CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA

RAMIRO SEVERINO RODRIGUES

ESTUDO DE UM PROCESSO ESTRUTURADO DE SEGURANÇA DA INFORMAÇÃO EM SISTEMAS DE INFORMAÇÃO DO SETOR DE SAÚDE COM BASE NA NORMA ISO 27799:2008

SÃO PAULO

AGOSTO/2010

RAMIRO SEVERINO RODRIGUES

ESTUDO DE UM PROCESSO ESTRUTURADO DE SEGURANÇA DA INFORMAÇÃO EM SISTEMAS DE INFORMAÇÃO DO SETOR DE SAÚDE COM BASE NA NORMA ISO 27799:2008

Dissertação apresentada como exigência parcial para obtenção do Título de Mestre em Tecnologia no Centro Estadual de Educação Tecnológica Paula Souza, no Programa de Mestrado em Tecnologia: Gestão, Desenvolvimento e Formação, sob orientação da Prof. Dra. Márcia Ito

SÃO PAULO

AGOSTO/2010

Rodrigues, Ramiro

R696e Estudo de um processo estruturado de segurança da informação em sistemas de informação do setor de saúde com base na Norma ISO 27799:2008. – São Paulo : CEETEPS, 2010.

134 f. : il.

Orientador: Prof. Dra. Márcia Ito.

Dissertação (Mestrado) – Centro Estadual de Educação Tecnológica Paula Souza, 2010.

1. Segurança da informação. 2. Sistemas de registro eletrônico de Saúde. 3. Norma ISO 27799:2008. 4. Informática na área de Saúde. I. Ito, Márcia. II. Centro Estadual de Educação Tecnológica Paula Souza. III. Título.

RAMIRO SEVERINO RODRIGUES

ESTUDO DE UM PROCESSO ESTRUTURADO DE SEGURANÇA DA INFORMAÇÃO EM SISTEMAS DE INFORMAÇÃO DO SETOR DE SAÚDE COM BASE NA NORMA ISO 27799:2008

PROFA. DRA. MÁRCIA ITO

PROF. DR. CARLOS HIDEO ARIMA

PROFA. DRA. MARILIA MACORIN DE AZEVEDO

São Paulo, 10 de agosto de 2010

Dedicatória

A minha esposa e aos meus filhos que compartilharam comigo os momentos de esforço dedicação a esse trabalho.

Agradecimentos

Agradeço a Deus por todos os dias da minha vida e por me permitir realizações pessoais e profissionais.

“A melhor maneira de ficar em segurança é nunca se sentir seguro.”
Benjamin Franklin

Resumo

SEVERINO RODRIGUES, R. **Estudo de um processo estruturado de segurança da informação em sistemas de informação do setor de Saúde com base na norma ISO 27799:2008**. 2010. 134f. Dissertação (Mestrado), Centro Estadual de Educação Tecnológica Paula Souza.

O surgimento e a evolução dos Sistemas de Registros Eletrônicos de Saúde (S-RES) possibilitaram a criação e a manutenção de registros de saúde de pacientes e a criação de bases de dados digitais que contém informações agregadas clínicas e administrativas apoiadas em infra estruturas tecnológicas e de telecomunicações. As soluções tecnológicas e de telecomunicações empregadas são complexas e introduzem riscos de segurança à confidencialidade, a integridade e a disponibilidade das informações nos sistemas S-RES que capturam, armazenam e trafegam informações pessoais de saúde, e em última análise, podem expor os pacientes e a organização de saúde a riscos. O surgimento da norma ISO 27799:2008 trouxe às organizações de saúde, orientação, apoio e referências sobre a gestão da segurança, da confidencialidade, da integridade e da disponibilidade das informações pessoais de saúde por meio da implementação de um Sistema de Gestão de Segurança da Informação (SGSI).

Entretanto a norma ISO 27799:2008 não oferece uma visão estruturada e detalhada dos processos e dos sub processos de implementação e manutenção de um SGSI para o setor de saúde. A principal contribuição desse estudo foi no sentido de apresentar uma proposta de processos e sub processos estruturados e sistematizados que orientam e direcionam para a implementação e manutenção do sistema de segurança em organizações de saúde. Esse estudo examinou os processos necessários para a implementação e manutenção de um sistema de segurança da informação para o setor de saúde de acordo com a norma ISO 27799:2008. O resultado do estudo apresentado nesse trabalho traz descrições detalhadas e explicações sobre os processos para uma organização de saúde que deseje implementar segurança da informação.

Palavras-Chave: gestão de segurança da informação, norma ISO 27799:2008, organização de saúde, sistemas de registro eletrônico de saúde, informática em saúde, riscos em segurança da informação.

Abstract

SEVERINO RODRIGUES, R. **Study of a structured process of information security for healthcare information systems based in ISO standard 27799:2008**. 2010. 134f. Dissertation (Master´s degree in Technology) - Program of Master´s degree, Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2010.

The advent and the evolution of Electronic Health Record Systems (EHR-S) made possible the creation and maintenance of patient health records and the creation of digital databases containing aggregated clinic and administrative information based in telecommunication and information technology infrastructure. These information technology and communication infrastructure are complex and introduce information security risks to the confidentiality, to integrity and availability of EHR-S systems information by exposing patient and heath organization to risks.

The international standard ISO 27799:2008 brought to health organizations, guidance, support and references on information security management, confidentiality, integrity and on availability of patient health personal information by the implementation of an information security management system (ISMS). However, the international standard ISO 27799:2008 does not present the structured and detailed process and sub process for implementing and maintaining the ISMS for health organization. The main contribution of this research was in developing a proposal of systematic and detailed structured process and sub process for implementation and maintenance of information security management system for health organization based in the international standard ISO 27799:2008.

The outcome of this research is a detailed descriptions and explanations of process and sub process to be implemented by the health organization that wishes to improve it information security system.

Keywords: information security management, health care systems, health informatics, ISO standard 27799:2008, heath care systems risk management, electronic health information.

Lista de Figuras

Lista de Quadros

Lista de Abreviaturas e Siglas

ABNT	Associação Brasileira de Normas Técnicas
AC	Autoridade Certificadora
AMB	Associação Médica Brasileira
ANS	Agência Nacional de Saúde Suplementar
ANS	Acordo de Nível de Serviço
ANSI	American National Standards Institute
ANVISA	Agência Nacional de Vigilância Sanitária
AR	Autoridade Registradora
ASSESPRO	Associação das Empresas Brasileiras de Tecnologia da Informação
CA	*Canadian Acreditation*
CCHIT	*Certification Commission for Healthcare Information Technology*
CEETEPS	Centro Estadual de Educação Tecnológica Paula Souza
CFM	Conselho Federal de Medicina
CNES	Cadastro Nacional de Estabelecimentos e Profissionais de Saúde do SUS
CNU	Cadastro Nacional de Usuários do SUS
CONARQ	Conselho Nacional de Arquivos
CRM	Conselho Regional de Medicina
DA	Declaração de Aplicabilidade
FATEC	Faculdade de Tecnologia
FGSI	Fórum de Gestão de Segurança da Informação
GNU	*General Public License*
HIPAA	*Health Insurance Portability Acountability Act*
HL7	*Health Level 7*
ICP	Infraestrutura de Chaves Públicas
IEC	*International Electrotechnical Commission*
ISO	*International Organization for Standardization*
ITA	Instituto Tecnológico de Aeronáutica
ITI	Instituto Nacional de Tecnologia da Informação
JCI	*Joint Commission International*
MS	Ministério da Saúde
NIST	*National Institute of Standards and Technology*
ONA	Organização Nacional de Acreditação
PEP	Prontuário Eletrônico do Paciente
RES	Registro Eletrônico em Saúde
SBIS	Sociedade Brasileira de Informática em Saúde
SGBD	Sistema de Gerenciamento de Banco de Dados
SGSI	Sistema de Gestão de Segurança da Informação
SRES	Sistema de Registro Eletrônico de Saúde
TI	Tecnologia da Informação
TISS	Troca de Informação em Saúde Suplementar
USP	Universidade de São Paulo

Sumário

1. INTRODUÇÃO

A gestão da segurança em sistemas de informação do setor de saúde no Brasil torna-se cada vez mais necessária em função do emprego crescente de novas tecnologias da informação na interoperabilidade dos sistemas com as organizações de serviços de saúde. A interoperabilidade é definida como "a interconexão efetiva de diferentes sistemas de computador, bancos de dados ou redes com o fim de apoiar a computação distribuída e/ou o intercâmbio de dados" (WASHINGTON DC, 1994). Esses sistemas e interconexões complexos podem aumentar os riscos relacionados à confiabilidade, integridade e disponibilidade das informações nos sistemas que capturam, armazenam e trafegam a informação identificada em saúde, denominados Sistemas de Prontuário Eletrônico do Paciente (PEP) ou Sistemas de Registro Eletrônico de Saúde (S-RES) e, em última análise, podem expor os pacientes a riscos.

Todas as organizações de fornecimento de serviços saúde precisam ter controles mínimos implementados para proteger a informação confiadas a elas. No Brasil, o Conselho Federal de Medicina (CFM) publicou em 2007 a Resolução 1821/2007 que regula o uso de métodos de digitalização de dados de pacientes e o uso de S-RES como registro de informações de saúde informatizado. Essa Resolução aprovou também o Manual de Certificação para Sistemas de Registro Eletrônico em Saúde, que detalha, dentre outros, os requisitos de segurança que os S-RES devem atender para serem utilizados.

A segurança da informação tem sido uma preocupação das grandes organizações. Eventos como o “10º Simpósio Segurança da Informação”, realizado no Instituto Tecnológico de Aeronáutica (ITA), em São José dos Campos – SP, em 2009, têm o objetivo de divulgar conceitos e técnicas de segurança da informação. As organizações têm investido na implementação de controles e na obtenção de certificações de qualidade em segurança da informação, que se agregam à imagem da empresa no mercado, apoiando-se, muitas vezes, em normas sobre o tema. A norma ISO/IEC 27002:2005 (Código de Prática para a Gestão de Segurança da Informação) é uma das principais referências para quem precisa de um *checklist* dos principais controles que compõem uma política de segurança da informação (ALVES, 2005).

