology
HCFMUSP	Hospital das Clínicas da Faculdade de Medicina da Universidade de São Paulo
HIPAA	Health Insurance Portability and Accountability Act
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISRAM	Information Security Risk Analysis Method
ITIL	Information Technology Infrastructure Library
NBR	Norma Brasileira
NETI	Núcleo Especializado em Tecnologia da Informação
PDCA	Plan, Do, Check, Act
SGSI	Sistema de Gestão de Segurança da Informação

LISTA DE TABELAS

Tabela 1 – Países com maior número de certificações.....	5
Tabela 2 – Algumas pessoas que podem causar problemas de segurança e os motivos para fazê-los	10
Tabela 3 – Descrição dos capítulos da ISO 27001	18
Tabela 4 – Possíveis valores para os controles analisados	27
Tabela 5 – Classificação dos riscos	36
Tabela 6 – Níveis de riscos	37
Tabela 7 – Documentos gerados para o SGSI.....	40
Tabela 8 – Descrição dos servidores	46
Tabela 9 – Descrição dos equipamentos de rede	46
Tabela 10 – Descrição das mídias	46
Tabela 11 – Informações dos funcionários do NETI.....	46
Tabela 12 – Análise/Avaliação de risco.....	48
Tabela 13 – Medidas que serão tomadas para cada risco encontrado	48
Tabela 14 – Análise estatística da pontuação obtida no início e ao término do projeto.....	49
Tabela 15 – Análise estatística dos controles implementados	50
Tabela 16 – Análise estatística dos controles parcialmente implementados	51
Tabela 17 – Análise estatística dos controles não implementados	52
Tabela 18 – Análise estatística dos controles obrigatórios.....	53
Tabela 19 – Número de pessoas que responderam ao questionário.....	54

Tabela 20 – Análise estatística do questionário	55
---	----

LISTA DE FIGURAS

Figura 1. Ciclo PDCA aplicado aos processos do SGSI	3
Figura 2. O crescente número de certificações no mundo.....	5
Figura 3. Empresas certificadas no Brasil.....	6
Figura 4. Estatística dos incidentes de segurança reportados ao CERT.br do ano de 1999 até março de 2010	12
Figura 5. Interação entre os componentes básicos	17
Figura 6. Ciclo PDCA proposto para o SGSI.....	24
Figura 7. Página de acesso ao questionário	29
Figura 8. Questionário respondido pelos funcionários do NETI – Parte 1 ...	30
Figura 9. Questionário respondido pelos funcionários do NETI – Parte 2 ...	31
Figura 10. Organograma da organização dividida por área, processo e ativo	44
Figura 11. Diagrama do <i>datacenter</i> do NETI.....	45
Figura 12. Análise dos controles obrigatórios	53
Figura 13. Segunda questão do questionário: Minha função tem ligação direta/indireta com a segurança da informação	56
Figura 14. Terceira questão do questionário: Conheço o documento que trata da Política de Segurança da Informação adotada pela organização	57
Figura 15. Quarta questão do questionário: Sou informado quando ocorrem mudanças na Política de Segurança da Informação.....	57
Figura 16. Quinta questão do questionário: Segurança da Informação é um	

item importante para os negócios desenvolvidos na organização	58
Figura 17. Décima primeira questão do questionário: As cópias de segurança são armazenadas em ambientes distintos dos sistemas de origem	58
Figura 18. Décima quarta questão do questionário: As cópias de segurança são criptografadas, tanto na execução quanto em seu armazenamento.....	59
Figura 19. Décima sexta questão do questionário: As cópias de segurança são periodicamente testadas para garantir que elas são suficientemente confiáveis para o uso de emergência	59
Figura 20. Décima sétima questão do questionário: Existe um ambiente separado para testar os procedimentos de restauração do sistema.....	60

RESUMO

Ribas CE. *Sistema de gestão de segurança da informação em organizações da área da saúde* [dissertação]. São Paulo: Faculdade de Medicina, Universidade de São Paulo; 2010. 87p.

INTRODUÇÃO: Este estudo descreve o processo de implantação de um sistema de gestão de segurança da informação em uma organização de saúde, visando assegurar a confidencialidade, a integridade e a disponibilidade das informações. **MÉTODOS:** Utilizou-se a norma ISO 27001 para o desenvolvimento do projeto e o seu “anexo A”, através de uma nova metodologia, para avaliar a organização. Um questionário foi elaborado para avaliar a percepção dos funcionários com a segurança da informação e também para checar itens relacionados ao escopo do projeto. Avaliamos a segurança da informação no início e ao término do estudo. A análise estatística foi realizada com o teste do qui-quadrado com correção de Yates. O resultado foi considerado significativo para $P < 0,05$. **RESULTADOS:** Houve resultado significativo na pontuação obtida pela organização, no total de controles implementados e no total de controles não implementados. Não houve resultados significativos com o questionário. **CONCLUSÃO:** O uso do SGSI trouxe benefícios para a organização com melhoras significativas no nível de conformidade com a norma de referência, além da redução dos riscos aos ativos da organização por meio da implementação de controles.

Descritores: 1.Gerenciamento da informação 2.Segurança (computação) 3.Normas técnicas

SUMMARY

Ribas CE. *Information security management system in a healthcare organization* [dissertation]. São Paulo: "Faculdade de Medicina, Universidade de São Paulo"; 2010. 87p.

INTRODUCTION: This study describes the implementation's process of an Information Security Management System in a healthcare organization in order to assure the confidentiality, integrity and availability of the information.

METHODS: We used the ISO 27001 standard for development of the project and its "Annex A", through a new methodology, to assess the organization. A questionnaire was designed to estimate the perception of staff with information security and also to check items related to project scope. We evaluated the information security at the beginning and at the end of the study. Statistical analysis was performed with the chi-square test with Yates correction. The result was considered significant for $P < 0,05$. **RESULTS:** The organization obtained significant improves on the score, on the number of implemented controls and on the number of not implemented controls, but there were no significant results with the questionnaire. **CONCLUSION:** The use of ISMS brought benefits to the organization with expressive improvements in the level of compliance with the standard's reference, besides the reduction of risks in the organization's assets through the implementation of controls.

Descriptors: 1.Information Management 2.Computer Security 3.Technical Standards

1 INTRODUÇÃO

1.1 Sistema de Gestão de Segurança da Informação

Um Sistema de Gestão de Segurança da Informação (SGSI) pode ser definido como um sistema de gestão utilizado para estabelecer e manter um ambiente seguro para as informações em uma organização (Sánchez et al., 2006).

Segundo McGee et al. (2007) a organização deve estabelecer, implantar, operar, monitorar, revisar, manter e melhorar um SGSI documentado dentro do contexto das atividades empresariais globais da organização e dos riscos que elas enfrentam.

A adoção de um SGSI deve ser uma decisão estratégica para uma organização. A especificação e a implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos empregados e tamanho e estrutura da organização. É esperado que o SGSI e seus sistemas de apoio mudem com o passar do tempo. É esperado que a implementação de um SGSI seja escalada conforme as necessidades da organização, por exemplo, uma situação simples requer uma solução de um SGSI simples (NBR ISO/IEC 27001:2006).

O SGSI deve identificar os ativos a serem protegidos, a abordagem para gerenciamento dos riscos, os objetivos e controles necessários para

proteger as informações da organização e garantir a continuidade do negócio no grau de qualidade requerido pela organização, seguindo o modelo proposto no PDCA – *Plan-Do-Check-Act* (Planejar-Implantar-Avaliar-Melhorar) (NBR ISO/IEC 27001:2006; Bastos, 2009).

O PDCA foi originalmente desenvolvido na década de trinta, nos laboratórios da *Bell Laboratories* – EUA, pelo estatístico americano *Walter A. Shewhart*, como um ciclo de controle estatístico de processo, que pode ser repetido continuamente sobre qualquer processo ou problema (Souza, 1997; Andrade, 2003).

Contudo, esse método somente foi popularizado na década de cinquenta pelo especialista em qualidade *W. Edwards Deming*, ficando mundialmente conhecido ao aplicar este método nos conceitos de qualidade em trabalhos desenvolvidos no Japão. Após refinar o trabalho original de Shewhart, Deming desenvolveu o que ele chamou de *Shewhart PDCA Cycle*, em honra ao mentor do método (Deming, 1990; Andrade, 2003).

Na estrutura do PDCA para um SGSI, cada uma das atividades pode ser descrita da seguinte forma (NBR ISO/IEC 27001:2006; Bastos, 2009):

- Planejar: estabelecer política do SGSI, objetivos, processos e procedimentos relevantes para o gerenciamento de riscos e a melhoria da segurança da informação para entregar resultados conforme as políticas globais de uma organização e objetivos.
- Fazer: implementar e operar a política do SGSI, controles, processos e procedimentos.
- Verificar: avaliar e, onde aplicável, medir o desempenho de um

processo em relação à política e aos objetivos do SGSI e, então, relatar os resultados para a revisão dos supervisores.

- Agir: tomar as ações corretivas e preventivas, baseado nos resultados da auditoria interna do SGSI e revisão gerencial ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

A Figura 1 ilustra como um ciclo PDCA de um SGSI considera as entradas de requisitos de segurança da informação e as expectativas das partes interessadas, e como as ações necessárias e processos de segurança da informação produzidos resultam no atendimento a estes requisitos e expectativas (NBR ISO/IEC 27001:2006).

Figura 1. Ciclo PDCA aplicado aos processos do SGSI

A gestão da segurança da informação traz benefícios para as organizações que implementam um SGSI, mesmo que o principal objetivo

não seja a obtenção da certificação junto a um organismo certificador credenciado. Entre outros benefícios específicos, Bastos (2009) cita os mais comuns:

- Fortalecer a percepção de segurança perante os usuários, clientes, fornecedores, sociedade, funcionários, acionistas, agências reguladoras e judiciárias;
- Integração da segurança da informação com os objetivos de negócio;
- Segurança da informação demonstrável e monitorada;
- Linguagem única internacional com padrões da família ISO 27000;
- Atendimento a requisitos jurídicos e regulatórios;
- Fortalecimento da cadeia de valor de segurança e tecnologia da informação;
- Aprimoramento da gestão de segurança da informação na organização, devido à aplicação do ciclo PDCA;
- Melhoria no poder de negociação de Riscos Operacionais e Seguros;
- Fortalecimento da área e profissionais de segurança da informação da organização.

A Figura 2 mostra um levantamento do número de empresas certificadas na norma ISO 27001, no mundo entre julho de 2005 e janeiro de 2010 (iso27001security).

Figura 2. O crescente número de certificações no mundo

A Tabela 1 mostra o número total de SGSI certificados na norma ISO 27001 por país.

Tabela 1 – Países com maior número de certificações

Posição	País	Quantidade
1°	Japão	3499
2°	Índia	494
3°	Reino Unido	444
4°	Taiwan	373
5°	China	362
6°	Alemanha	137
7°	Coréia	106
8°	EUA	96
9°	República Tcheca	85
10°	Hungria	71
11°	Itália	60
12°	Polônia	56
13°	Espanha	40
14°	Irlanda	37
15°	Áustria	35
16°	Tailândia	34
17°	Hong Kong	31
18°	Austrália	29
19°	Grécia	27
20°	Malásia	27
21°	Romênia	26
22°	México	24
23°	Brasil	23
24°	Turquia	21
25°	Emirados Árabes Unidos	19

FONTE: www.iso27001certificates.com, acessado em 23/06/2010

No Brasil, entre as empresas que possuem a certificação ISO 27001 (Figura 3), nenhuma atua na área da saúde (iso27001certificates. Acessado em 21/06/2010).