Já a norma ISO/IEC 27001:2005 (Tecnologia da informação – Técnicas de segurança – Sistemas de gerenciamento da segurança da informação – Requisitos) é empregada extensivamente para a gestão de segurança de sistemas informatizados no setor de saúde na Austrália, Canadá, França, na Holanda, Nova Zelândia, África do Sul e Reino Unido, por meio das agências reguladoras (HUMPHREYES, 2007). No Brasil, até a conclusão desse trabalho, não foram identificados registros da adoção da norma ISO/IEC 27001:2005 em organizações de saúde de acordo com a base de dados de registros de certificados internacionais.

Publicada pela *International Organization for Standardization* (ISO) em 2008, a norma internacional ISO 27799:2008 (*Health informatics - Information security management in health using ISO/IEC 27002*) baseia-se na experiência obtida nos esforços internacionais em lidar com a segurança de informação pessoal de saúde e é um documento associado à ISO/IEC 27002:2005. Não é intenção desta norma, suplantar as normas ISO/IEC 27002 ou a ISO/IEC 27001.

A norma ISO 27799:2008 trata das peculiaridades específicas do setor de saúde no âmbito da segurança das informações. Ela fornece guias de implementação das normas ISO/IEC 27001 e ISO/IEC 27002:2005, portanto, fornece as melhores práticas internacionais para o setor de Saúde

Este trabalho propõe um modelo de processos estruturados para implementação e manutenção de segurança da informação com base norma ISO 27799:2008, e tendo como base as características dos Sistemas de Registros Eletrônicos em Saúde (S-RES).

1.1 Problematização

As tecnologias de informação e o nível de interoperabilidade presentes nas organizações de saúde aumentam os riscos relacionados à confiabilidade, integridade e disponibilidade da informação em Sistemas de Registro Eletrônico em Saúde (S-RES) porque tais tecnologias trazem embutidas falhas e erros, e em última análise, sua utilização, pode expor os pacientes a riscos.

Um artigo publicado em um jornal nos Estados Unidos, em maio de 2006, denunciou que uma falha no S-RES (Sistema de Registro Eletrônico em Saúde) pode ter levado ao roubo de dados referentes a 60.000 pacientes que foram atendidos no Centro Médico da Universidade de Ohio, causando impactos à privacidade da informação pessoal de saúde (BOSWORTH, 2006).

De acordo com uma pesquisa recente realizada pelo Ponemon Institute junto às organizações de saúde nos Estados Unidos, as três maiores ameaças emergentes que afetam a habilidade das organizações de saúde em proteger informações de seus pacientes são: infecção por vírus (*malware*), perda de informações de pacientes (*data breach*) e ataques internos de funcionários. (PONEMOM INSTITUTE LLC, 2009).

A Figura 1 exibe o resultado parcial da pesquisa que aponta também que as ameaças mais prováveis e mais severas são: falha na identificação e autenticação, perda de informações (*data breach*) e ataques internos de funcionários.

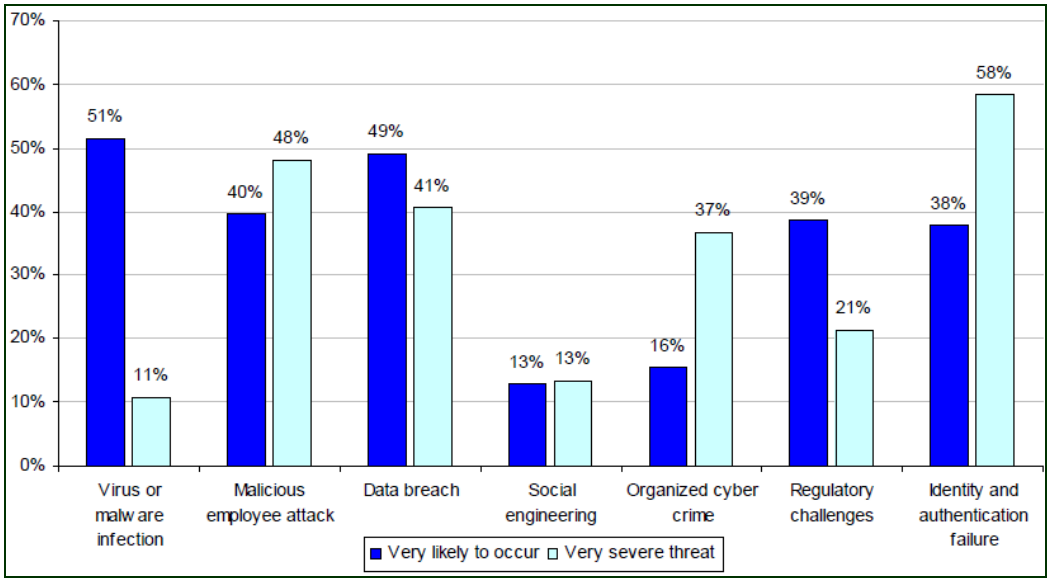

Figura 1– Probabilidade e severidade das ameaças de segurança às informações eletrônicas de saúde dos pacientes
Fonte**:** Ponemon Institute LLC (2009)

De acordo com a norma ISO 27799:2008, existem algumas diferenças na proteção de sistemas de informação do setor de saúde quando comparadas com outros setores de negócios

baseados em Tecnologia da Informação. Como exemplo pode-se citar que enquanto muitos bancos e empresas podem parar suas operações devido a um evento inesperado de desastre natural ou indisponibilidade da plataforma de tecnologia em função de falhas de segurança, as organizações do setor de saúde, notadamente hospitais, necessitam manter a operação funcionando sob várias condições adversas. Isso é imprescindível para manter o tratamento dos pacientes, bem como, manter e restaurar a saúde da comunidade em caso de desastres.

Dada a relevância e criticidade atual do tema Segurança da Informação em saúde, este estudo propõe a apresentar processos estruturados para implementação e manutenção de segurança da informação nos sistemas informatizados de saúde.

1.2 Objetivo Geral

O objetivo geral desse trabalho é o estudo de uma proposta conceitual de processos estruturados para implementação e manutenção da segurança da informação em sistemas de informação do setor de saúde com base na norma ISO 27799:2008.

1.3 Objetivos Específicos

Com intuito de atingir o objetivo principal desse estudo são propostos os seguintes objetivos específicos:

- A partir da revisão bibliográfica, objetiva-se analisar as propriedades dos macros processos atuais de implementação e manutenção de segurança em saúde, conforme definidos na norma ISO 27799:2008.
- Identificar os subprocessos para implementação e manutenção de segurança, com a identificação das respectivas entradas, ferramentas, técnicas e saídas dos processos.

1.4 Justificativa

A boa governança se tornou um tema crítico para todos os tipos de organizações nos últimos tempos, particularmente em respostas às demandas regulatórias presentes nos Estados Unidos como a *Sarbanes Oxley Act* e o HIPAA – *Health Insurance Portability Acountability Act,* o *Basel II Accords* na Europa, o *Turnbull Code* no Reino Unido e, na Alemanha, o *KontraG*. Além disso, a crescente dependência de informações nas organizações e de tecnologias de suporte à informação, faz da gestão da informação um componente importante do processo de gerenciamento do risco operacional.

De acordo com a norma ISO 27799 (ISO, 2008, p. 9), as seguintes informações de saúde devem ser protegidas e ter sua confidencialidade, integridade e disponibilidade preservadas

- Informação pessoal de saúde;
- Dados pseudomizados derivados da informação pessoal de saúde por meio de alguma metodologia de pseudomização da identificação;
- Dados estatísticos e de pesquisas, incluindo dados anonimizados derivados de informação pessoal de saúde pela remoção de dados de identificação pessoal;
- Conhecimento clínico ou médico não associado para um paciente específico ou pacientes, incluindo dados de suporte de decisão clínica (por exemplo, dados sobre reações adversas à drogas);
- Dados sobre profissionais de saúde e equipes de apoio;
- Informação relacionada à vigilância de saúde pública;
- Auditoria de rastreamento de dados que são produzidos pelos sistemas de informação de saúde contendo informação pessoal de saúde ou dados pseudônimos derivados da informação pessoal de saúde ou dados sobre ações de usuários em relação à informação pessoal de saúde;
- Sistema de segurança de dados, incluindo dados de controle de acesso e outras seguranças relacionadas ao sistema de configuração de dados, para sistemas de informação de saúde.

A extensão da proteção da confidencialidade, da integridade e da disponibilidade depende da natureza da informação, dos usos aos quais se destinam e dos riscos aos quais está

é exposta. Por exemplo, dados estatísticos podem não ser confidenciais, mas a proteção de sua integridade pode ser muito importante.

Da mesma forma, dados de trilhas de auditoria podem não requerer alta disponibilidade (seus tempos de armazenamento e recuperação medidos em horas em vez de segundos que podem ser exigidos por certas aplicações), mas seu conteúdo pode ser altamente confidencial. A avaliação de risco pode determinar corretamente o nível de esforço necessário para proteger a confidencialidade, a integridade e a disponibilidade das informações em questão. Os resultados das avaliações regulares de risco devem ser ajustados às prioridades e recursos da organização.

Estar em conformidade com normas como a ISO/IEC 27001:2005 não é meramente uma questão de adoção de um *checklist*, mas sim, para estarem verdadeiramente em conformidade, as organizações de saúde precisam ser capazes de demonstrar que seu Sistema de Gestão de Segurança da Informação está efetivo e que existem processos apropriados de planejamento e manutenção desse Sistema.

1.5 Metodologia de Pesquisa

A presente dissertação está apoiada em uma pesquisa com as seguintes classificações:

Com relação à natureza, trata-se de uma pesquisa aplicada, pois de acordo com Silva e Meneses (2003, p. 20) a pesquisa aplicada “objetiva gerar conhecimentos para aplicação prática dirigidos à solução de problemas específicos”.

Do ponto de vista de abordagem do problema, classifica-se como pesquisa qualitativa, à medida que é descritiva e os dados tendem a ser analisados indutivamente.

O método exploratório se justifica, com relação aos objetivos, pelo fato do assunto abordado ser novo em termos de Brasil, sendo importante identificar os processos de implementação e manutenção de segurança recomendados na ISO 27799:2008 e a sua forma de implementação. De acordo com Gil (1999), a pesquisa exploratória é desenvolvida com o objetivo de proporcionar visão geral acerca de determinado fato e visa proporcionar maior

familiaridade com o problema, com vistas a torná-lo explícito ou a construir hipóteses. Envolve levantamento bibliográfico.

Com relação aos procedimentos técnicos adotados, esta dissertação se classifica como uma pesquisa bibliográfica, à medida que se baseia no conteúdo das normas de segurança da informação e em outras referências bibliográficas de implementação e manutenção de segurança da informação. De acordo com Gil (1991), a pesquisa é classificada como bibliográfica quando elaborada a partir de material já publicado, constituído principalmente de livros, artigos de periódicos e, atualmente, também com material disponibilizado na Internet.

1.6 Organização do Trabalho

Este trabalho está organizado conforme estrutura descrita a seguir:

O **capítulo 1** apresenta os elementos do projeto de pesquisa dessa dissertação, os quais são respectivamente: a introdução ao trabalho, a definição do problema a ser pesquisado, os objetivos que se pretendem atingir, as justificativas que levaram ao trabalho e a metodologia empregada.

O **capítulo 2** compreende o referencial teórico que suporta o desenvolvimento deste estudo. Ele estabelece uma base conceitual para os termos e conceitos concernentes a informação e à segurança da informação em particular para o segmento de saúde. Trata também de apresentar um exame das normas internacionais e padrões de segurança da informação, em particular na norma ISO 27799:2008. A importância de se considerar os requerimentos regulatórios e normativos de órgão governamentais e de classe são também considerados nesse capitulo. O capítulo apresenta ainda conceitos e modelos de gestão de riscos.

O **capítulo 3** compreende o desenvolvimento da pesquisa e apresenta de forma detalhada a descrição dos processos e subprocessos de implementação e manutenção de segurança da informação, considerando Sistemas de Registro Eletrônico em Saúde (S-RES), tomando como ponto de partida o ciclo PDCA e conceitos da norma ISO 27799:2008. Neste

capítulo os processos foram pesquisados em várias referencias bibliográficas citadas e documentadas e descritos com seus respectivos elementos de entrada, saída e atividades.

O **capítulo 4** apresenta as considerações e as análises concernentes aos processos de implementação e manutenção de um sistema de gestão de segurança no segmento de saúde. Nesse capítulo é discutida a necessidade de considerar técnicas de gerenciamento de projeto para planejar a implementação do sistema de segurança. Entretanto, é importante registrar também que esse trabalho não pretende explorar os processos de gestão de projetos necessários para uma implementação de sucesso.

O **capítulo 5** apresenta as conclusões e contribuições desse estudo e seus resultados em benefício das organizações de saúde que desejam implementar sistemas de segurança da informação para a adequada governança e proteção das informações dos pacientes.

2. SEGURANÇA DA INFORMAÇÃO: CONCEITOS, RISCOS E NORMATIZAÇÃO PARA O SETOR DE SAÚDE

Este capítulo constitui a fundamentação teórica para o presente estudo, no qual os conceitos sobre segurança da informação, riscos, normatização e regulamentação para o setor de saúde são pesquisados e apresentados.

2.1 Segurança da Informação

O objetivo deste capítulo é apresentar a base conceitual para os termos utilizados neste trabalho e também apresentar a norma referente à gestão de segurança da informação em saúde, ISO 27799:2008, sua origem, seu significado e importância, para servir de referência para a abordagem desse estudo.

2.1.1 Princípios da Segurança da Informação

Segundo o Código de Prática para Gestão da Segurança da Informação ISO/IEC 27002:2005 (ISO/IEC, 2005b, p. ix), “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”. 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.

O princípio fundamental da segurança da informação está no controle de acesso a recursos críticos que requerem proteção contra modificação e revelação não autorizada (DEY, 2007).

Segundo a norma ISO/IEC 27002:2005, segurança da informação é a proteção da informação contra vários tipos de ameaças de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno sobre investimentos e oportunidades

de negócios. Ainda segundo a ISO/IEC 27002:2005 a segurança da informação é caracterizada pela preservação dos três atributos básicos da informação:

- **Confidencialidade**: A informação não deve ser divulgada para pessoas não autorizadas.
- **Disponibilidade**: A informação precisa estar disponível para as pessoas autorizadas sempre que necessário.
- **Integridade**: A informações deve ser exata e completa. A informação deve ser protegida contra modificações não autorizadas.

A segurança não é uma questão técnica, mas uma questão gerencial e humana (KOVACICH, 2006). Apesar de exercer um papel fundamental, a tecnologia não deve ser o único pilar para garantir a segurança da informação. É necessário treinar e conscientizar as pessoas por meio de uma política de segurança da informação.

2.1.2 Política de Segurança da Informação

A Política de Segurança da Informação é uma declaração formal da organização acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores (HERRERA, 2005). Seu propósito é estabelecer as diretrizes a serem seguidas pela organização no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança da informação.

A política de segurança da informação é composta por um conjunto de regras e padrões que definem o que deve ser feito para garantir às informações da organização os princípios de confidencialidade, disponibilidade e integridade. A política deve conter as diretrizes e regras de segurança na organização, e os procedimentos para implementar cada medida de segurança.

A seguir, é apresentado um exemplo de treco Política de Segurança da Informação:

> Toda informação, independente de sua forma ou formato, que é criada ou utilizada para suportar as atividades de negócio é de propriedade da organização. Informações corporativas são ativos e devem ser protegidos desde sua criação até o fim de sua vida útil. Devem ser mantidas em um local seguro, correto e de forma confiável sendo prontamente disponibilizadas para uso autorizado. A informação será

> classificada baseada na sua capacidade crítica, exigências legais, necessidade de retenção e tipos de acesso requeridos pelos funcionários ou outros colaboradores.
> A Segurança da Informação é a proteção dos dados contra divulgação acidental ou intencional, modificação não autorizada ou destruição. A informação será protegida tendo como princípio seu valor para a organização, confidencialidade e o risco de perda ou seu comprometimento. As informações somente serão manipuladas por indivíduos formalmente autorizados (FERREIRA, 2006 p. 20).

A estrutura da Política de Segurança da Informação é composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

- Política de Segurança da Informação (Política): constituída em documento, define a estrutura, as diretrizes e as obrigações referentes à segurança da informação;
- Normas de Segurança da Informação (Normas): estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem seguidos em diversas situações em que a informação é tratada;
- Procedimentos de Segurança da Informação (Procedimentos): instrumentalizam o disposto nas Normas e na Política, permitindo a direta aplicação nas atividades da organização.

A Política e as Normas de Segurança da Informação devem ser divulgadas a todos os colaboradores da organização e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento.

A área de Gestão de Segurança da Informação da organização deve manter um inventário atualizado que identifique e documente a existência e as principais características de todos os seus ativos de informação (base de dados, arquivos, diretórios de rede, trilhas de auditoria, códigos fonte de sistemas, documentação de sistemas, manuais, planos de continuidade etc.). As informações inventariadas devem ser associadas a um “proprietário”, que pode ser um diretor ou um gerente dentro da organização, designado formalmente pela alta administração como responsável pela autorização de acesso às informações sob a sua responsabilidade.

As informações inventariadas devem ser classificadas de acordo com o grau de confidencialidade e criticidade para o negócio da organização, e com base na Norma específica de classificação de informações estabelecida pela organização.

2.1.3 Classificação das Informações

A classificação da informação ajuda a definir níveis e critérios adequados de proteção das informações, garantindo a confidencialidade, conforme a importância da organização (BASTOS; CAUBIT, 2009). As informações tanto em meio físico quanto eletrônico, possuem necessidades de proteção quanto a confidencialidade, integridade e disponibilidade, bem como quaisquer outros requisitos que sejam necessários. Em geral, a classificação dada à informação é uma maneira de determinar como esta informação vai ser tratada e protegida de acordo com uma política definida.

Conforme citado por (Ferreira, 2006, p. 20), o autor menciona que "(...) a informação será classificada baseada na sua capacidade crítica, exigências legais, necessidade de retenção e tipos de acesso requeridos pelos funcionários ou outros colaboradores". Portanto, para definir a política de segurança, é necessário identificar e classificar as informações da organização. A classificação das informações proporciona os seguintes benefícios indiretos:

- A confidencialidade, integridade e disponibilidade são mantidas devido à aplicação de controles adequados apropriados ao nível classificado;
- Melhor direcionamento dos investimentos em recursos físicos e lógicos para garantir a segurança da informação nos ativos mais críticos da organização.

A política e o processo classificação das informações podem variar de organização para organização. O Quadro 1 apresenta um exemplo de critérios classificação de informações para uma determinada organização.

Quadro 1 – Critérios para classificação das informações

Informação Pública	Considera informações que, se forem divulgadas fora da organização, não trarão impactos aos negócios. Desta forma, a confidencialidade dos dados não é vital. Exemplos: testes de sistemas ou serviços sem dados confidenciais, *folders* da organização;
Informação Interna	Consiste em informações que não devem ser divulgadas fora da organização. Entretanto, se estes dados tornarem-se públicos, as conseqüências não são críticas. A integridade dos dados é importante, mas não vital. Exemplos: agendas de telefones e ramais, documentos e procedimentos internos etc.
Informação Confidencial	Trata-se de informações que devem ser protegidas de acesso interno e externo. Se alguns destes dados forem acessados por pessoas não autorizadas, as operações da organização podem ser comprometidas, causando perdas financeiras e perda de competitividade. A integridade dos dados é vital. Exemplos: salários, dados pessoais, dados de clientes, senhas e informações sobre as vulnerabilidades da organização.