Name of the Organization	Country	Certificate Number	Certification Body	Standard BS 7799-2:2002 or ISO/IEC 27001:2005
Atos Origin Brasil Ltda	Brazil	IS 98429		ISO/IEC 27001:2005
Axur Information Security	Brazil	IS 509742		ISO/IEC 27001:2005
BT	Brazil	LRQ 4003984	LRQA	ISO/IEC 27001:2005
Cardif do Brasil Vida e Previdencia S/A	Brazil	IS 521855		ISO/IEC 27001:2005
CIP Camara Interbancaria de Pagamentos	Brazil	IS 96934		ISO/IEC 27001:2005
Fucapi-Fundacao	Brazil	IS 504391		ISO/IEC 27001:2005
IBM ITD Brazil	Brazil	62.691	Bureau Veritas Certification - Brazil	ISO/IEC 27001:2005
Módulo Security Solutions S/A	Brazil	IS 510466		ISO/IEC 27001:2005
Poliedro - Informática, Consultoria e Serviços Ltda.	Brazil	44121081309		ISO/IEC 27001:2005
Prodesp	Brazil	IS 512881		ISO/IEC 27001:2005
Promon Engenharia Ltda.	Brazil	IS 500248		ISO/IEC 27001:2005
Promon Tecnologia Ltda	Brazil	IS 500564		ISO/IEC 27001:2005
Samarco Mineração S/A.	Brazil	IS 524157		ISO/IEC 27001:2005
SERASA S.A.	Brazil	262326 ISMS		ISO/IEC 27001:2005
Serviço Federal de Processamento de Dados - SERPRO	Brazil	IS 515421		ISO/IEC 27001:2005
Superior Tribunal de Justiça	Brazil	IS 538457		ISO/IEC 27001:2005
Telefonica Empresas S/A	Brazil	IS 501039		ISO/IEC 27001:2005
Tivit Tecnologia da Informacao S.A.	Brazil	00017-2006-AIS-OSL-NA	DNV	ISO/IEC 27001:2005
TIVIT TERCEIRIZAÇÃO DE TECNOLOGIA E SERVIÇOS S.A.	Brazil	16203-2007-AIS-BRA-NA	DNV	ISO/IEC 27001:2005
T-Systems Brazil	Brazil	336227 ISMS		ISO/IEC 27001:2005
T-Systems do Brasil Ltda.	Brazil	341898 ISMS		ISO/IEC 27001:2005
UNISYS Global Outsourcing	Brazil	IS 97102		ISO/IEC 27001:2005
Zamprogna S/A Importacao	Brazil	IS 518855		ISO/IEC 27001:2005

Figura 3. Empresas certificadas no Brasil

1.2 Justificativas

Diversas organizações no mundo possuem um sistema de gestão de segurança da informação auditado e certificado. No Brasil existem poucas empresas que utilizam um SGSI e, entre aquelas que o utilizam, nenhuma atua na área da saúde. Portanto, pretende-se estabelecer, documentar e implementar um SGSI em uma organização da área da saúde e verificar os ganhos obtidos com a segurança da informação.

2 REVISÃO DA LITERATURA

2.1 Segurança da Informação

A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconnectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (ABNT NBR ISO/IEC 27002).

A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente (ABNT NBR ISO/IEC 27002; Bernard, 2007).

Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos,

procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio (ABNT NBR ISO/IEC 27002).

A segurança da informação deve sempre atender a três elementos (Ramos et al., 2008; Miller e Murphy, 2009):

- **Confidencialidade:** quando falamos de confidencialidade estamos, basicamente, falando de sigilo. Preservar a confidencialidade de uma informação significa garantir que apenas as pessoas que devem ter conhecimento a seu respeito poderão acessá-la.
- **Integridade:** a preservação da integridade envolve proteger as informações contra alterações em seu estado original. Estas alterações podem ser tanto intencionais quanto acidentais.
- **Disponibilidade:** garante que uma informação esteja acessível quando alguém que precisa tenta obtê-la. As informações solicitadas devem ser fornecidas conforme esperado pelo demandante.

2.2 Segurança em Rede de Computadores

Com o crescimento das redes de computadores e do desenvolvimento de aplicações baseadas em redes, os aspectos da segurança têm chamado atenção (Duan e Wu, 1999).

Durante as primeiras décadas de sua existência, as redes de computadores foram usadas principalmente por pesquisadores universitários, com a finalidade de enviar mensagens de correio eletrônico, e também por funcionários de empresas, para compartilhar impressoras. Sob essas condições a segurança nunca precisou de maiores cuidados. Porém, como milhões de cidadãos comuns atualmente estão usando as redes para executar operações bancárias, fazer compras e arquivar suas devoluções de impostos, a segurança das redes está despontando no horizonte como um problema em potencial.

A segurança é um assunto abrangente e inclui inúmeros tipos de problemas. Em sua forma mais simples, a segurança se preocupa em garantir que pessoas mal-intencionadas não leiam ou, pior ainda, modifiquem secretamente mensagens enviadas a outros destinatários. Outra preocupação da segurança são as pessoas que tentam ter acesso a serviços remotos que elas não estão autorizadas a usar. Ela também permite que você faça a distinção entre uma mensagem supostamente verdadeira e um trote. A segurança trata de situações em que mensagens legítimas são capturadas e reproduzidas, além de lidar com pessoas que tentam negar o fato de terem enviado determinadas mensagens (Tanenbaum, 2003).

Harrington (2005) diz que ao conversar com alguém que trabalha implementando segurança de redes, muito se ouve sobre buffer overflows, ataques de negação de serviços, entre outras coisas. Mas a segurança da rede vai além de ataques e suas respectivas defesas. Uma boa segurança de rede começa no topo da organização, com um plano para determinar

onde a organização deve concentrar esforços em termos de segurança e onde investir seu dinheiro.

A mídia faz com que se acredite que os problemas de segurança são causados pelos hackers. Contudo, Harrington (2005) relata que ao questionar as pessoas que trabalham na área de segurança, elas dizem que quase metade dos problemas encontrados vem de dentro da empresa e, em particular, dos funcionários. Isto quer dizer que não é suficiente garantir a segurança contra ataques externos, é preciso prestar atenção com o que ocorre dentro da organização.

Tanenbaum (2003) cita que a maior parte dos problemas de segurança é causada intencionalmente por pessoas maliciosas que tentam obter algum benefício, chamar a atenção ou prejudicar alguém. Alguns dos invasores mais comuns estão listados na Tabela 2.

Tabela 2 – Algumas pessoas que podem causar problemas de segurança e os motivos para fazê-los

Adversário	Objetivo
Estudante	Divertir-se bisbilhotando as mensagens de correio eletrônico de outras pessoas
Hacker/Cracker	Testar o sistema de segurança de alguém; roubar dados
Executivo	Descobrir a estratégia de marketing do concorrente
Ex-funcionário	Vingar-se por ter sido demitido
Contador	Desviar dinheiro de uma empresa
Vigarista	Roubar números de cartão de créditos e vende-los
Espião	Descobrir segredos militares ou industriais de um inimigo
Terrorista	Roubar segredos de armas bacteriológicas

FONTE: Tanenbaum A. *Redes de Computadores*. 2003. p.768

Existem vários tipos de ataques (Harrington, 2005), abaixo estão listados os mais comuns:

- Negação de serviço: este tipo de ataque é caracterizado pela explícita tentativa de um atacante de impedir que um usuário legítimo acesse um sistema (Lau et al., 2000). Isto pode ser feito enchendo um servidor ou uma rede com tráfego, fazendo com que usuários legítimos não consigam acessar ou que um servidor pare de funcionar (Harrington, 2005).
- *Malware: Malicious Software* (Software Maldoso) refere-se a vários tipos de softwares que podem causar perdas, danos ou interromper o uso de um computador (Alsagoff, 2008).
- Força bruta: utilizado para obter acesso a um sistema realizando tentativa de acesso por força bruta. Assumindo que um atacante conhece um ou mais usuários de um determinado sistema, ele pode tentar adivinhar a senha (Harrington, 2005).
- Engenharia social: o ponto fraco da segurança da informação geralmente são os usuários, porque as pessoas podem ser manipuladas. Atacar um sistema utilizando informações obtidas por meio de uma conversa é uma forma da engenharia social (Mitnick e Simon, 2002; Laribee et al., 2006).
- *Phishing*: o atacante cria uma réplica de uma página WEB existente com o intuito de obter informações sensíveis dos usuários (Chen e Guo, 2006; Irani et al., 2008).
- *Bot*: termo derivado da palavra *robot*. Trata-se de um pedaço de

um software geralmente instalado na máquina sem o conhecimento do usuário. Ele é programado para responder instruções de um atacante remotamente (Al-Hammadi e Aickelin, 2008).

A Figura 4 mostra estatística sobre notificações de incidentes reportados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br). Estas notificações são voluntárias e refletem os incidentes ocorridos em redes que espontaneamente os notificaram ao CERT.br.

Figura 4. Estatística dos incidentes de segurança reportados ao CERT.br do ano de 1999 até março de 2010

2.3 Segurança da informação na área da saúde

O uso de computadores em hospitais iniciou-se com o uso dos mesmos em funções administrativas, geralmente utilizados pelo setor financeiro. Os registros dos pacientes eram coletados inicialmente para propósitos administrativos (Collen, 1995; Luethi e Knolmayer, 2009).

O uso da documentação em formato eletrônico na área da saúde tem muitas vantagens, mas em contrapartida traz alguns riscos, principalmente do ponto de vista de segurança (Brechlerova e Candik, 2008).

Registro médico contém informações de pacientes, algumas comuns, outras mais sensíveis. Informações sobre a saúde pessoal devem ser confidenciais e o acesso a tal informação deve ser controlado para evitar que a divulgação venha a prejudicar o paciente, por exemplo, causando constrangimento ou prejudicando um emprego (Shortliffe et al., 2001). As companhias de seguros ou os empregadores seriam altamente interessados em tais informações (Huber et al., 2008). Dados médicos devem ser protegidos para evitar perdas, se hoje é utilizado um sistema informatizado, este deve estar disponível sempre que necessário e a informação deve ser exata e atualizada (Shortliffe et al., 2001).

Sistemas de informação estão expostos a numerosas ameaças que podem resultar em perdas significativas e danos aos registros médicos (Ahmad et al., 2009). As ameaças de segurança em sistemas da informação em saúde têm aumentado significativamente nos últimos anos. Por exemplo, durante o período de 2006 a 2007, mais de 1.5 milhões de nomes

foram expostos durante falhas ocorridas em hospitais (Ayotollahi et al., 2008).

O compartilhamento de informações sensíveis tem sido uma preocupação e diferentes abordagens estão sendo tomadas. Nos Estados Unidos depende de uma regulação setorial, na qual se protege a informação de saúde através de legislações, como o *Health Insurance Portability and Accountability Act* (HIPAA) de 1996. Já na maioria dos países europeus, criou-se uma regulamentação legislativa abrangente para privacidade, protegendo todas as informações pessoais independentes da indústria (Samy et al., 2009).

2.4 Os Componentes Básicos

Para que possamos oferecer a segurança adequada que uma organização precisa sem perder de vista o bom senso financeiro dos investimentos, analisamos a interação de alguns agentes e consideramos certos fatores (Ramos et al., 2008).

2.4.1 Ativo

Qualquer coisa que tenha valor para a organização (ISO/IEC 13335-1:2004). No contexto da segurança da informação na saúde, segundo a ISO 27799 os ativos podem ser:

- Informação sobre saúde

- Serviços de tecnologia da informação
- Hardware
- Software
- Dispositivos médicos ou dados de relatório

2.4.2 Ameaça

Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (ISO/IEC 13335-1:2004).

2.4.3 Vulnerabilidade

A ausência de um mecanismo de proteção ou falhas em um mecanismo de proteção existente. São as vulnerabilidades que permitem que as ameaças se concretizem. O que vai determinar se um incêndio pode ou não afetar os negócios de uma empresa é a ausência/existência de mecanismos de prevenção, detecção e extinção, mecanismos de proteção da informação aos seus efeitos, além do correto funcionamento dos mesmos (Ramos et al., 2008).

2.4.4 Risco

Combinação da probabilidade de um evento e de suas consequências (ABNT ISO/IEC Guia 73:2005).

2.4.5 Impacto

Tamanho do prejuízo, medido através de propriedade mensuráveis ou abstratas, que a concretização de uma determinada ameaça causará. Diferentes ameaças possuem impactos diferentes (Ramos et al., 2008).