Fonte: Ferreira (2006)

O segmento de saúde (hospitais, clinicas, laboratórios etc.) apresenta desafios e requerimentos específicos em segurança das informações em função da natureza das informações manipuladas, ou seja, informações dos pacientes. Esse tema será tratado em detalhes no capítulo seguinte.

2.2 Segurança da Informação para o Setor de Saúde

O objetivo deste capítulo é discorrer sobre como o tema de segurança da informação se relaciona com o setor de organizações de saúde no Brasil. As normas e padrões de segurança da informação fornecem uma abordagem sistemática de gerenciamento adotada para a melhoria das práticas de segurança. Elas contribuem para quantificar um nível aceitável de risco e implementar medidas apropriadas de segurança que garantam a confidencialidade, integridade e disponibilidade das informações (HUMPHREYES, 2007).

2.2.1 Informação Pessoal de Saúde

De acordo com a norma ISO 27799:2008, a informação pessoal de saúde refere-se à informação sobre uma pessoa identificável, relacionada à saúde física ou mental do indivíduo, ou à provisão de serviços de saúde ao indivíduo que podem incluir:

- Informação sobre o registro do indivíduo para a provisão de serviços de saúde;
- Informação sobre pagamentos ou elegibilidade para a saúde com respeito ao indivíduo;
- Um número, um símbolo ou um detalhe particular atribuído a um indivíduo para identificar unicamente o indivíduo para propósitos de saúde;
- Qualquer informação sobre o indivíduo coletada no decorrer da provisão de serviços de saúde ao indivíduo;
- Informação derivada do ensaio ou do exame de uma parte do corpo ou substância corporal;
- Identificação de uma pessoa (por exemplo, um profissional de saúde) como o fornecedor da saúde ao indivíduo.

A informação pessoal de saúde não inclui a informação que, por si só ou combinada com outras informações disponíveis àquele que a detém, é anonimizada, isto é, situação em que a identidade do indivíduo que é o sujeito da informação não pode ser verificada por meio desta.

As informações pessoais de saúde podem estar em papéis, formulários impressos, e também em sistemas computacionais, como exemplo os Sistemas de Registro Eletrônico em Saúde (S-RES).

No Brasil, o Conselho Federal de Medicina (CFM) publicou em 2007 a Resolução 1821/2007, que regula o uso de métodos de digitalização de dados de pacientes e os requisitos de segurança da informação que S-RES deve atender para ser utilizado.

2.2.2 Requisitos da Segurança da Informação em Saúde

Os requisitos de segurança de um S-RES são fundamentais para aqueles interessados em eliminar o registro em papel das informações relativas a cada paciente (CONSELHO FEDERAL DE MEDICINA, 2002. Existe uma série de recomendações quanto ao acesso, uso e armazenamento dos prontuários em papel, várias delas visando resguardar a sua legitimidade das informações ali contidas. Os requisitos de segurança apresentados pelo Conselho Federal de Medicina buscam resguardar a legitimidade das informações manipuladas e armazenadas em um S-RES, ao mesmo tempo preservando a segurança e confidencialidade destas informações. Os prontuários em papel estão sujeitos a falsificações, destruição (exemplo: incêndio ou inundação), além de extravio ou roubo.

Com o prontuário médico em um S-RES os riscos não são diferentes, podendo ser maiores para um S-RES, na medida em que sistemas informatizados conectados a redes corporativas e à internet podem vir a ser acessados por indivíduos não autorizados, caso os requisitos de segurança estejam incompletos, sejam inadequados ou obsoletos, ou até mesmo, caso não tenham sido implementados no S-RES, expondo-os a riscos de roubo de informações, quebra de confidencialidade, dentre outros. Além disso, os sistemas operacionais ou de suporte incorretamente configurados, podem permitir que usuários

inexperientes ou mal treinados cometam erros durante sua operação (exemplo: formatação equivocada ou intencional de uma unidade de armazenamento de dados do S-RES).

Os requisitos de segurança apresentados no Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde do CFM visam orientar desenvolvedores de software, no caso, o de S-RES e seus respectivos usuários quanto aos cuidados mínimos que devem ser observados na utilização de sistemas computadorizados.

Desde 2002, o Grupo de Interesse (GI) em Certificação e Padrões da Sociedade Brasileira de Informática em Saúde (SBIS) juntamente com a Câmara Técnica de Telemedicina e Informática em Saúde do Conselho Federal de Medicina (CFM) vêm conduzindo discussões a respeito de como melhorar a qualidade dos sistemas de informação em saúde no Brasil, em especial aqueles sistemas que capturam, armazenam e trafegam a informação identificada em saúde, ou seja, Sistemas de Prontuário Eletrônico do Paciente (PEP) ou Sistemas de Registro Eletrônico de Saúde (S-RES). O processo de certificação SBIS/CFM destina-se a sistemas que capturam, armazenam e trafegam a informação identificada em saúde, ou seja, Sistemas de Registro Eletrônico de Saúde (S-RES). As definições são abrangentes e amplas, de maneira que qualquer sistema que capture, armazene, apresente, transmita ou imprima informação identificada em saúde poderá se submeter ao processo de certificação voluntariamente. Não há obrigatoriedade das organizações de saúde de certificar o seu sistema RES.

O processo de certificação SBIS/CFM classifica os S-RES, do ponto de vista de segurança da informação, em dois Níveis de Garantia de Segurança (NGS):

- NGS1 - categoria constituída por S-RES que não contemplam o uso de certificados digitais para assinatura digital das informações clínicas, consequentemente sem amparo para a eliminação do papel e com a necessidade de impressão e aposição manuscrita da assinatura;
- NGS2 - categoria constituída por S-RES que viabilizam a eliminação do papel nos processos de registros de saúde. Para isso, especifica a utilização de certificados digitais para os processos de assinatura e autenticação.

O Manual de Certificação para Sistemas de Registro Eletrônico de Saúde, editado e publicado pela SBIS/CFM, recomenda, para ambos os níveis, a observância das boas práticas

para a gestão da segurança da informação descritas na norma NBR ISO/IEC 27.002 publicada pela ABNT, adaptadas as necessidades organizacionais de cada instalação do S-RES. (CONSELHO FEDERAL DE MEDICINA, 2002).

2.3 Regulamentação para o Setor de Saúde

De acordo com o Ministério da Saúde, "regulação" é o "poder de arbítrio que é exercido pelo Estado, em prol do interesse coletivo, no âmbito da administração e da fiscalização de atividades públicas ou privadas" (BRASIL, 2009, p. 43). No Brasil, o setor de saúde basicamente é regulado pela ANVISA – Agência Nacional de Vigilância Sanitária, pela ANS – Agência Nacional de Saúde Suplementar e pelo CFM – Conselho Federal de Medicina. O setor de saúde conta ainda com o apoio da Sociedade Brasileira de Informática em Saúde (SBIS) que, juntamente com o CFM, desenvolve, orienta, publica processos e normas técnicas sobre o uso da informática na área de saúde.

2.3.1 Resoluções da SBIS/CFM

No segmento das organizações de saúde, a segurança e a privacidade das informações transmitidas e/ou armazenadas em prontuários eletrônicos e sistemas de informação sempre são assuntos muito sensíveis (SALVADOR, 2005). O setor de saúde no Brasil tem investido muito em tecnologia da informação nos últimos anos, de acordo com notícia publicada no sítio Saúde *Business Web*[1]. Da mesma forma, tem havido alguns avanços nas resoluções normativas a respeito da segurança e da privacidade da informação, o que tem exigido cuidados específicos com estes temas pelo setor de saúde. A normatização do setor de saúde está apoiada principalmente em resoluções normativas do Conselho Federal de Medicina (CFM), em resoluções da Agência Nacional em Saúde Complementar (ANS) e em leis do próprio Código Penal brasileiro.

[1] Disponível em http://www.saudebusinessweb.com.br/noticias/index.asp?cod=68328

Em 2004, o Conselho Federal de Medicina em cooperação técnica com a Sociedade Brasileira de Informática em Saúde, normatizou o uso de sistemas de informatizados para a guarda e manuseio do prontuário de pacientes. O Conselho Federal de Medicina (CFM) publicou o Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (SRES), com o objetivo de estabelecer melhores práticas e permitir que os operadores se preparem para o cumprimento das normas estabelecidas.

Em 2007, as “Normas Técnicas Concernentes à Digitalização e Uso dos Sistemas Informatizados para a Guarda e Manuseio dos Documentos dos Prontuários dos Pacientes, Autorizando a Eliminação do Papel e a Troca de Informação Identificada em Saúde”, elaboradas pela SBIS em conjunto com o CFM, foram aprovadas pela resolução no. 1821/2007, substituindo a resolução no. 1639/2002, (Normas Técnicas para o Uso de Sistemas Informatizados para a Guarda e Manuseio do Prontuário Médico). Além das resoluções do CFM, a certificação se apóia na Infraestrutura de Chaves Públicas Brasileira (ICP Brasil), nos Cadastros Nacionais em Saúde e no padrão de Troca de Informações em Saúde Suplementar (TISS) da Agência Nacional em Saúde Suplementar (ANS). Para atender às questões de segurança e à privacidade da informação, o Manual do CFM estabelece dois níveis distintos de proteção, sendo um básico e outro mais profundo, dependendo do risco do sistema de registro eletrônico de saúde associado. Os requisitos de segurança requeridos dependem do nível de proteção, abrangendo controle de versão do software, identificação e autenticação do usuário, controle de sessão do usuário, autorização e controle de acesso, disponibilidade, comunicação remota, segurança de dados, auditoria, documentação, certificação digital, assinatura digital, autenticação de usuário utilizando certificado digital e digitalização de documentos.

Há também leis e outras resoluções que tem a informação como elemento critico, como exemplo, aquelas sobre violação de segredo profissional, divulgação de segredo e violação de sigilo funcional do Código Penal e também o Código de Ética Medica do Conselho Federal de Medicina (CFM).

2.3.2 Sistemas de Registro Eletrônico de Saúde (S-RES)

O Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde do SBIS/CFM apresenta algumas de definições importantes para a Informática em Saúde. Cabe destacar as seguintes definições:

- Registro Eletrônico de Saúde – RES – Um repositório de informação a respeito da saúde de indivíduos, numa forma processável eletronicamente.
- Sistemas de Registro Eletrônico de Saúde – S-RES – Sistema para registro, recuperação e manipulação das informações de um Registro Eletrônico de Saúde.

Como se pode observar, estas definições são propositalmente abrangentes. É importante lembrar que um S-RES pode englobar diversos sub-sistemas ou componentes. De acordo com (LEAO, et al, 2008), qualquer sistema que capture, armazene, apresente, transmita ou imprima informação identificada em saúde pode ser considerado como sendo um SRES. Tendo em vista a existência de um grande número de S-RES no mercado brasileiro, englobando uma ampla faixa de sistemas focados em diferentes nichos do mercado de saúde, não seria possível, num primeiro momento, certificar em segurança todo e qualquer S-RES existente.

Além dos componentes que implementam as funcionalidades de um S-RES (componente principal), em geral desenvolvido pela empresa terceirizada, podem existir componentes acessórios sobre os quais "dependerá a implementação de diversas funcionalidades do sistema. Exemplos típicos são o sistema de gerenciamento de base de dados (SGBD), um componente dinâmico WEB (*applet* ou *activeX*), ou ainda um sistema de diretórios (ex. AD, LDAP, etc.) utilizado para armazenar parâmetros dos usuários, papeis e grupos. Um S-RES é o conjunto de todos estes subsistemas e módulos que são necessários para atender os requisitos especificados no manual de certificação do SBIS/CFM" (LEAO *et al*., 2008).

2.3.2.1 Categorias dos Sistemas de Registro Eletrônico de Saúde

O Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde do SBIS/CFM apresenta as seguintes categorias dos sistemas de registro eletrônico de saúde conforme a seguir:

- **Assistencial** – sistemas voltados para a assistência, ou seja, todo o S-RES que registra atendimentos em saúde, tais como: sistemas de automação de consultórios clínicos, sistemas de informação hospitalar e ambulatorial, sistemas de vigilância epidemiológica etc.;
- **SADT** – sistemas de apoio diagnóstico e terapêutica, tais como: automação de laboratório, emissão de laudos, imagens médicas e outros;
- **GED** – sistemas de gerenciamento eletrônico de documentos, utilizados para o armazenamento e visualização de documentos relacionados à informação de saúde;
- **TISS** – criada para atender ao padrão TISS da ANS, especialmente aqueles em uso por operadoras de planos de saúde e prestadores de assistência em saúde, que são obrigados a trocar informações usando o padrão TISS.

Qualquer organização de saúde que queira obter o selo SBIS/CFM deve fazer uma solicitação formal à SBIS para dar início ao processo de certificação Neste momento, a pessoa ou organização interessados deverão indicar em quais categorias o seu sistema se enquadra.

Sistemas voltados para consultórios médicos se enquadram apenas na categoria Assistencial, mas um grande sistema hospitalar integrado pode apresentar características e funcionalidades que atendam não apenas à categoria Assistencial, mas também às categorias SADT, GED e ainda TISS. Neste caso, pode-se solicitar certificação em todas as categorias.

2.3.3 Troca de Informação em Saúde Suplementar (TISS)

O padrão para Troca de Informação em Saúde Suplementar (TISS) é o padrão definido pela Agência Nacional de Saúde Suplementar - ANS para registro e intercâmbio de dados entre operadoras de planos privados de assistência à saúde e prestadores de serviços de saúde. O objetivo do padrão TISS é permitir a compatibilidade e interoperabilidade funcional e

semântica entre os diversos sistemas independentes para fins de avaliação da assistência à saúde (caráter clínico, epidemiológico ou administrativo) e seus resultados, orientando o planejamento do setor (LEÃO *et al*., 2008).

O padrão TISS se divide em quatro categorias: conteúdo e estrutura, representação de conceitos em saúde, comunicação, e segurança e privacidade, conforme descrevem as resoluções normativas publicadas no sítio da ANS[2].

A ANS determinou que as normas técnicas estabelecidas na resolução do Conselho Federal de Medicina e os requisitos do Nível de Garantia de Segurança do Manual de Certificação para Sistemas de Registro Eletrônico em Saúde devem obrigatoriamente ser observados no padrão TISS (LEÃO *et al.*, 2008).

A não aderência às especificações, aos requerimentos e aos controles normatizados pode expor as organizações a riscos operacionais que podem desdobrar em danos físicos, materiais, financeiros e de vidas humanas. A próxima Seção visa examinar o tema de gestão de riscos da informação e sua relação com a gestão e operação para o segmento de saúde brasileiro.

2.4 Gestão de Riscos da Informação na Área de Saúde

De acordo com a publicação especial *Risk Management Guide for Information Technology Systems* do NIST (*National Institute of Standards and Technology*), o termo risco de informação é definido em função da probabilidade de uma determinada fonte de ameaça explorar uma potencial vulnerabilidade e resultar em impacto adverso na organização (GARY *et al.*, 2003).

Dentro do ciclo do Sistema de Gestão de Segurança da Informação – SGSI, o processo de avaliação de riscos é o passo no qual os riscos são identificados, avaliados e um conjunto dos controles e objetivos de controles da ISO/IEC 27002:2005 são identificados e aplicados. (Anexo A).

---

[2] Fonte: http://www.ans.gov.br/portal/site/_hotsite_tiss/f_materia_21227.htm

O processo de avaliação e gestão de riscos é especificado na série de normas ISO/IEC TR 13335 (*Management of Information and Communications Technology Security* – MICTS); na norma ISO 31000:2009 que apresenta um processo da gestão de riscos corporativos e, também, na norma ABNT NBR ISO/IEC 27005:2008 (Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação). Os riscos de segurança da informação na área de saúde são endereçadas na norma ISO 27799:2008, específica para esse segmento.

2.4.1 Riscos de Segurança da Informação na Área de Saúde

De acordo com a norma ISO 27799:2008, existem algumas diferenças no que concerne à proteção de S-RES quando comparados com outros sistemas de TI (Tecnologia da Informação) em outros ambientes de negócios. Por exemplo, à medida que muitos bancos ou empresas podem fechar suas operações em um evento de desastre natural ou falha de TI, uma instalação de saúde como hospital, em geral necessita permanecer aberto, prestando os serviços de cuidados médicos e assistenciais. A operação sob condições adversas é essencial para prestar os serviços de cuidados aos pacientes, e para restaurar e manter a saúde da comunidade em um evento de desastre.

Embora a continuidade das operações no segmento de saúde seja um elemento puramente operacional por que a continuidade é inerente ao tipo de serviços prestados (KOVACICH, 2006), ela é um elemento essencial em segurança à medida que segurança inclui a proteção da confidencialidade, integridade e disponibilidade das informações de saúde.

A seguir são apresentados alguns exemplos e cenários que descrevem riscos emergentes de segurança da informação na área de saúde. Esses cenários foram apontados no relatório *Information Security Risk Management for Healthcare Systems* do *Joint Security and Privacy Commitee do International Medical Informatics*, em 2007. Muitos riscos apontados impactam diretamente na proteção da privacidade dos pacientes. A falha em não proteger a privacidade pode violar a regulação do setor (exemplo. HIPAA nos Estados Unidos e Código Civil no Brasil).

Os cenários de riscos descritos a seguir têm o objetivo de descrever e elucidar situações reais ocorridas em organizações de saúde, e indicam que esses riscos de segurança da informação, quando ocorrem, podem ter um impacto significativo na privacidade das informações dos pacientes ou na continuidade da prestação dos serviços de assistência ou cuidados médicos.

Cenário de risco 1 - Falha localizada na de rede comunicações

Uma falha localizada na rede de comunicações de um hospital pode desconectar a sala de emergência (Pronto Atendimento) da rede principal. Dessa forma, os serviços básicos de sistemas de TI poder ficar indisponíveis (exemplo: enderaçamento, roteamento, autenticação de usuários etc.) enquanto os pacientes continuam a chegar ao Pronto Atendimento em busca de serviços críticos de saúde. Os sistemas S-RES do Pronto Atendimento precisam continuar a disponibilizar serviços críticos de saúde.

Cenário de risco 2 – Desastre de grandes proporções

Tais desastres poderiam ser naturais (exemplo: terremoto, tsunami, furacão, vulcão ou incêndio) ou ter causas humanas (exemplo: terrorismo, guerra ou falha de fornecimento de energia elétrica). Durante a ocorrência de riscos assim, a infraestrutura geral (redes, estradas, fornecimento de energia e água) pode ser afetada e ficar indisponível. O desastre pode ainda causar danos às instalações de saúde e poderia destruir dados e informações levando, os sistemas de saúde à falência.

Cenário de risco 3 – Vírus de software de computador

Um equipamento médico é utilizado no paciente (exemplo:, X-ray, ultrasom, ECG – eletrocardiograma, CT – tomografia computadorizada, MRI – imagem de ressonância magnética, PET- tomografia de emissão de pósitrons) quando um software malicioso (vírus de computador) ataca. Isso pode acontecer como conseqüência de um *cyber* ataque de grandes proporções quando os dispositivos médicos não são o alvo. Esses ataques são conhecidos como vírus, cavalos de tróia ou vermes. Mesmo durante essas circunstâncias, os sistemas S-RES devem ser capazes de proteger as informações dos pacientes. Um ataque pode levar ao vazamento de dados pessoais dos pacientes e comprometer seriamente a integridade e a confidencialidade dessas informações criticas.