2.4.6 Negócio

Atividades que são fundamentais aos propósitos para a existência da organização (ISO/IEC 27001:2005).

2.4.7 Interação entre os componentes

A Figura 5 nos ajuda a ter uma ampla visão de como esses componentes interagem. Ele apareceu pela primeira vez em dezembro de 1985 na norma *Trusted Computer System Evaluation Criteria*, popularmente conhecido como *Orange Book*. Este documento foi publicado pelo *National Computer Security Council*, entidade atrelada à *National Security Agency*, agência nacional de segurança dos Estados Unidos (Ramos et al., 2008).

Figura 5. Interação entre os componentes básicos

2.5 Normas de Segurança da Informação

As normas desempenham um papel essencial para a elaboração de um plano de segurança da informação (Karabacak e Sogukpinar, 2006). Elas fornecem uma abordagem sistemática de gestão para adotar as melhores práticas em controles, quantificar o nível de risco aceitável e implementar as medidas adequadas que protejam a confidencialidade, integridade e disponibilidade das informações (Dey, 2007).

A série 27000 de normas da *International Organization for Standardization / International Electrotechnical Commission* (ISO / IEC)

concentra-se nos requisitos, controles de segurança e orientação para implementação de um SGSI na organização (McGee et al., 2007).

2.5.1 ISO/IEC 27001

A ISO 27001 surgiu com base na norma britânica BS7799 e na ISO/IEC 17799 (Fenz et al., 2007). Ela foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação - SGSI (NBR ISO/IEC 27001:2006). Este padrão é o primeiro em segurança da informação relacionado com a família de padrões ISO/IEC (Fenz, et al, 2007). A Tabela 3 apresenta os capítulos da norma com seus respectivos requisitos.

Tabela 3 – Descrição dos capítulos da ISO 27001

Nr	Nome	Descrição
0	Introdução	Apresentação da norma
1	Objetivo	Abrangência da norma
2	Referencia normativa	Outras normas necessárias para o SGSI
3	Termos e definições	Termos e definições sobre segurança da informação
4	Sistema de Gestão de Segurança da Informação	Informações sobre o estabelecimento, a implementação, o monitoramento e a melhoria de um SGSI
5	Responsabilidades da direção	Comprometimento da direção, treinamento e provisão de recursos para o SGSI
6	Auditorias internas do SGSI	Auditorias internas realizadas por pessoal treinado e comprometido com o SGSI
7	Análise crítica do SGSI pela direção	Análise realizada pela direção da organização das ações efetuadas pelo SGSI
8	Melhoria do SGSI	Ações corretivas e preventivas efetuadas pelo SGSI

FONTE: adaptado da ISO 27001

Esta norma é utilizada em todo o mundo por organizações comerciais e governamentais como base para a gestão da política da organização e implementação da segurança da informação. Ela está sendo usada por pequenas, médias e grandes organizações. De fato, o padrão é projetado para ser flexível o suficiente para ser utilizado por qualquer tipo de organização (Humphreys, 2008).

2.5.2 ISO/IEC 27002

A ISO 27002 estabelece um código com as melhores práticas em segurança da informação (Dey, 2007). Ela lista os objetivos de controle e recomenda uma série de controles de segurança específicos (Sahibudin et al., 2008). 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, e para ajudar a criar confiança nas atividades interorganizacionais (ABNT NBR ISO/IEC 27002).

A ISO 27002 contém 11 seções de controles de segurança da informação, que juntas totalizam 39 categorias principais de segurança e uma seção introdutória que aborda a análise/avaliação e o tratamento de riscos (ABNT NBR ISO/IEC 27002). Kamel et al. (2007) cita os 11 capítulos fundamentais da norma:

1. Política de Segurança da Informação
2. Organizando a Segurança da Informação
3. Gestão de Ativos
4. Segurança em Recursos Humanos
5. Segurança Física e do Ambiente
6. Gestão das Operações e Comunicações
7. Controle de Acesso
8. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação
9. Gestão de Incidentes de Segurança da Informação
10. Gestão da Continuidade do Negócio
11. Conformidade

2.5.3 ISO/IEC 27799

A ISO 27799 define diretrizes para auxiliar organizações da área da saúde e outras que armazenam informações médicas na interpretação e na execução da ISO 27002. Não é intenção da ISO 27799 competir com a ISO 27002, e sim complementar a mesma. Todos os objetivos de controle de segurança descritos na ISO 27002 são relevantes para a área da saúde, mas alguns controles requerem esclarecimentos adicionais a respeito de como eles podem ser usados para proteger a confidencialidade, integridade e disponibilidade de informações médicas. Há também requisitos adicionais específicos do setor de saúde. Esta norma fornece uma orientação adicional

de forma que as pessoas responsáveis pela segurança da informação na saúde possam facilmente compreender e aprovar (ISO/IEC 27799).

2.6 Ambiente Analisado

O Núcleo Especializado em Tecnologia da Informação (NETI) é a organização onde está sendo realizado o desenvolvimento deste projeto. O NETI atua na área da tecnologia da informação em um dos hospitais mais importantes do Brasil, o Hospital das Clínicas da Faculdade de Medicina da Universidade de São Paulo (HCFMUSP). O NETI dispõe de uma rede informatizada com aproximadamente 40 servidores e cerca de 20 sistemas em funcionamento, abrangendo virtualmente diversas áreas e setores do hospital, desde gestão de materiais, sistemas de informações de pacientes, agendamento de consultas, medicamentos, imagens médicas, laboratório, até registro de diagnósticos e procedimentos.

Apesar de a organização reconhecer a importância de manter seus dados de forma segura, ainda não existe um trabalho específico na área da gestão de segurança de informação.

3 OBJETIVOS

3.1 Objetivo Geral

O objetivo deste trabalho é estabelecer, documentar e implementar um Sistema de Gestão da Segurança da Informação (SGSI) dentro do Núcleo Especializado em Tecnologia da Informação (NETI) do Hospital das Clínicas da Faculdade de Medicina da Universidade de São Paulo (HCFMUSP).

3.2 Objetivos Específicos

- Propor metodologia para implantação;
- Avaliar o ambiente organizacional; e
- Avaliar o impacto do processo de implantação, através de indicadores selecionados, sobre o ambiente organizacional e o desempenho dos processos.

Como resultado deste trabalho é esperado o fortalecimento e a integração da segurança da informação com os objetivos de negócio da organização, com o uso de linguagem única internacional por meio de padrões da família ISO 27000.

4 MÉTODO

4.1 Seleções das normas

Foi realizado um levantamento e uma avaliação das normas nacionais e internacionais que poderiam ser utilizadas como guia para o Núcleo Especializado em Tecnologia da Informação implantar seu sistema de gestão de segurança da informação. Os critérios para avaliação e seleção das normas foram: aplicabilidade ao escopo do NETI e reconhecimento nacional e internacional. Foram escolhidas, então, as seguintes normas:

- NBR ISO/IEC 27001:2006 – Sistemas de gestão de segurança da informação;
- NBR ISO/IEC 27002:2005 – Código de prática para a gestão da segurança da informação;
- ISO/IEC 27799 – *Information security management in health using ISO/IEC 27002*.

4.2 Estruturação do projeto

A ISO 27001 será o documento base para implantação. Esta norma está alinhada com a ferramenta PDCA utilizada em outros sistemas de gestão, como a ISO 9001, portanto, esta ferramenta foi adotada na estruturação do projeto.

A Figura 6 apresenta a estruturação deste projeto utilizando PDCA. A fase de melhoria, apesar de ser parte integrante da ferramenta PDCA utilizada, não faz parte deste estudo, por isso a menção a estudos futuros. Os números destacados ao final de cada etapa indicam os itens da ISO 27001. Estes itens trazem as orientações do que deve ser realizado.

Figura 6. Ciclo PDCA proposto para o SGSI

4.3 Planejamento

4.3.1 Definição dos indicadores e avaliação de diagnóstico

Optamos pela utilização de dois indicadores, descritos nos itens 4.3.1.1 e 4.3.1.2. As respostas foram organizadas numa base de dados de onde foram extraídas as estatísticas apresentadas na discussão dos resultados.

Utilizou-se o qui-quadrado com correção de Yates ou o teste exato de Fisher para comparar as proporções de adequação/inadequação aos quesitos da norma analisados. As diferenças foram consideradas significantes para $p < 0,05$.

Massad, et al (2004) cita que quando a tabela de contagens observadas tem duas linhas e duas colunas, os totais de linhas e colunas estão fixos e todas as contagens esperadas são maiores ou iguais a 5, recomenda-se o uso da correção de Yates para calcular a estatística χ^2 . Caso pelo menos uma das contagens esperadas seja menor que 5, não se deve usar o teste qui-quadrado porque a distribuição da estatística χ^2 não é bem aproximada pela distribuição qui-quadrado. Nestes casos, deve-se usar o teste exato de Fischer que, apesar de potencialmente mais trabalhoso, calcula a probabilidade exata de observar a diferença em questão, como o próprio nome indica.

Todas as análises foram realizadas utilizando o software estatístico Epi Info (versão 6).

4.3.1.1 ISO/IEC 27001:2006

Foi utilizado o “anexo A” da norma ABNT NBR ISO/IEC 27001:2006, que trata dos objetivos de controle e controles. Os objetivos de controle e controles são derivados diretamente e estão alinhados com aqueles listados na ABNT NBR ISO/IEC 27002:2005 – seções 5 a 15. Este indicador é apresentado de forma resumida no Anexo A desta dissertação.

Na avaliação inicial foi verificado se o controle estava implementado e se o mesmo atendia aos requisitos da norma ABNT NBR ISO/IEC 27002:2005. Para tanto, realizou-se uma reunião de consenso com os integrantes do comitê de segurança para verificar quais controles já estavam sendo utilizados. Cada controle da norma foi classificado de acordo com um dos seguintes critérios: implementado, parcialmente implementado, não implementado ou não se aplica. Como exemplo de controle parcialmente implementado podemos citar o controle “Inventário dos Ativos”, pois a organização não possuía todos os ativos inventariados.

Para checagem do atendimento do controle aos requisitos da norma e classificação de acordo com os critérios previamente estabelecidos (ver Tabela 4), documentos foram solicitados e analisados. Cada controle da norma foi classificado de acordo com um dos seguintes critérios: atende completamente aos requisitos da norma, atende parcialmente aos requisitos da norma, não atende aos requisitos da norma ou não se aplica. Atende parcialmente aos requisitos da norma um controle que não segue todas as orientações da mesma, exceto quando a orientação não se aplica ao estudo

de caso. Os níveis de adequação foram pontuados conforme a tabela 4.

Tabela 4 – Possíveis valores para os controles analisados

Descrição	Pontos
O controle não se aplica	-
Controle não implementado	0
Controle parcialmente implementado	1
Controle implementado, mas sem comprovação ou a comprovação não atende as normas ISO	2
Controle implementado, com comprovação, mas atendendo parcialmente as normas ISO	3
Controle implementado, com comprovação e atendendo as normas ISO	4
Controle implementado, com comprovação, atendendo as normas ISO e sendo este um item obrigatório (27001 ou escopo do projeto)	5

Foi estabelecido que os controles que não se aplicam ao estudo de caso não seriam pontuados e, portanto, não influenciariam nos resultados obtidos. Dos 133 controles existentes na norma apenas três foram desconsiderados. Os controles excluídos fazem parte do item 10.9 da norma que trata de Serviços de Comércio Eletrônico.

Por outro lado, foi atribuído valor máximo para os controles que estavam implementados de acordo com o que a norma estabelece e, que foram considerados obrigatórios por ao menos um dos seguintes motivos:

- a) Análise dos controles com o que a ABNT NBR ISO/IEC 27001:2006 determina fazer.
- b) Análise dos controles com o escopo estabelecido para o projeto.

4.3.1.2 Questionário

Foi elaborado um questionário para avaliar a percepção dos funcionários com segurança da informação e também para checar itens que são exclusivos do escopo do projeto.