Cenário de risco 4 – Ataque direcionado e financiado

Em um ataque direcionado e financiado, geralmente, o atacante é alguém de fora de organização de saúde e seus objetivos são as informações médicas de pessoas famosas como atletas e celebridades. Deve-se considerar também que informações médicas de políticos importantes podem ter valor para uso político. Os sistemas S-RES como alvo não são diferentes de outros sistemas de negócios que contém informações confidenciais, sensíveis e criticas. Entretanto, comparado com a inconveniência temporária de ter que trocar a senha caso algum sistema seja invadido, o efeito do vazamento uma informação médica privada (exemplo: câncer, situação de HIV) pode nunca ser desfeito e pode causar conseqüências financeiras e sociais a paciente e à organização responsável pelas S-RES em questão.

Cenário de risco 5 – Ataques cometidos por pessoas internas à organização

Um risco pode surgir de colaboradores internos mal intencionados (empregados, terceiros e até mesmo pacientes da organização de saúde). De acordo com a pesquisa recente realizada pelo Ponemon Institute (PONEMON INSTITUTE LLC, 2009), a maioria desses ataques vem de dentro das organizações. Essas pessoas têm a intenção de cometer um dano proposital a alvos específicos dentro da instalação de saúde. Esses ataques não são sofisticados em termos de conhecimento sobre os sistemas explorados, mas seus impactos são sérios à medida que a integridade e confidencialidade das informações dos pacientes estão expostas.

Cenário de risco 6 – Vulnerabilidades técnicas nos equipamentos de TI

Um determinado componente técnico da plataforma de um sistema médico (S-RES) é identificado como tendo uma vulnerabilidade conhecida que pode ser explorada por atacantes. Essas vulnerabilidades técnicas geralmente são de conhecimento público e estão disponíveis na Internet, nos sítios dos fabricantes ou em fóruns específicos.

Os riscos explorados nos cenários apresentados aqui devem ser gerenciados por meio de Sistema de Gestão de Segurança da Informação, descrito na norma ISO 27799:2008. A seguir são apresentados os principais conceitos concernentes à avaliação de riscos de segurança da informação no segmento de saúde.

2.4.2 Avaliação de Riscos da Informação na Área de Saúde

Tanto a norma ISO/IEC 27001:2005 (Tecnologia da informação – Técnicas de segurança – Sistemas de gerenciamento da segurança da informação – Requisitos) quanto a norma ISO/IEC 27005:2008 ((Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação)) definem os componentes da análise e gerenciamento de risco como:

- Identificação dos ativos de negócio, ameaças e vulnerabilidades;
- Avaliação de impacto nos negócios;
- Probabilidade de ameaça e avaliação de vulnerabilidade;
- Determinação dos níveis de risco;
- Identificação dos controles de segurança recomendados;
- Comparação com controles existentes, permitindo identificação de áreas de risco residual;
- Opções para tratamento de risco, incluindo: gerenciamento direto, aceitação de risco, evasão, transferência gerenciada, etc.;
- Planos de avaliação e tratamento de risco;
- Mapeamento de decisões tomadas contra a lista de controles da norma ISO/IEC 27002.

Além dos componentes mencionados, é importante também estabelecer um entendimento da dependência dos processos operacionais sobre serviços de TI, hardware, software, mídia e localização. Sem este entendimento, seguindo a análise de impacto nos negócios, não é possível entender os cenários de falha que podem levar à indisponibilidade das informações e sistemas. Os gestores das áreas de sistemas da área de saúde serão beneficiados pelos processos orientados a identificar riscos e cenários de falhas na infra-estrutura, nos dispositivos médicos e de TI.

A área de saúde é uma área com consideráveis obrigações de conformidade (tanto legal quanto profissional) e responsabilidades de gestão de risco, portanto, convém que um processo sistemático de governança seja estabelecido para permitir a aderência e eficiência dos requerimentos de conformidades.

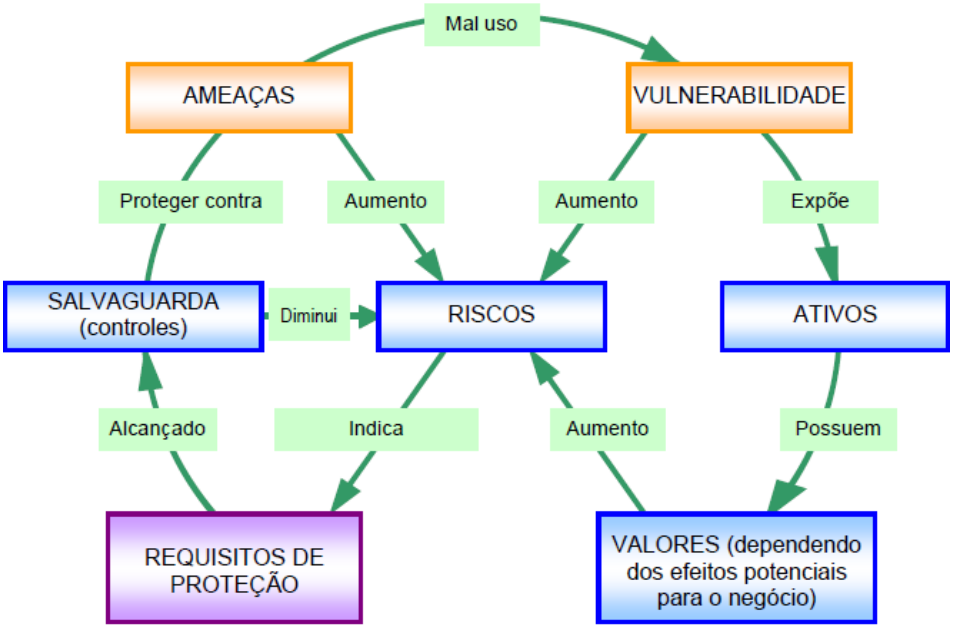

Figura 2 – Relação entre risco e fonte do risco em um modelo de risco simplificado
Fonte: ISO, 2008

O risco é composto por relacionamentos de causa entre diversas fontes de risco (GARY *et al*., 2003). A

Figura **2** apresenta o relacionamento entre riscos e fontes de riscos, conforme especificado na norma ISO 27799:2008, tornando claro que o valor de um risco é determinado a partir dos valores dos ativos de informação, das ameaças e das vulnerabilidades dos ativos ao seu redor.

A crescente interconexão de sistemas de informação da área de saúde torna o gerenciamento de riscos especialmente desafiador nesta área. As organizações da área de saúde não podem agir como se seus sistemas estivessem isolados em ilhas de informação, mas sim, entendendo que eles fazer parte de um sistema complexo de fluxo de informações. Os riscos precisam ser identificados e tratados apropriadamente.

2.4.3 Tratamento de Riscos

A norma Australiana AS/NZ 4360:2004 (Gestão de Riscos - diretrizes para a Implementação) introduziu o processo de tratamento de risco, conceito também abordado pela norma ISO/IEC 27001:2005. O termo “tratamento de risco” destaca a atividade de reduzir o risco a níveis aceitáveis. O processo de tratamento de risco introduzido na norma traz consigo os conceitos de ameaça, transferência ou tolerância em relação aos riscos. Organizações da área de saúde precisam definir e documentar seus critérios para a adequada aceitação ou mitigação de seus riscos. Os fatores a serem levados em conta para aceitação dos riscos são numerosos e variados, mas os fatores a seguir devem ser considerados para inclusão de acordo com a norma ISO 27799:2008:

- Setor de saúde, indústria e padrões organizacionais: refere-se ao tipo de organização e padrões organizações já adotados.
- Clínica ou outras prioridades: refere-se a qualquer fator clínico avaliado por um especialista.
- Adequação cultural: refere-se ao aspecto cultural da organização no que tange adesão das pessoas aos processos.
- Reação do paciente: refere-se ao aspecto de possíveis impactos aos serviços prestados a pacientes da organização.
- Custo: esse fator refere-se a aspecto financeiro para custear a implantação dos processos e controles de mitigação ou aceitação dos riscos.
- Efetividade: refere-se a correta avaliação da eficiência das decisões tomadas relacionados às estratégias de riscos.
- Tipo de proteção: refere-se aos tipos de proteção de segurança da informação adotadas para mitigar um determinado risco.

Estes fatores, avaliados em conjunto, podem resultar em uma relação aceitável de custo *versus* benefícios e podem servir de base, se necessário, para a busca de financiamento para implementar os processos de gestão de risco.

Uma tomada de decisão, usualmente pela alta administração da organização, de não implementar um determinado controle e não liberar investimento para tal, em particular ou por completo é inteiramente válido, mas convém que seja formalmente registrado para revisão

periódica e reavaliação. As organizações da área de saúde devem documentar riscos aceitos, conforme normatização a ser apresentada na Seção a seguir.

2.5 Normas de Segurança da Informação para o Setor de Saúde

O objetivo deste capítulo é apresentar o conjunto de normas internacionais e nacionais que regem o tema de segurança da informação junto às organizações de saúde. Todas as normas apresentadas neste capítulo aplicam-se a todos os tipos de organizações, com exceção da norma ISO 27799:2008, que se destina exclusivamente ao segmento de saúde.

2.5.1 Norma ISO/IEC 27002:2005

A norma ISO/IEC 27002:2005 (Código de Prática para a Gestão de Segurança da Informação) tem como objetivo "estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização". Anteriormente esta norma era conhecida como ISO/IEC 17799, mas a partir de 2005 a nova edição da ISO/IEC 17799 foi incorporada ao novo esquema de numeração como ISO/IEC 27002:2005.

A norma ISO/IEC 27002:2005 fornece um *checklist* padrão de objetivos de controle em 11 áreas, contendo um total de 39 categorias principais de segurança, cada uma com uma descrição de um ou mais controles de segurança. O Anexo A apresenta a relação completa de todos os objetivos de controle, categorias e descrição da norma ISO/IEC 27002.