O questionário foi elaborado em formato eletrônico e foi testado em outra organização antes de ser preenchido pelos integrantes do NETI. Com este teste foi possível corrigir algumas falhas em perguntas e, com isso, minimizar eventuais dúvidas no preenchimento.

Os funcionários do NETI foram orientados via e-mail sobre como proceder ao preenchimento do questionário. Não foi preciso se identificar e as respostas ficaram anônimas já que o preenchimento foi realizado utilizando usuário e senha comum.

A primeira pergunta do questionário tratava do cargo/função exercida pelo funcionário, as possíveis respostas eram: diretor/gerente, analista, técnico ou outros.

As perguntas de número 2, 3, 4 e 5 avaliavam a percepção do funcionário com a segurança da informação na organização. As demais perguntas, de 6 a 20, tratavam de assuntos relacionados com o escopo do projeto. Para todas estas perguntas as possíveis respostas eram: concordo totalmente, concordo parcialmente, não concordo nem discordo, discordo parcialmente e discordo totalmente.

A figura 7 apresenta a tela de acesso ao questionário, enquanto que as figuras 8 e 9 apresentam o questionário com as perguntas realizadas.

Figura 7. Página de acesso ao questionário

Adicionar questionário | Site de administração do Django - Mozilla Firefox

Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda

https://sistema.nara.org.br/questionario/questionario/add/

Mais visitados Gmail ANSP Webmail USP NARA Lacnic IEEE

Adicionar questionário | Site de admi...

Início > Questionário > Questionários > Adicionar questionário

Adicionar questionário

Prezado(a) colega,

Este questionário faz parte do Sistema de Gestão de Segurança da Informação (SGSI) em desenvolvimento no NETI. Ele foi elaborado para avaliar o ambiente organizacional e visa efetuar melhorias em processos.

As perguntas de número 1, 2, 3, 4 e 5 são de caráter geral. As perguntas de 6 a 20 são específicas do escopo do projeto, que trata das rotinas de backup dos servidores sob responsabilidade do NETI.

Voce não levará mais do que 10 minutos para respondê-lo. Quando não souber ou não tiver opinião, assinale a alternativa **Não concordo nem discordo**. Suas respostas são anônimas. Este questionário ficará ativo até o dia 16/04/2010.

Atenciosamente,

Carlos Eduardo Ribas.

1. Minha função/cargo atual que exerço é de: Técnico

2. Minha função tem ligação direta/indireta com a segurança da informação: Concordo totalmente

3. Conheço o documento que trata da Política de Segurança da Informação adotada pela organização: Discordo totalmente

4. Sou informado quando ocorrem mudanças na Política de Segurança da Informação: Discordo totalmente

5. Segurança da Informação é um item importante para os negócios desenvolvidos na organização: Concordo totalmente

6. Conheço os procedimentos de cópias de segurança adotados pela organização (Ex: frequência de geração, tipo de backup, etc):

7. Atualmente, o método utilizado para a realização de cópias de segurança atende as necessidades da organização: -----

Concluído

Discordo totalmente
Discordo parcialmente
Não concordo nem discordo
Concordo parcialmente
Concordo totalmente

Figura 8. Questionário respondido pelos funcionários do NETI – Parte 1

Adicionar questionário | Site de administração do Django - Mozilla Firefox

Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda

https://sistema.nara.org.br/questionario/questionario/add/

Mais visitados Gmail GMail ANSP Webmail USP NARA Lacnic IEEE IEEE

Adicionar questionário | Site de admi...

8. As cópias de segurança realizadas pela organização contêm informações suficientes para restaurar um sistema de informação a um estado recente, operável, e preciso:

9. A frequência de geração das cópias de segurança reflete os requisitos de negócio:

10. O período de armazenamento das informações esta determinado:

11. As cópias de segurança são armazenadas em ambientes distintos dos sistemas de origem:

12. As cópias de segurança que são mantidas em outros ambientes são protegidas contra acesso não autorizado:

13. São realizados cópias de segurança de dados sensíveis:

14. As cópias de segurança são criptografadas, tanto na execução quanto em seu armazenamento:

15. São mantidos registros precisos e completos das cópias de segurança realizadas:

16. As cópias de segurança são periodicamente testadas para garantir que elas são suficientemente confiáveis para o uso de emergência:

17. Existe um ambiente separado para testar os procedimentos de restauração do sistema:

18. Existe um procedimento escrito e atualizado para a realização das cópias de segurança:

19. Este procedimento escrito contém instruções para tratamento de erros ou outras condições excepcionais:

20. Este procedimento escrito contém dados para contatos de suporte para o caso de eventos operacionais inesperados ou dificuldades técnicas:

Salvar e adicionar outro Salvar e continuar editando Salvar

Concluído

Figura 9. Questionário respondido pelos funcionários do NETI – Parte 2

4.3.2 Criação do Comitê de Segurança

Um Comitê de Segurança foi criado e seus representantes foram escolhidos de diferentes partes da organização, com funções e papéis relevantes. Estes representantes irão acumular as funções que já desempenham com os novos cargos criados dentro do comitê, os novos cargos são:

- Gestor de Segurança da Informação
- Consultor de Segurança
- Analista de Segurança
- Auditor de Sistema de Informação

A organização fornecerá treinamento a todo o pessoal que tem responsabilidades atribuídas no SGSI.

Foi estabelecido em reunião que o comitê se reunirá semanalmente e estará envolvido de maneira direta nos passos iniciais da estruturação do projeto, porém, ao longo do tempo, as reuniões poderão acontecer mensalmente ou bimestralmente, de acordo com a necessidade.

4.3.3 Definição do escopo

Realizou-se uma reunião onde foi explicada a importância do escopo do projeto e, seguindo as orientações de melhores práticas em segurança da informação, a equipe decidiu, então, que o escopo inicial, objeto do presente estudo, irá abranger as rotinas de *backup* da organização, pelos seguintes

motivos:

- É um processo definido e maduro, já que a estruturação de um SGSI não tem como objetivo definir processos de trabalho, mas sim implementar segurança no que já existe.
- É relevante para a organização.
- Representa valor para os diretores e colaboradores.
- Permite implementações, alterações e melhorias.
- É um processo onde a organização possui a gerência sobre os ativos.

4.3.4 Inventário dos Ativos

Realizou-se um levantamento/atualização dos ativos tecnológicos (hardware e software) e não tecnológicos (pessoas, ambientes e processos). Para isso foi criado um organograma que separa o NETI em área, processo e ativo. Baseado nele foi possível identificar todos os ativos envolvidos com o escopo.

Para os ativos tecnológicos o software OCS Inventory NG (*Open Computer and Software Inventory Next Generation*) foi utilizado. Todas as máquinas envolvidas diretamente no escopo do projeto tiveram seus *hardwares* e *softwares* inventariados. Além disso, foi criada uma planilha com as principais informações dos computadores. Outros ativos tecnológicos inventariados foram: equipamentos de rede e mídias.

Para os ativos não tecnológicos, foi elaborado um organograma para representar as relações hierárquicas dentro da organização e todos os

funcionários foram listados dentro de suas respectivas funções. Também foi elaborado um diagrama do *datacenter* do NETI e todos os servidores que fazem parte do escopo foram listados.

4.3.5 Definição de Responsabilidades

Designou-se um proprietário para cada ativo inventariado. Este proprietário tem a responsabilidade autorizada para controlar a produção, o desenvolvimento, a manutenção, o uso e a segurança do ativo.

4.3.6 Elaboração da Política de Segurança

A organização adotou uma estrutura normativa com três níveis hierárquicos, assim relacionados:

- a) Políticas - define a estrutura, as diretrizes e as obrigações referentes à segurança da informação;
- b) Normas - estabelecem obrigações e procedimentos definidos de acordo com as Políticas; e
- c) Procedimentos - instrumentalizam o disposto nas Normas e nas Políticas, permitindo a direta aplicação nas atividades da organização.

A organização utiliza uma política de segurança de âmbito corporativo que foi elaborada pelo Grupo de Segurança e Infra-estrutura Corporativa do Hospital das Clínicas (GSIC-HC). Contudo, uma política interna e específica

para as necessidades do NETI se faz necessária.

Criou-se, então, uma política interna que foi redigida de forma simples, clara e de fácil entendimento para todos os níveis hierárquicos. Ficou decidido que as políticas adotadas pelo NETI seriam:

- Política de Segurança da Informação Corporativa – Regras de alto nível para o uso dos recursos disponíveis na rede corporativa. Este documento norteia a política de segurança dos institutos e fundações pertencentes ao complexo do HCFMUSP para proteção dos seus principais ativos de informação.
- Regulamento Interno de Segurança da Informação – Diretriz interna que tem a finalidade de atribuir legalmente responsabilidades, obrigações, penalidades e direitos, de acordo com a visão estratégica da direção do NETI.

Além destas políticas, haverá também um Termo de Responsabilidade com a Segurança da Informação. Este termo será um instrumento aplicado aos usuários e/ou pessoas contratadas pelo NETI, objetivando formalizar a ciência e o aceite com a Política de Segurança da Informação Corporativa e com o Regulamento Interno de Segurança da Informação.

As políticas foram definidas de acordo com as características do negócio e dos ativos e tecnologias utilizadas, bem como alinhada com o contexto estratégico de gestão de riscos. As políticas foram aprovadas pela direção.

4.3.7 Análise/Avaliação de Riscos

Para fazer a análise dos riscos foram identificados os parâmetros que envolvem o processo das rotinas de backup dos servidores sob responsabilidade do NETI, a saber:

- Ativos considerados no escopo da análise
- Controles a serem investigados
- Probabilidade de exploração
- Consequência da exploração
- Relevância do evento para o negócio

Para a execução desta etapa foi definido o uso do método qualitativo. A Tabela 5 informa a classificação adotada para a definição dos níveis de probabilidade de ocorrência de um determinado evento, severidade das consequências deste evento e a relevância ou impacto do ativo para o negócio:

Tabela 5 – Classificação dos riscos

Níveis	Muito Baixo	Baixo	Médio	Alto	Muito Alto
P - Probabilidade	1	2	3	4	5
C - Consequência	1	2	3	4	5
R – Relevância para o Negócio	1	2	3	4	5

O risco será calculado por meio da fórmula: $RISCO = P \times C \times R$. Como resultado desta classificação, os seguintes níveis de riscos foram

criados (Tabela 6):

Tabela 6 – Níveis de riscos

Nível de Risco	Interpretação	Possíveis Valores (PxRxR)
Muito alto	Riscos inaceitáveis. Os gestores dos ativos devem ser orientados para que os eliminem imediatamente.	60, 64, 75, 80, 100, 125
Alto	Riscos inaceitáveis. Os gestores dos ativos devem ser orientados para pelo menos controlá-los.	32, 36, 40, 45, 48, 50
Médio	Riscos que podem ser aceitáveis após a revisão e confirmação dos gestores dos ativos, contudo a aceitação do risco deve ser feita por meios formais.	18, 20, 24, 25, 27, 30
Baixo	Riscos que podem ser aceitáveis após a revisão e confirmação dos gestores dos ativos.	8, 9, 10, 12, 15, 16
Muito baixo	Riscos aceitáveis. Devem ser informados para os gestores dos ativos.	1, 2, 3, 4, 5, 6

Foi realizado um levantamento dos riscos presentes na organização e, na sequência, a equipe de segurança da informação reuniu-se para avaliar os mesmos. Esta etapa compreende o processo de analisar os riscos que foram previamente identificados e estimá-los com critérios de risco definidos pela organização. Com essa análise, foi decidido se o risco seria tratado ou aceitado.

4.3.8 Definição dos controles

Foram identificados os controles que precisam ser implementados

para que o NETI possua ativos mais seguros. Os controles foram selecionados de acordo com os seguintes critérios:

- a) Resultado da análise/avaliação de riscos
- b) Controles considerados obrigatórios

4.3.9 Plano de tratamento de risco

Foram estabelecidos prioridades, responsabilidades e prazos para o tratamento dos riscos encontrados. O motivo da não implementação ou a descrição das ações que serão tomadas foram descritas. Além disso, foram listados quais controles do “Anexo A” da ISO 27001 devem servir como instrumento de orientação no tratamento do risco. Para os riscos que não serão tratados, ficou decidido que as razões para o não tratamento será documentado e comunicado a todas as partes envolvidas que precisam ter conhecimento a respeito deles.