A abordagem geral adotada pela ISO/IEC 27002:2005 é encorajar cada organização a considerar e interpretar o padrão dentro de seu próprio contexto, requisitos legais e de negócios. Experiências obtidas em muitos países incluindo Austrália, Canadá, França, Holanda, Nova Zelândia, África do Sul e no Reino Unido têm mostrado a necessidade de certas cláusulas de controle e categorias de controle nos quais as informações pessoais de saúde necessitam estar seguras (HUMPHREYES, 2007).

As seguintes seções fazem parte da norma ISO/IEC 27002:2005:

Política de segurança da informação de saúde: Contempla normas para definição de uma política de segurança da informação na organização de saúde.

Organizando a segurança da informação: Contém recomendações sobre como atribuir responsabilidades no gerenciamento da segurança da informação e sua infra-estrutura na organização de saúde. Também prescreve a necessidade de manter a segurança dos ativos e informações acessados por prestadores de serviço e a segurança quando o processamento é responsabilidade de terceiros.

Gestão de ativos: Contém recomendações sobre classificação e controle dos ativos da organização de saúde. Propõe que as informações sejam classificadas de forma a permitir um nível adequado de proteção.

Segurança em recursos humanos: Contém recomendações para redução dos riscos de erro humano, fraude ou uso indevido das instalações de saúde. Propõe que os usuários sejam treinados nos procedimentos de segurança e uso correto das instalações.

Segurança física e do ambiente: Esta seção contém recomendações para prevenção de acesso não autorizado, danos e interferência às informações, instalações físicas e equipamentos da organização de saúde.

Gerenciamento das operações e comunicações: Possui recomendações para garantir a operação segura dos recursos de processamento da informação, minimização do risco de falhas dos sistemas (por meio do planejamento e aceitação dos sistemas), e proteção contra a vulnerabilidade dos softwares. Também propõe proteção das informações armazenadas em rede, e transmitidas por meio de mídias removíveis ou por meios de comunicação entre organizações.

Controle de acesso: Possui recomendações para controlar o acesso à informação, prevenindo acessos não autorizados nos sistemas de saúde. A norma abrange a proteção aos recursos computacionais, aplicações, rede e trabalho remoto. Também propõe a monitoração do uso e acesso aos sistemas.

Desenvolvimento e manutenção de sistemas: Por meio dos controles desta seção, a norma recomenda que a segurança de informação seja parte integrante dos requisitos do sistema de informação de saúde, propondo o uso de técnicas para criptografia de informações.

Também recomenda o controle para segurança dos programas em ambiente de produção e controle de mudanças.

Gestão da continuidade do negócio: Esta seção possui recomendações para evitar a interrupção das atividades e proteger os processos mais críticos contra efeitos de falhas significativos.

Conformidade: Esta seção possui recomendações para evitar violação de leis, contratos e requisitos de segurança. O objetivo é garantir a conformidade dos sistemas com as políticas e normas de segurança da organização. A norma propõe a utilização ou criação de ferramentas para controle de auditorias de sistema.

As organizações que desejam implementar a norma ISO/IEC 27002:2005 em ambientes da área de saúde verificarão que a maioria dos objetivos de controle é aplicada em quase todas as situações. Entretanto, usuários dessa norma na área de saúde também precisam reconhecer situações em que objetivos de controle adicionais podem ser necessários.

2.5.2 Norma ISO/IEC 27001:2005

Segundo a Organização Internacional de Padronização (*International Organization for Standardization* - ISO), padrão é um documento estabelecido por consenso e aprovado por um grupo reconhecido, que estabelece para uso geral e repetido um conjunto de regras, protocolos ou características de processos com o objetivo de ordenar e organizar atividades em contextos específicos para o benefício de todos.

A norma internacional ISO/IEC 27001:2005 foi elaborada baseada na norma inglesa BS7799-1. Ela apresenta um padrão para o estabelecimento, implementação, funcionamento, acompanhamento, revisão, manutenção e melhoria de um Sistema de Gestão de Segurança da Informação (SGSI) documentado no contexto dos riscos de negócio de uma determinada organização (KOVACICH, 2006). Esse padrão pode ser aplicado em todos os tipos de organizações como, por exemplo, empreendimentos comerciais, agências governamentais, organizações sem fins lucrativos, hospitais etc.

Esta norma é adotada para o estabelecimento de estratégias de segurança pela organização e pode ser usada para avaliar a conformidade pelas partes interessadas internas e externas (ISO/IEC, 2005a). O SGSI proposto pela norma assegura a seleção de controles de segurança adequados e proporcionados para proteger os ativos de informação e propiciar confiança às partes interessadas. Todos os controles de segurança recomendados pela norma ISO/IEC 27001:2005 são detalhados na norma ISO/IEC 27002:2005.

A ISO/IEC 27001:2005 introduz o conceito de um Sistema de Gestão de Segurança da Informação – SGSI, e descreve a necessidade de um *framework* detalhado de controles para alcançar os objetivos de segurança apresentados como relevantes pela avaliação de risco, como também, especifica um ciclo sistêmico de processos em uma organização, junto com a identificação e interações destes processos.

A norma ISO/IEC 27001:2005 incorpora o ciclo sistêmico *Plan-Do-Check-Act* (PDCA), que é adotado em toda a estrutura dos processos do Sistema de Gestão de Segurança da Informação. O ciclo PDCA apóia-se no ciclo de melhoria contínua que consiste em planejar (*Plan* – P), fazer (*Do* – D), verificar (*Check* – C) e agir (*Act* – A). O ciclo PDCA é uma ferramenta importante para a análise e melhoria dos processos organizacionais, contribuindo para a tomada de decisões gerenciais e para o alcance das metas e objetivos porque apresenta processos estruturados para a organização que deseje implementá-los (FERREIRA *et al*., 2006).

2.5.3 Norma ISO 27799:2008

A norma internacional ISO 27799:2008 (Informática em saúde – Gestão de segurança da informação em saúde usando ISO/IEC 27002:2005) baseia-se na experiência obtida nos esforços internacionais em lidar com a segurança de informação pessoal de saúde e é um documento associado à ISO/IEC 27002:2005 e à ISO/IEC 27001:2005. Não é sua intenção suplantar a ISO/IEC 27002:2005 ou a ISO/IEC 27001:2005. A norma ISO 27799:2008 trata das peculiaridades específicas do setor de saúde no âmbito da segurança das informações. Ela fornecer guias de implementação da norma ISO/IEC 27001:2005 e ISO/IEC 27002:2005, portanto, fornece as melhores práticas internacionais para o setor de Saúde.

A norma ISO 27799:2008 fornece orientação às organizações de saúde e a outros custodiantes de informações pessoais de saúde sobre a melhor maneira de proteger a confidencialidade, a integridade e a disponibilidade de tais informações pessoais de saúde por meio da implementação da norma ISO/IEC 27002:2005. Especificamente, esta norma internacional endereça as necessidades especiais de gerenciamento da segurança do setor de saúde e seus ambientes operacionais diferenciados. Enquanto a proteção e a segurança da informação pessoal de saúde são importantes para todos os indivíduos, corporações, instituições e governos, há requisitos específicos do setor de saúde que precisam ser cumpridos para assegurar a confidencialidade, a integridade, a auditabilidade e a disponibilidade da informação pessoal de saúde.

A informação pessoal de saúde é considerada a mais confidencial de todos os tipos de informação pessoal (ISO, 2008), e garantir a confidencialidade é essencial pois a privacidade do paciente precisa ser mantida. A integridade da informação de saúde deve ser protegida para assegurar a segurança do paciente, e um componente importante desta proteção é assegurar que todo o ciclo de vida da informação seja completamente auditável. A disponibilidade da informação de saúde, por sua vez, também é crítica para a entrega efetiva dos serviços de cuidados de saúde. Sistemas informatizados de saúde devem satisfazer exigências únicas para permanecerem operacionais mesmo na ocorrência desastres naturais, falhas de sistemas e ataques de negação de serviço. Garantir a confidencialidade, a integridade e a disponibilidade da informação de saúde requer especialização específica do setor de saúde (ISO, 2008)

A efetiva Gestão de Segurança da Informação em Saúde se torna cada vez mais necessária pelo uso crescente de redes sem fio (*wireless*) e tecnologias de internet no fornecimento de serviços de saúde. Se não forem implementadas corretamente, estas tecnologias complexas poderão aumentar os riscos à confiabilidade, integridade e disponibilidade da informação de saúde.

Não obstante o tamanho, a posição e o modelo do fornecimento de serviços, todas as organizações de saúde precisam ter controles rígidos implantados para proteger a informação de saúde confiada a elas. Contudo, muitos profissionais de saúde trabalham em consultórios ou clínicas de pequeno porte em que faltam recursos voltados para gerenciar a segurança da informação. Portanto, as organizações de saúde devem ter orientação clara, concisa, e específica de saúde na seleção e na implementação de controles de segurança da informação.

Esta orientação deve ser adaptável a qualquer tamanho, localização, e tipos diferentes de serviço disponibilizados pelas instituições de saúde.

Finalmente, com aumento da troca eletrônica da informação de pacientes entre profissionais de saúde, há um benefício em adotar uma referência comum para a gerência de da informática de saúde. Esta norma internacional ISO 27799:2008 baseia-se na experiência obtida em esforços nacionais e internacionais em lidar com a segurança de informação pessoal de saúde e é um documento associado à ISO/IEC 27002:2005. Esta norma aplica a norma ISO/IEC 27002:2005 no domínio da área de saúde de forma a considerar cuidadosamente a aplicação apropriada de controles de segurança para os propósitos de proteção de informação pessoal de saúde.

Figura 3 a seguir apresenta o relacionamento da norma ISO 27799:2008 com as normas ISO/IEC 27002:2005 e ISO/IEC 27001:2005.