4.3.10 Declaração de aplicabilidade

Foram estabelecidos quais controles da ISO 27001:2006, com base na letra “j” do requisito 4.2.1 da norma, são aplicáveis ao Sistema de Gestão de Segurança da Informação, as razões para a seleção e as justificativas da não seleção dos controles.

Além disso, foram apresentas as ações ou documentos de referência que comprovam a implementação dos controles selecionados.

4.4 Implantação

4.4.1 Executar o Plano de Tratamento de Risco

O Gestor de Segurança da Informação irá fiscalizar todas as atividades desenvolvidas para que as etapas propostas no Plano de Tratamento de Riscos sejam cumpridas.

4.4.2 Implantação dos controles

Os integrantes do Comitê de Segurança serão responsáveis pelas implantações dos controles seguindo as orientações das normas de referência utilizadas.

4.4.3 Realizar treinamentos e implementar programas de conscientização

Os funcionários serão orientados sobre a importância da segurança da informação independente da função exercida na organização. Isto será realizado por meio de apresentações. Além disso, a intranet da empresa será utilizada para divulgar informações sobre segurança.

Também haverá a apresentação das Políticas de Segurança adotadas. Na ocasião, os funcionários poderão apresentar sugestões de melhorias.

4.4.4 Controle de documentos

Documentos que formalizam o sistema de gestão foram elaborados durante toda a fase de Planejamento do projeto (Tabela 7). O Comitê de Segurança criou alguns documentos considerados obrigatórios por determinação da ISO 27001 e outros considerados obrigatórios porque a própria organização decidiu.

Tabela 7 – Documentos gerados para o SGSI

Etapa da fase de planejamento do ciclo PDCA	Documento Gerado
Criação do Comitê de Segurança	Comitê de Segurança
Definição do escopo	Escopo
Inventário dos ativos	Gestão de Ativos
Definição de responsabilidades	
Elaboração da política do SGSI.	Gestão de Políticas; Regulamento Interno de Segurança da Informação; Termo de Responsabilidade com a Segurança da Informação; Norma de Classificação da Informação; Norma de Utilização do <i>Datacenter</i>
Análise/Avaliação de risco	Gestão de Riscos
Definição dos controles	
Plano de tratamento de risco	
Declaração de aplicabilidade	Declaração de aplicabilidade

Um procedimento documentado foi estabelecido para definir as ações de gestão necessárias para:

- a) Aprovar documentos para adequação antes de sua emissão;
- b) Analisar criticamente e atualizar, quando necessário, e re-aprovar documentos;
- c) Assegurar que as alterações e a situação da revisão atual dos documentos sejam identificadas;

- d) Assegurar que as versões pertinentes de documentos aplicáveis estejam disponíveis nos locais de uso;
- e) Assegurar que os documentos permaneçam legíveis e prontamente identificáveis;
- f) Assegurar que os documentos estejam disponíveis àqueles que deles precisam e sejam transferidos, armazenados e finalmente descartados conforme os procedimentos aplicáveis à sua classificação;
- g) Assegurar que documentos de origem externa sejam identificados;
- h) Assegurar que a distribuição de documentos seja controlada;
- i) Prevenir o uso não intencional de documentos obsoletos; e
- j) Aplicar identificação adequada nos casos em que sejam retidos para qualquer propósito.

4.5 Avaliação

4.5.1 Auditoria interna

Um funcionário foi selecionado e treinado para executar uma auditoria interna. Esta auditoria tem o objetivo de determinar a conformidade do sistema de gestão da organização frente ao padrão internacional, determinar a eficácia e apresentar à organização oportunidades de melhorias no SGSI.

4.5.2 Análise crítica

Foi definido que o diretor e o comitê de segurança da informação realizarão uma reunião ao término da auditoria interna para avaliar os resultados encontrados. Esta reunião visa propor orientações para a

melhoria do sistema e principalmente apresentar conclusões que poderão variar desde a abertura de solicitação de ações corretivas até solicitações de correções ou melhoria em processos ou procedimentos.

4.5.3 Auditoria independente

Uma auditoria externa, feita por uma empresa independente, será utilizada apenas quando a organização se sentir preparada. A direção, com o respaldo do comitê de segurança, decidirá quando será o momento para isto ocorrer. Esta auditoria avalia a existência, adequação e eficácia dos requisitos da norma, avaliando ou não a aderência à referida norma, que pode resultar em um selo de certificação de aderência, renovável em ciclos predeterminados.

4.5.4 Avaliação de diagnóstico

Uma nova avaliação utilizando os mesmos indicadores do início do projeto (itens 4.3.1.1 e 4.3.1.2) será realizada para avaliar os ganhos obtidos com o SGSI.

5 RESULTADOS

5.1 Documentos gerados

Todos os documentos criados para compor o SGSI seguem um mesmo padrão (Anexo B). Eles possuem um cabeçalho para preenchimento de informações como: nome do documento, versão, data de criação, autor e tipo de informação. Além disso, foi criada uma tabela para inserir informações de atualizações realizadas. Esta tabela possui os seguintes campos: versão, data, autor e descrição da atualização. O restante do documento é composto ao menos por: introdução, objetivos e informações relativas ao documento criado.

Os documentos Comitê de Segurança e Escopo são apresentados nos Anexos C e D respectivamente. Entretanto, os nomes dos integrantes do comitê foram omitidos.

Alguns documentos gerados durante o SGSI possuem informações sensíveis e/ou expõem falhas de segurança na organização, por este motivo eles não serão apresentados nesta dissertação. Contudo, apresentaremos alguns dados para representar o que foi criado.

Para a geração do documento Gestão de Ativos, um item que auxiliou na identificação foi um organograma dividindo a organização em área, processo e ativo (Figura 10). Com base neste organograma, foram identificados os ativos que precisariam ser inventariados.

Figura 10. Organograma da organização dividida por área, processo e ativo

O ativo *Datacenter* foi representado com um diagrama (Figura 11). Para os ativos Servidores, Equipamentos de Rede, Mídias e Pessoas foram criados as tabelas 8, 9, 10 e 11 respectivamente. Todas as informações desta tabelas foram omitidas. No ativo Documentação dos Procedimentos de Operação consta o nome do documento gerado: POP – *Backup* de servidores.

Figura 11. Diagrama do *datacenter* do NETI

Tabela 8 – Descrição dos servidores

Rack	Servidor	Descrição	S.O.¹	Apl./B.D.²	Versão	Observação	Discos	RAM³	Processador	Criticidade

¹ Sistema operacional utilizado

² Aplicativo/Banco de dados instalado

³ Total de memória RAM do servidor

Tabela 9 – Descrição dos equipamentos de rede

Quantidade	Descrição	Modelo

Tabela 10 – Descrição das mídias

Quantidade	Descrição	Volumes

Tabela 11 – Informações dos funcionários do NETI

Nome	Cargo	Setor/Seção

O Regulamento Interno de Segurança da Informação é apresentado no Anexo E. O Termo de Responsabilidade com a Segurança da Informação é apresentado no Anexo F. Os demais documentos gerados para compor a política de segurança da organização não serão apresentados nesta dissertação.

A Tabela 12 representa a tabela criada para executar a análise/avaliação de risco. Nela foram descritas as vulnerabilidades encontradas na organização, os possíveis controles contra estas vulnerabilidades, as ameaças relacionadas, além de atribuir níveis para a probabilidade, consequência e relevância para se chegar ao nível de risco.

A Tabela 13 representa a tabela criada para descrever as ações tomadas com cada risco encontrado. Foram descritos se os riscos serão tratados ou não, as razões para a não implementação ou a descrição do que será implementado, os controles da ISO 27001 que podem auxiliar no tratamento do risco, prazos e responsáveis pelo controle. Todas as informações referentes à análise/avaliação de risco foram inseridas em um documento chamado Gestão de Riscos.

A declaração de aplicabilidade é apresentada de forma resumida no Anexo G. Este documento cita quais controles foram implementados e apresenta as razões para a seleção ou as justificativas da não seleção dos controles. Além disso, esta declaração apresenta as ações ou documentos de referência que comprovam a implementação dos controles.

Tabela 12 – Análise/Avaliação de risco

Nr	Vulnerabilidade	Controle	Detalhe do Controle	Ameaças Relacionadas	P¹	C²	R³	Risco (PxCxR)

¹ Valor para a probabilidade de ocorrência de um determinado evento

² Valor para a consequência deste evento

³ Valor para a relevância ou impacto do ativo para o negócio

Tabela 13 – Medidas que serão tomadas para cada risco encontrado

Nr	Controle	Será Imp. ?¹	Motivo da não implementação ou Descrição da implementação	Controles “Anexo A”	Prazo	Resp.²

¹ Decisão se o controle será ou não implementado

² Responsável pela implementação do controle

5.2 Indicadores

5.2.1 ISO/IEC 27001:2006

Utilizando a classificação proposta para este projeto a Tabela 14 apresenta os resultados obtidos no início deste estudo, em agosto de 2009, em comparação com a análise feita em junho de 2010, para a apresentação desta dissertação.

Tabela 14 – Análise estatística da pontuação obtida no início e ao término do projeto

Item	Max	Inic	Fin	X ²	P
Política de Segurança	10	3	10	-	0,001548*
Organizando a Segurança da Informação	48	4	17	8,78	0,0030503
Gestão de Ativos	22	1	16	18,79	0,0000146
Segurança nos Recursos Humanos	39	2	16	12,21	0,0004765
Segurança Física e do Ambiente	58	12	18	1,12	0,2890521
Gerenciamento das Operações e Comunicações	126	23	37	3,7	0,0545145
Controle de Acesso	101	30	37	0,8	0,369906
Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação	64	11	11	0,05	0,8147653
Gestão de Incidentes de Segurança da Informação	21	0	1	-	0,5*
Gestão de Continuidade de Negócios	20	0	3	-	0,1153846*
Conformidade	41	0	4	-	0,0578997*
Total	550	86	170	35,07	<0,00000001

* Teste exato de Fischer

Max = valor máximo do item, Inic = valor inicial encontrado no item, Fin = valor final encontrado no item, χ^2 = valor do qui-quadrado, P = nível de significância

Na análise inicial a organização obteve 86 dos 550 pontos possíveis,

ou seja, 15,6% de conformidade com a norma de referência utilizada. Na análise final a pontuação passou de 86 para 170 pontos. Este valor equivale a 30,9% de conformidade com a norma. Note que houve diferença estatística nos itens: política de segurança, organizando a segurança da informação, gestão de ativos e segurança nos recursos humanos. Além disso, também houve diferença estatística na avaliação geral.

A Tabela 15 demonstra a análise estatística (qui-quadrado) entre a análise inicial e a análise final nos controles implementados.

Tabela 15 – Análise estatística dos controles implementados

Item	Max	Inic	Fin	X²	P
Política de Segurança	2	1	2	-	0,5*
Organizando a Segurança da Informação	11	2	4	-	0,3175586*
Gestão de Ativos	5	0	4	-	0,0238095*
Segurança nos Recursos Humanos	9	1	5	-	0,0656109*
Segurança Física e do Ambiente	13	5	6	0	1,0
Gerenciamento das Operações e Comunicações	29	11	16	1,11	0,2923600
Controle de Acesso	25	12	15	0,32	0,5703716
Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação	16	5	5	0,15	0,7029176
Gestão de Incidentes de Segurança da Informação	5	0	0	-	-**
Gestão de Continuidade de Negócios	5	0	1	-	0,5*
Conformidade	10	0	1	-	0,5*
Total	130	37	59	7,28	0,0069619

* Teste exato de Fischer

** Não é possível realizar estatística quando o total da coluna ou da linha é nulo

Max = total de controles no item, Inic = quantidade de controles implementados na análise inicial, Fin = quantidade de controles implementados na análise final, χ^2 = valor do qui-quadrado, P = nível de significância

No início eram 37 (28,4%) controles em uso, no final este número passou para 59 (45,3%). Note que houve diferença estatística no item gestão de ativos e na avaliação geral.

A Tabela 16 demonstra a análise estatística (qui-quadrado) entre a análise inicial e a análise final nos controles parcialmente implementados.

Tabela 16 – Análise estatística dos controles parcialmente implementados

Item	Max	Inic	Fin	χ^2	P
Política de Segurança	2	0	0	-	-
Organizando a Segurança da Informação	11	0	1	-	0,5*
Gestão de Ativos	5	1	0	-	0,5*
Segurança nos Recursos Humanos	9	0	0	-	-
Segurança Física e do Ambiente	13	2	3	-	0,5*
Gerenciamento das Operações e Comunicações	29	1	0	-	0,5*
Controle de Acesso	25	4	2	-	0,3335504*
Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação	16	1	1	-	0,7580645*
Gestão de Incidentes de Segurança da Informação	5	0	1	-	0,5*
Gestão de Continuidade de Negócios	5	0	0	-	-
Conformidade	10	0	1	-	0,5*
Total	130	9	9	0,06	0,8069901

* Teste exato de Fischer

Max = total de controles no item, Inic = quantidade de controles parcialmente implementados na análise inicial, Fin = quantidade de controles parcialmente implementados na análise final, χ^2 = valor do qui-quadrado, P = nível de significância

Estatisticamente não houve diferença. Contudo, apesar do número total nas duas avaliações permanecer o mesmo, ou seja, 9 controles (6,9% do total), houve mudanças em quais controles foram considerados

parcialmente implementados. Enquanto alguns controles foram finalizados, outros começaram a ser utilizados.

A Tabela 17 demonstra a análise estatística (qui-quadrado) entre a análise inicial e a análise final nos controles não implementados.

Tabela 17 – Análise estatística dos controles não implementados

Item	Max	Inic	Fin	χ^2	P
Política de Segurança	2	1	0	-	0,5*
Organizando a Segurança da Informação	11	9	6	-	0,1807276*
Gestão de Ativos	5	4	1	-	0,1031746*
Segurança nos Recursos Humanos	9	8	4	-	0,0656109*
Segurança Física e do Ambiente	13	6	4	0,16	0,6868652
Gerenciamento das Operações e Comunicações	29	17	13	0,62	0,4305169
Controle de Acesso	25	9	8	0	1,0
Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação	16	10	10	0,13	0,7150007
Gestão de Incidentes de Segurança da Informação	5	5	4	-	0,5*
Gestão de Continuidade de Negócios	5	5	4	-	0,5*
Conformidade	10	10	8	-	0,2368421
Total	130	84	62	6,89	0,0086729

* Teste exato de Fischer

Max = total de controles no item, Inic = quantidade de controles não implementados na análise inicial, Fin = quantidade de controles não implementados na análise final, χ^2 = valor do qui-quadrado, P = nível de significância

Note que houve diferença estatística na avaliação geral. No início eram 84 (64,6%) controles sem nenhuma implementação, ao término esse número caiu para 62 (47,6%).

A Tabela 18 demonstra a análise estatística (qui-quadrado) entre a análise inicial e a análise final nos controles considerados obrigatórios.

Tabela 18 – Análise estatística dos controles obrigatórios

Controles obrigatórios	Tot	Inic	Fin	χ^2	P
Implementados	30	5	19	11,74	0,0006130
Parcialmente Implementados		5	6	0,0	1,0
Não Implementados		20	5	13,44	0,0002463

Tot = quantidade de controles obrigatórios, Inic = valor inicial encontrado, Fin = valor final encontrado, χ^2 = valor do qui-quadrado, P = nível de significância

Note que houve diferença estatística nos controles implementados e nos controles não implementados. O total de controles implementados passou de 5 (16,6%) para 19 (63,3%), controles parcialmente implementados passaram de 5 (16,6%) para 6 (20%), enquanto que os controles não implementados caíram de 20 (66,6%) para 5 (16,6%) (Figura 12).

Figura 12. Análise dos controles obrigatórios

5.2.2 Questionário

Na análise inicial 18 (72%) pessoas responderam ao questionário, enquanto que na análise final ele foi respondido por 15 funcionários (60%). A Tabela 19 apresenta os cargos ocupados pelas pessoas que responderam ao questionário.

Tabela 19 – Número de pessoas que responderam ao questionário

Cargo	Análise inicial	Análise final
Gerente/Diretor	2	1
Analista	6	6
Técnico	7	7
Outros cargos	3	1
Total	18	15

A Tabela 20 apresenta os resultados obtidos com o questionário. Para as perguntas de números 2 a 6 todas as respostas foram consideradas. Para as demais perguntas, direcionadas ao escopo do projeto, analisamos os resultados de quem afirmou conhecer totalmente os procedimentos de cópias de segurança adotados pela organização. Na análise inicial 10 (55,5%) pessoas afirmaram conhecer totalmente os procedimentos de cópias de segurança, enquanto que na análise final 9 (60%) pessoas afirmaram conhecer.

Tabela 20 – Análise estatística do questionário

Qst	Conc totalmente			Conc parcialmente			Não conc nem disc			Disc parcialmente			Disc totalmente		
	Inic	Fin	P	Inic	Fin	P	Inic	Fin	P	Inic	Fin	P	Inic	Fin	P
2	77%	93%	0,229	17%	7%	0,373	0%	0%	-	0%	0%	-	6%	0%	0,545
3	28%	46%	0,447	33%	27%	0,488	11%	20%	0,409	11%	7%	0,570	17%	0%	0,149
4	28%	40%	0,710	32%	46%	0,672	6%	7%	0,710	17%	7%	0,373	17%	0%	0,149
5	94%	100%	0,545	6%	0%	0,545	0%	0%	-	0%	0%	-	0%	0%	-
6	55%	59%	0,923	16%	20%	0,577	6%	7%	0,710	6%	7%	0,710	17%	7%	0,373
7	50%	45%	0,585	50%	45%	0,585	0%	10%	0,473	0%	0%	-	0%	0%	-
8	70%	78%	0,555	30%	0%	0,123	0%	22%	0,210	0%	0%	-	0%	0%	-
9	90%	78%	0,458	10%	11%	0,736	0%	11%	0,473	0%	0%	-	0%	0%	-
10	90%	78%	0,458	10%	22%	0,458	0%	0%	-	0%	0%	-	0%	0%	-
11	30%	45%	0,429	40%	22%	0,369	20%	0%	0,263	0%	0%	-	10%	33%	0,249
12	40%	33%	0,570	30%	22%	0,555	20%	0%	0,263	0%	0%	-	10%	45%	0,119
13	50%	78%	0,219	20%	11%	0,541	20%	0%	0,263	0%	11%	0,473	10%	0%	0,526
14	0%	22%	0,210	30%	34%	0,630	40%	11%	0,184	10%	0%	0,526	20%	33%	0,444
15	60%	56%	0,605	30%	44%	0,429	10%	0%	0,526	0%	0%	-	0%	0%	-
16	0%	22%	0,210	30%	22%	0,555	30%	34%	0,630	20%	11%	0,541	20%	11%	0,541
17	0%	23%	0,210	10%	22%	0,458	30%	11%	0,332	10%	22%	0,458	50%	22%	0,219
18	60%	67%	0,570	40%	22%	0,369	0%	11%	0,473	0%	0%	-	0%	0%	-
19	20%	22%	0,667	40%	45%	0,605	20%	33%	0,444	0%	0%	-	20%	0%	0,263
20	40%	67%	0,242	40%	22%	0,369	20%	11%	0,541	0%	0%	-	0%	0%	-

Qst = número da questão, Conc totalmente = concordo totalmente, Conc parcialmente = concordo parcialmente, Não conc nem disc = não concordo nem discordo, Disc parcialmente = discordo parcialmente, Disc totalmente = discordo totalmente, Inic = porcentagem inicial encontrada, Fin = porcentagem final encontrada, P = nível de significância.

Note que não houve diferença estatística entre as respostas nas duas avaliações. Contudo, o resultado da análise inicial do questionário mostrou alguns dados importantes. Vejamos alguns:

A maioria dos funcionários (77%) considera ter alguma responsabilidade com a segurança da informação (Figura 13). Na análise final o percentual passou para 93%.

Figura 13. Segunda questão do questionário: Minha função tem ligação direta/indireta com a segurança da informação

Um ponto crítico encontrado pelo questionário foi a do pouco conhecimento da política de segurança da informação utilizada pela organização (Figura 14). O resultado mostrou a necessidade de treinamento dos funcionários.

Figura 14. Terceira questão do questionário: Conheço o documento que trata da Política de Segurança da Informação adotada pela organização

A Figura 15 apresenta os dados referentes à divulgação ou não de mudanças na política de segurança.

Figura 15. Quarta questão do questionário: Sou informado quando ocorrem mudanças na Política de Segurança da Informação

Um dado satisfatório é que 94% dos funcionários concordam que a segurança da informação é um quesito importante para a organização (Figura 16). Na análise final o número passou para 100% dos funcionários.

Figura 16. Quinta questão do questionário: Segurança da Informação é um item importante para os negócios desenvolvidos na organização

O questionário também mostrou alguns pontos críticos nos itens relacionados ao escopo do projeto. A Figura 17 mostra que apenas 30% das pessoas concordam totalmente que as cópias de segurança são armazenadas em ambientes distintos dos sistemas de origem.

Figura 17. Décima primeira questão do questionário: As cópias de segurança são armazenadas em ambientes distintos dos sistemas de origem

A Figura 18 mostra que a criptografia é pouco utilizada nas rotinas de cópias de segurança.

Figura 18. Décima quarta questão do questionário: As cópias de segurança são criptografadas, tanto na execução quanto em seu armazenamento

Ninguém concordou totalmente e apenas 30% concordaram parcialmente com a questão 16 do questionário (Figura 19).

Figura 19. Décima sexta questão do questionário: As cópias de segurança são periodicamente testadas para garantir que elas são suficientemente confiáveis para o uso de emergência

A Figura 20 mostrou um ponto crítico. 50% das pessoas discordaram totalmente com a afirmativa da questão 17 do questionário.

Figura 20. Décima sétima questão do questionário: Existe um ambiente separado para testar os procedimentos de restauração do sistema

Todos os pontos críticos levantados pelo questionário foram analisados e as possíveis ações e correções foram listadas em um documento chamado gestão de riscos.

6 DISCUSSÃO

Dey (2007) ressalta que as etapas de execução de um SGSI podem variar de empresa para empresa. O autor cita os passos para uma organização estabelecer um SGSI partindo do princípio que o projeto irá começar do zero e que a organização deseja obter a certificação de segurança da ISO. Segundo o autor, os passos para a implementação de um SGSI são:

- a) Formar uma equipe técnica de segurança de informação;
- b) Definir um comitê executivo para o projeto de segurança da informação;
- c) Definir uma equipe de implementação de segurança;
- d) Treinar a equipe de implementação com as mais recentes normas;
- e) Realizar uma análise detalhada dos riscos e vulnerabilidades associados aos ativos de informação;
- f) Para cada ativo a ser protegido, identificar medidas extras de segurança;
- g) Preparar uma proposta de projeto com plano de implementação juntamente com as necessidades de recursos incluindo hardware, software, treinamento, recursos humanos e compromissos. Apresentar a proposta do projeto ao comitê executivo para aprovação;
- h) Escrever os documentos "políticas" e "procedimentos" abrangendo

todas as áreas pertinentes;

- i) Apresentar as políticas e procedimentos (ou um documento único combinado) para o Comitê Executivo para aprovação final;
- j) Implementar o projeto em fases, de acordo com as prioridades. As fases devem ter sido definidas anteriormente no plano de execução;
- k) Junto com outras normas, adotar algumas das melhores práticas como ITIL, COBIT ou outras;
- l) Organizar as ações de sensibilização dos funcionários para fazê-los compreender as políticas e procedimentos de segurança. Garantir que as políticas e procedimentos sejam distribuídos por toda a organização;
- m) Estabelecer procedimentos periódicos para checar vulnerabilidades em segurança e realizar testes de penetração em áreas sensíveis. Rever, avaliar e aperfeiçoar o SGSI seguindo o ciclo PDCA; e
- n) Realizar auditorias no SGSI com auditores competentes.

As etapas propostas pelo autor podem ser utilizadas em qualquer organização, mas o autor não contempla duas importantes etapas na elaboração do SGSI. A primeira é a definição do escopo do projeto. É com base no escopo que todas as demais etapas devem ser elaboradas. A segunda é a elaboração da declaração de aplicabilidade. Este documento é um item obrigatório na implantação de um SGSI, sem ele a organização não obtém a certificação.

Ku, Chang e Yen (2009) relatam que a experiência com a implementação de outras normas, como a ISO 9001, auxilia no desenvolvimento de um SGSI.

Na organização que analisamos nenhuma ISO é utilizada, portanto os funcionários não possuíam nenhuma experiência. Outro ponto a ser considerado em nosso estudo de caso é que até o momento da segunda avaliação, ocorrida em junho de 2010, nenhum funcionário havia recebido o treinamento necessário na norma de referência utilizada. A previsão é de que os funcionários integrantes do comitê de segurança da informação recebam o treinamento no segundo semestre de 2010.

Karabacak e Sogukpinar (2006) propõem um método de pesquisa quantitativa para avaliar o nível de conformidade com a ISO 17799. O método é construído sobre o modelo de risco ISRAM (Information Security Risk Analysis Method) (Karabacak e Sogukpinar, 2005). O ISRAM é uma ferramenta de análise quantitativa que utiliza operações matemáticas básicas. Ele converte as perguntas e as opções de resposta em números e faz os cálculos necessários para expressar o risco. O número de perguntas é limitado pelo número de controles da norma, ou seja, 133.

Os autores criaram pesos para os controles e também para as possíveis respostas. Estes pesos podem ser alterados de acordo com a organização que utilizá-la. Eles variam de 1 a 3 para as perguntas e de 0 a 4 para as respostas.

A eficácia do método proposto depende exclusivamente da atribuição correta dos pesos, da verificação de quais controles serão analisados e,

obviamente, das respostas corretas dos funcionários. O ponto negativo é que o questionário pode ficar muito extenso e cansativo para ser respondido.

No nosso estudo a análise estatística da pontuação da organização mostrou que não houve melhoras significativas em alguns itens da norma. Para o item Segurança Física e do Ambiente a organização aguarda a realização de uma licitação para que os controles identificados na redução dos riscos sejam aplicados. Para o item Gerenciamento das Operações e Comunicações os controles ainda estão sendo aplicados na organização. Para os demais itens da norma (Controle de Acesso; Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação; Gestão de Incidentes de Segurança da Informação; Gestão de Continuidade de Negócios e Conformidade) o resultado já era esperado, pois a prioridade de implantação foi dada aos controles obrigatórios e, todos estes itens somados possuíam apenas 10% do número total de controles obrigatórios.

A análise estatística do questionário mostrou que não houve melhoras significativas em nenhuma questão. Para as primeiras perguntas do questionário, que tratam de como os funcionários enxergam a segurança da informação, ainda esta sendo realizado um trabalho de conscientização por meio de palestras. Para as demais perguntas que tratam das rotinas de cópias de segurança o resultado já era esperado, uma vez que a organização ainda não implementou os controles necessários em virtude dos custos relacionados. Como se trata de uma organização pública, o processo de compra envolve uma série de medidas que acabam levando muito tempo para serem concretizadas.

Além destes motivos existe também o fato do N ser baixo. Na análise inicial foram 18 questionários respondidos, contra 15 da análise final. A organização possui poucos funcionários e, além disso, houve certa dificuldade em fazer com que as pessoas respondessem ao questionário.

Para finalizar, este estudo mostrou ser viável a implantação de um SGSI em uma organização pública de saúde, porém houve uma limitação no alcance dos resultados obtidos em função da não alocação de recursos específicos para o projeto.

7 CONCLUSÕES

Neste estudo foi avaliado a implantação de um sistema de gestão de segurança da informação em uma organização da área da saúde. Ao término do projeto foi possível concluir que:

- a) A implantação de um SGSI é perfeitamente possível em organizações da área da saúde e traz diversos benefícios, como a redução dos riscos associados por meio de controles adequados;
- b) O método proposto para avaliar a organização utilizando o “anexo A” da norma ISO 27001 foi eficiente, uma vez que apontou os controles que precisavam ser priorizados;
- c) A organização obteve melhoras significativas no nível de conformidade com a norma de referência; e
- d) O questionário utilizado para avaliar a organização indicou alguns pontos a serem melhorados, embora estatisticamente não tenha apontado melhoras significativas.

8 ANEXOS

Anexo A – Amostra da planilha gerada com base nos controles do “Anexo A” da ISO 27001

ABNT NBR ISO/IEC 27001:2006 (Anexo A)			Controles implementados ²				Atende aos requisitos da norma ³				Requisito obrigatório ⁴		Obs. ⁵	Pontuação ⁶	
Item	Nr ¹	Controle	Sim	Par	Não	N/A	Sim	Par	Não	N/A	27001	SGSI	---	Máx	Atual
Política de Segurança	5.1	Política de segurança da informação													
	5.1.1	Documento da política de segurança da informação													
	5.1.2	Análise crítica da política de segurança da informação													

¹ Número do controle

² Análise dos controles em utilização. “Sim” representa que o controle está implementado, “Par” representa que o controle está parcialmente implementado, “Não” representa que o controle não está implementado e “N/A” representa que o controle não se aplica ao estudo de caso.

³ Análise do atendimento do controle com a norma de referência. “Sim” representa que o controle atende aos requisitos da norma, “Par” representa que o controle atende parcialmente aos requisitos da norma, “Não” representa que o controle não atende aos requisitos da norma e “N/A” representa que o controle não se aplica ao estudo de caso.

⁴ Controles considerados obrigatórios pela ISO 27001 ou pelo escopo escolhido para o projeto.

⁵ Campo para observações. Foi utilizado para indicar os itens da norma que cobram a implementação do controle.

⁶ Pontuação máxima e pontuação obtida no momento da avaliação.

Anexo B – Padrão de documento criado para o SGSI

SGSI - Sistema de Gestão de Segurança da Informação	
Nome do documento	Exemplo de documento
Versão	1.0
Data de criação	27/08/2009
Autor	Carlos Eduardo Ribas
Informação	Pública

Histórico do documento

Versão	Data	Autor	Descrição da atualização
1.0	28/08/2009	Carlos E. Ribas	Aprovação do documento

1. Introdução

Este é um modelo de documento utilizado no SGSI.

2. Objetivos

Padronizar os documentos gerados com as informações necessárias para o SGSI segundo a ISO 27001.

3. Descrição

...

Aprovado por:

Gestor de Segurança da Informação

Anexo C – Comitê de segurança da informação

SGSI - Sistema de Gestão de Segurança da Informação	
Nome do documento	Comitê de Segurança da Informação
Versão	1.0
Data de criação	03/09/2009
Autor	Carlos Eduardo Ribas
Informação	Interna

Histórico do documento

Versão	Data	Autor	Descrição da atualização
1.0	04/09/2009	Carlos E. Ribas	Aprovação do documento

1. Introdução

A atribuição de papéis e responsabilidades pela segurança da informação é um item obrigatório em um SGSI. No início do projeto é importante indicar os representantes que irão conduzir as ações e decisões relativas à segurança da informação da organização.

2. Objetivos

Criar um Comitê de Segurança da Informação para coordenar as atividades do Sistema de Gestão de Segurança da Informação.

2. O Comitê de Segurança da Informação

Os representantes escolhidos para compor o Comitê de Segurança da Informação são de diferentes partes da organização, com funções e papéis relevantes. Estes representantes irão acumular as funções que já desempenham com os novos cargos criados. Os novos cargos e seus representantes são:

“continua”

Anexo C – “Conclusão”. Comitê de segurança da informação

Cargo	Nome
Gestor de Segurança da Informação	xxx
Consultor de Segurança	xxx
Auditor de Sistema de Informação	xxx
Analista de Segurança	xxx
	xxx
	xxx
	xxx
	xxx

Aprovado por:

Diretor do NETI

Anexo D – Escopo do SGSI

SGSI - Sistema de Gestão de Segurança da Informação	
Nome do documento	Escopo
Versão	1.1
Data de criação	10/09/2009
Autor	Carlos Eduardo Ribas
Informação	Pública

Histórico do documento

Versão	Data	Autor	Descrição da atualização
1.0	11/09/2009	Carlos E. Ribas	Aprovação do documento
1.1	17/05/2010	Carlos E. Ribas	Conformidade com a declaração de aplicabilidade

1. Introdução

O escopo é o perímetro de abrangência que define os ativos que serão contemplados no SGSI, sejam eles sistemas, equipamentos, processos, etc.

2. Objetivos

Definir o escopo e os limites do SGSI nos termos das características de negócio do NETI.

3. Escopo

O Sistema de Gestão de Segurança da Informação aplica-se ao processo das rotinas de *backup*. Ele abrange os sistemas utilizados pelo Hospital das Clínicas que estão armazenados nos servidores sob responsabilidade do NETI, de acordo com a Declaração de Aplicabilidade, versão 1.0, datada de 17/05/2010.

“continua”

Anexo D – “Conclusão”. Escopo do SGSI

Aprovado por:

Diretor do NETI

Gestor de Segurança da Informação

Anexo E – Regulamento Interno de Segurança da Informação

SGSI - Sistema de Gestão de Segurança da Informação	
Nome do documento	Regulamento Interno de Segurança da Informação – RISI
Versão	1.0
Data de criação	05/10/2009
Autor	Carlos Ribas
Informação	Pública

Histórico do documento

Versão	Data	Autor	Descrição da atualização
1.0	25/05/2010	Carlos Ribas	Aprovação do regulamento

1. Introdução

A informação é principal ativo do NETI, afinal, ela é de extrema importância para o desenvolvimento das atividades realizadas pelo Hospital das Clínicas da Faculdade de Medicina da Universidade de São Paulo (HCFMUSP).

A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas.

Assim, para protegermos este ativo, a segurança da informação deve atender a três elementos:

- *Confidencialidade*: garantir que apenas as pessoas devidamente autorizadas tenham acesso à informação.
- *Integridade*: proteger as informações contra alterações em seu estado original. Estas alterações podem ser tanto intencionais quanto acidentais.
- *Disponibilidade*: garantir que uma informação esteja acessível sempre que necessário.

“continua”

Anexo E – “Continuação”. Regulamento Interno de Segurança da Informação

2. Objetivos

O Regulamento Interno de Segurança da Informação (RISI) é uma declaração formal da organização acerca de seu compromisso com a proteção das informações, sejam elas de sua propriedade e/ou sob sua guarda, e tem por finalidade atribuir responsabilidades, obrigações, definir direitos, deveres, expectativas de acesso e uso, e, criar uma cultura educativa de proteção aos dados. Este regulamento aplica-se a todos os funcionários, parceiros e terceiros que utilizem o ambiente do NETI ou que tenham acesso às informações pertencentes a esta organização.

3. Referências utilizadas

O RISI foi elaborado de acordo com as normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27799 e sua implementação, seguindo as orientações destes padrões internacionais, assegura um nível de segurança que é apropriada para as organizações que armazenam informações da área da saúde.

4. Responsabilidades

Da direção:

- a) Aprovar este regulamento e suas revisões;
- b) Tomar as decisões administrativas referentes aos casos de descumprimento deste Regulamento e/ou da Política de Segurança da Informação Corporativa.

“continua”

Anexo E – “Continuação”. Regulamento Interno de Segurança da Informação

Dos funcionários, parceiros e terceiros:

- a) Cumprir e fazer cumprir a política, o regulamento, as normas e os procedimentos de segurança da informação;
- b) Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;
- c) Assinar o Termo de Responsabilidade com a Segurança da Informação, formalizando a ciência e o aceite com este regulamento e com a Política de Segurança da Informação Corporativa, bem como assumindo responsabilidade por seu cumprimento;
- d) Proteger as informações sob sua responsabilidade contra acesso, modificação, destruição ou divulgação não-autorizados.

Do Comitê de Segurança da Informação:

- a) Propor ajustes, aprimoramentos e modificações deste Regulamento;
- b) Propor projetos e iniciativas relacionados à melhoria da segurança da informação.

Qualquer dúvida, orientação, sugestão ou situação que viole o presente documento deverá ser reportada ao Comitê de Segurança, por meio da seguinte conta: sgsi@hcnet.usp.br.

5. Classificação da Informação

As informações devem ser inventariadas e classificadas de acordo com seu grau de confidencialidade. Isto deve ser realizado com base na Norma de Classificação de Informações estabelecida pelo NETI.

“continua”

Anexo E – “Continuação”. Regulamento Interno de Segurança da Informação

6. Procedimentos de segurança

As regras aqui descritas não constituem uma relação exaustiva e podem ser atualizadas com o tempo, sendo que qualquer modificação será avisada em tempo hábil para remodelação (se necessário) do ambiente.

6.1 Segurança física

- a) Como primeiro nível de segurança de acesso físico as dependências do NETI, faz-se uso de um dispositivo de identificação biométrica por digital. Todos os funcionários da organização devem ser cadastrados neste dispositivo. Esta condição é também estendida a todos os parceiros. Para terceiros, esta regra é aplicada apenas quando a organização julgar necessária. Caso contrário, o acesso de terceiros as dependências do NETI será autorizado apenas mediante identificação na recepção e em horário comercial.
- b) Os funcionários e parceiros têm acesso físico liberado somente aos locais necessários ao desempenho de suas atividades e em conformidade com os interesses do NETI.
- c) Todos os funcionários, parceiros e terceiros, devem utilizar alguma forma visível de identificação.
- d) O NETI se reserva no direito de monitorar suas dependências por meio de câmeras, sendo tais imagens armazenadas e de uso exclusivo da organização.

6.2 Comportamento Seguro

- a) Funcionários, parceiros e terceiros devem assumir atitude pró-ativa e engajada no que diz respeito à proteção das informações da Organização.

“continua”

Anexo E – “Conclusão”. Regulamento Interno de Segurança da Informação

- b) Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas, tais como: aviões, restaurantes, encontros sociais, etc.

7.0 Violações

O não cumprimento das regras definidas nessa política implicará em penalidades definidas pela administração do Hospital. De acordo com a Ordem Conjunta de serviço nº06/98.

8.0 Termos e Definições

- Parceiro: Empresa ou pessoa não pertencente ao quadro funcional com aproximação profissional sem ônus para o NETI.
- Terceiro: Pessoa não pertencente ao quadro funcional do NETI alocada para prestação interna de serviço.

Anexo F – Termo de Responsabilidade com a Segurança da Informação

SGSI - Sistema de Gestão de Segurança da Informação	
Nome do documento	Termo de Responsabilidade com a Segurança da Informação
Versão	1.0
Data de criação	05/10/2009
Autor	Carlos Eduardo Ribas
Informação	Pública

1. Introdução

O Termo de Responsabilidade com a Segurança da Informação é um instrumento que formaliza a ciência e o aceite das políticas de segurança da informação.

2. Objetivo

Assegurar o conhecimento das políticas de segurança adotadas pelo NETI.

3. Termo de Responsabilidade com a Segurança da Informação

Declaro, nesta data, ter ciência e estar de acordo com as políticas de segurança adotadas pelo NETI, a saber:

- a) Política de Segurança da Informação Corporativa
- b) Regulamento Interno de Segurança da Informação

Assumo o compromisso de respeitá-los e cumpri-los plena e integralmente.

“continua”

Anexo F – “Conclusão”. Termo de Responsabilidade com a Segurança da Informação

São Paulo, ____ de _____ de _____

Nome:

RG:

Anexo G – Declaração de aplicabilidade

ABNT NBR ISO/IEC 27001:2006 (Anexo A)			Seleção Sim/Não	Razões para Seleção			Justificativas / Documentos comprobatórios
Item	Número	Controle		ENR ¹	EN/MP ²	RAAR ³	
Política de Segurança	5,1	Política de segurança da informação					
	5.1.1	Documento da política de segurança da informação	Sim	X			Ref. RISI
	5.1.2	Análise crítica da política de segurança da informação	Sim	X			Ref. Gestão de Políticas
Organizando a Segurança da Informação	6,1	Organização interna					
	6.1.1	Comprometimento da direção com a segurança da informação	Sim	X			Ref. Carta do Diretor
	6.1.2	Coordenação da segurança da informação	Sim	X			Ref. Comitê de Segurança
	6.1.3	Atribuição de responsabilidades para a segurança da informação	Não				Será criado no próximo ciclo PDCA
	6.1.4	Processo de autorização para os recursos de processamento da informação	Não				Não faz parte do escopo do projeto
	6.1.5	Acordos de confidencialidade	Não				Será criado no próximo ciclo PDCA
	6.1.6	Contato com autoridades	Não				Não faz parte do escopo do projeto
	6.1.7	Contato com grupos especiais	Não				Não faz parte do escopo do projeto
	6.1.8	Análise crítica independente de segurança da informação	Sim	X			Etapa ainda não contemplada pelo SGSI

¹ Exigências da norma de referência

² Exigências de negócio/melhores práticas

³ Resultado da análise/avaliação de risco

9 REFERÊNCIAS

ABNT ISO/IEC Guia 73:2005 – Gestão de riscos – Vocabulário – Recomendações para uso em normas.

ABNT NBR ISO/IEC 27001:2006 Sistemas de Gestão de Segurança da Informação - Requisitos. 2006.

ABNT NBR ISO/IEC 27002 – Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação. 2005.

Ahmad R, Samy GN, Ibrahim NK, Bath PA, Ismail Z. Threats identification in healthcare information systems using genetic algorithm and cox regression. In: IAS 09 - Fifth International Conference on Information Assurance and Security. 2009. p. 757-60.

Al-Hammadi Y, Aickelin U. Detecting bots based on keylogging activities. In: ARES 08 - Third International Conference on Availability, Reliability and Security. 2008. p. 896-902

Alsagoff SN. Malware self protection mechanism. In: ITSim 2008 - International Symposium on Information Technology. 2008. p.1-8.

Andrade FF. O método de melhorias PDCA [dissertação]. São Paulo: Escola Politécnica, Universidade de São Paulo; 2003.

Ayotollahi H, Bath PA, Goodacre S. Paper-based versus computer-based records in the Emergency Department: Staff preferences, expectations, and concerns. In: ISHIMR 2008 - The Thirteenth International Symposium for Health Information Management Research. 2008. p. 159-69.

Bernard, R. Information Lifecycle Security Risk Assessment: A tool for closing security gaps. Computers & Security. 2007;26(1):26-30.

Brechlerova D, Candik M. New trends in security of electronic health documentation. In: ICCST 2008 - 42nd Annual IEEE International Carnahan Conference on Security Technology. 2008. p. 13-16.

Chen J, Guo C. Online detection and prevention of phishing attacks. In: ChinaCom 06 - First International Conference on Communications and Networking in China. 2006. p.1-7.

Collen MF. A history of medical informatics in the United States, 1950 to 1990. J Am Med Inform Assoc. 1995. p.489.

Dey M. Information security management - a practical approach. In: Africon 2007 - 8th IEEE Africon Conference. 2007. p. 1-6.

Deming WE. Qualidade: a revolução da administração. São Paulo: Marques Saraiva, 1990.

Duan H, Wu J. Security Management for Large Computer Networks. In: APCC/OECC'99 - Fifth Asia-Pacific Conference on Communications and Fourth Optoelectronics and Communications Conference. 1999. p.1208-13.

Fenz S, Goluch G, Ekelhart A, Riedl B, Weippl E. Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard. In: PRDC 2007 - 13th Pacific Rim International Symposium on Dependable Computing. 2007. p. 381 – 8.

Harrington JL. Network security. A practical approach. San Francisco. Elsevier. 2005.

Huber M, Sunyaev A, Krcmar H. Security analysis of the health care telematics infrastructure in Germany. In ICEIS 2008 - Proceedings of the Tenth International Conference on Enterprise Information Systems. 2008. p. 144-53.

Humphreys E. Information security management standards: Compliance, governance and risk management. Information Security Technical Report. 2008; 13(4):247-55.

Iso27001certificates [online]. Acessado em 23/06/2010. Disponível em: www.iso27001certificates.com.

Iso27001security [online]. Acessado em 21/06/2010. Disponível em: www.iso27001security.com/html/27001.html.

ISO/IEC 13335-1:2004 - Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management.

ISO/IEC 27799 – Health informatics – Information security management in health using ISO/IEC 27002. 2008.

Irani D, Webb S, Giffin J, Pu C. Evolutionary study of phishing. In: eCrime Researchers Summit. 2008. p.1-10.

Kamel M, Benzekri A, Barrere F, Laborde R. Evaluating the conformity of an access control architecture for Virtual Organizations with ISO/IEC 17799. In: GIIS 2007 - Global Information Infrastructure Symposium. 2007. p.173-80.

Karabacak B, Sogukpinar I. ISRAM: Information security risk analysis method. J Comput Secur. 2005; 24(2):147–59.

Karabacak B, Sogukpinar I. A quantitative method for ISO 17799 gap analysis. *Computers & Security*. 2006; 25(6):413-9.

Ku CY, Chang YW, Yen DC. National information security policy and its implementation: A case study in Taiwan. *Telecommunications Policy*. 2009; 33(7):371-84.

Laribee L, Barnes DS, Rowe NC, Martell CH. Analysis and defensive tools for social-engineering attacks on computer systems. In: *Proceedings of the IEEE Workshop on Information Assurance*. 2006. p.388-9.

Lau F, Rubin SH, Smith MH, Trajkovic L. Distributed denial of service attacks. In: *ICSMC 2000 - IEEE International Conference on Systems, Man and Cybernetics*. 2000. p.2275-80.

Luethi M, Knolmayer GF. Security in health information systems: an exploratory comparison of U.S. and Swiss hospitals. In: *HICSS 09 - Hawaii International Conference on System Sciences*. 2009. p.1-10.

Massad E, Menezes RX, Silveira PSP, Ortega NRS. *Métodos quantitativos em medicina*. Barueri. Manole. 2004.

McGee AR, Bastry FA, Chandrashekhar U, Vasireddy SR, Flynn LA. Using the bell labs security framework to enhance the ISO 17799/27001 information

security management system". Bell Labs Technical Journal. 2007;12(3):39-54.

Miller HG., Murphy RH. Secure cyberspace: answering the call for intelligent action. IT Professional. 2009;11(3):60-3.

Mitnick K, Simon W. The art of deception. Indianapolis. Wiley. 2002.

Ramos A, Bastos A, Lyra A, Andrucio A, Affonso C, Poggi E, Pinto E, Blum RO, Alevate W, Marinho Z. Security officer – guia oficial para formação de gestores em segurança da informação. 2th ed. Porto Alegre: Zouk; 2008.

Sahibudin S, Sharifi M, Ayat M. Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive it framework in organizations. In: AICMS 08 - Second Asia International Conference on Modeling & Simulation, 2008. p. 749-53.

Samy GN, Ahmad R, Ismail Z. Threats to health information security. In: IAS 09 - Fifth International Conference on Information Assurance and Security. 2009. p. 540-3.

Sánchez LE, Villafranca D, Fernandez-Medina E, Piattini M. Practical approach of a secure management system based on ISO/IEC 17799. In: ARES 2006 - First International Conference on Availability, Reliability and Security. 2006. p. 585-92.

Shortliffe EH, Perreault LE, Wiederhld G, Fagan LM. Medical informatics, computers applications in health care and biomedicine. New York. Springer 2001.

Souza R. Metodologia para desenvolvimento e implantação de sistemas de gestão da qualidade em empresas construtoras de pequeno e médio porte [tese]. São Paulo: Escola Politécnica, Universidade de São Paulo; 1997.

Tanenbaum AS. Redes de computadores. Rio de Janeiro. Campus. 2003.