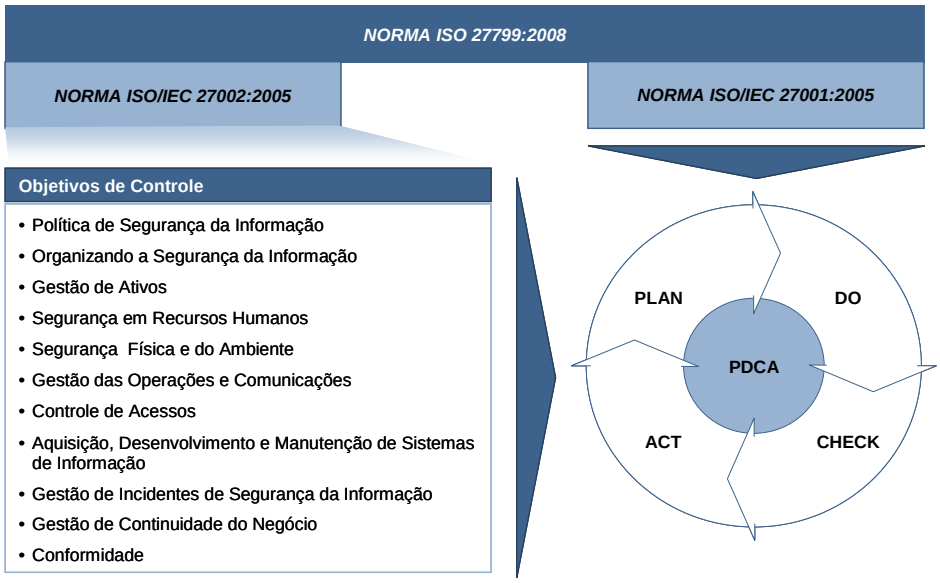

Figura 3 – Relacionamento das normas ISO 27799:2008, ISO/IEC 27001:2005 e ISO/IEC 27002:2005
Fonte: Resultado da pesquisa

O relacionamento apresentado na Figura 3 mostra que os objetivos de controle de segurança da informação que são descritos na norma ISO/IEC 27002:2005 suportam a implementação da norma ISO 27799:2008 no ambiente de saúde, ao mesmo tempo em que a norma ISO/IEC 27001:2005 apresenta um ciclo (planejar/fazer/verificar/agir) sistêmico de gestão (apresentado na Seção 2.5.4), que quando implementados e seguidos, conduzem a uma execução robusta de um Sistema de Gestão da Segurança da Informação para a organização de saúde.

2.5.4 Sistema de Gestão de Segurança da Informação (SGSI)

As subseções 6.4 a 6.7 da norma ISO 27799:2008 fornecem o direcionamento para estabelecer e operar um Sistema de Gestão de Segurança da Informação (SGSI) em um ambiente da área de saúde. Isto requer seguir um ciclo de atividades, como ilustrado na Figura 8 também conhecido como fluxo PDCA.

A norma ISO 27799:2008 incorpora o ciclo *Plan-Do-Check-Act* (PDCA), que é adotado em toda a estrutura dos processos do SGSI, conforme pode ser visualizado na Figura 4.

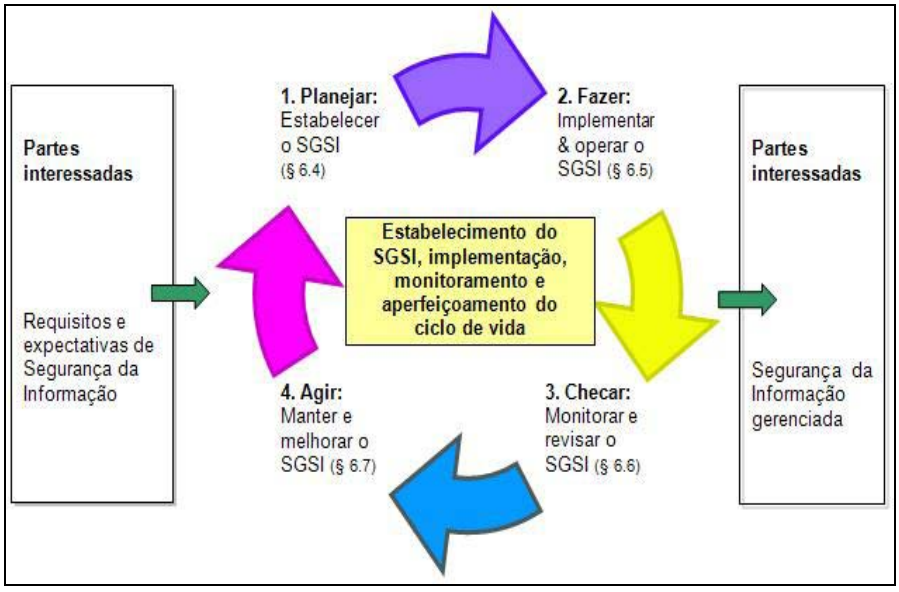

Figura 4 – Sistema de Gestão de Segurança da Informação (SGSI)

Fonte: ISO, 2008

A necessidade de garantir a confidencialidade, integridade e disponibilidade das informações faz com que as organizações estabeleçam um Sistema de Gestão de Segurança da Informação (HERRERA, 2005). Um SGSI é uma maneira de proteger e de gerenciar as informações a partir de uma abordagem de riscos do negócio, que estabelece, implementa, monitora, revisa, mantém e melhora a segurança da informação (HANASHIRO, 2007).

O desenvolvimento de um SGSI não é uma tarefa fácil (DEY, 2007). As organizações devem analisar e projetar os meios de assegurar a segurança para manter a continuidade dos negócios. Processos necessários devem ser definidos para proteger os ativos da informação e políticas e procedimentos de segurança devem ser estabelecidos.

No desenvolvimento de um processo de SGSI deve ser aplicado um conjunto adequado de controles tais como políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware (HANASHIRO, 2007). Esse conjunto de controles de segurança é suportado por normas e guias de segurança. A efetividade de um SGSI desenvolvido por uma organização está condicionada à efetividade dos controles de segurança da informação disponíveis (HERRERA, 2005). Sem a implementação adequada dos controles ou sem o apoio das normas de segurança, um SGSI pode não atender às necessidades de segurança organizacionais.

Um erro comumente cometido, especialmente por organizações públicas da área de saúde onde tipicamente não há requisitos centrais para credenciamento ou certificação formais de segurança da informação, é descrever a conformidade com a ISO/IEC 27001 como sendo uma questão de adoção de uma *checklist*. Para estarem verdadeiramente em conformidade, as organizações precisam ser capazes de demonstrar um SGSI operacional, no qual há processos apropriados de conformidade.

Na Figura 4, o objetivo do processo “Fazer” é implementar e operar a política, controles, processos e procedimentos do SGSI. O objetivo do processo “Verificar” é avaliar e verificar, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.

Finalmente, o objetivo do processo “Agir” é executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

2.6 Resumo da Fundamentação Teórica

Os princípios fundamentais que norteiam a segurança das informações em qualquer organização são os princípios da confidencialidade, da integridade e da disponibilidade das informações que constituem parte dos ativos mais valiosos e críticos das organizações do setor de saúde em particular.

A base de um modelo de gestão de segurança das informações é formada pelo tripé de processos, pessoas e tecnologias. A fim de reduzir as vulnerabilidades inerentes às pessoas no que diz respeito ao tratamento das informações críticas da organização, as políticas e um sistema de classificação de informações precisa ser estabelecido e comunicado para a comunidade de pessoas que compõem a organização. Um sistema de classificação de informações definido, publicado e presente nas decisões das pessoas permite que elas arbitrem seguramente sobre a criticidade das informações de pacientes ou clínicas que se deparam e manipulam. Políticas claras, definidas e comunicadas orientam sobre as diretrizes e responsabilidades sobre essa prática, levando as pessoas a seguirem processos padrões e a protegerem os ativos de informação mais importante.

No contexto operacional das organizações de saúde (hospitais, laboratórios, clinicas, etc.) as informações apresentam níveis de criticidade complexos e variados em função da própria complexidade das tecnologias e dos processos utilizados na operação e gestão dos cuidados com os pacientes. Nesse contexto, requisitos específicos são elaborados para endereçar os riscos e as peculiaridades das informações sobre pacientes que suportam a decisão de médicos, enfermeiros e outros agentes que operam nessas organizações.

O setor de saúde apresenta desafios inerentes aos seus processos e ambiente, pois a quebra dos princípios fundamentais de confidencialidade, de integridade e de disponibilidade pode desdobrar em perdas maiores e até, em casos extremos, levar pessoas à morte.

Um ecossistema regulador composto de resoluções, de normas e de padrões circunda o entorno do segmento de saúde e atua sob os mais diversos processos e atores da cadeia de gestão e operação de saúde no Brasil. No que tange à segurança das informações, foram publicadas resoluções específicas para os sistemas de registros eletrônicos de pacientes, com o objetivo de categorizar, classificar e determinar o nível de criticidade desses sistemas.

Tais resoluções também especificam elementos de controles mínimos e mitigadores de riscos para a proteção e cuidados com as informações de pacientes em sistemas eletrônicos. O ambiente regulatório complexo entre varias entidades e os processos, somados a uma miríade de riscos inerentes às informações no ambiente de saúde permitiu que fosse desenvolvida a norma internacional ISO 27799:2008, que visa estabelecer processos padrões para a efetiva gestão de segurança das informações na organização de saúde.

Nos próximos capítulos desse trabalho são estudados e examinados os elementos que compõem essa norma, bem como, a análise de quais elementos principais permitem a manutenção e a perenidade de um sistema de gestão de segurança contínuo nas organizações de saúde do Brasil.

3. PROCESSOS DE SEGURANÇA DA INFORMAÇÃO

O objetivo deste capítulo é identificar e examinar os processos para implementação e manutenção de um sistema de segurança da informação em organizações de saúde com base na norma ISO 27799:2008.

3.1 Processos de Implementação de Segurança da Informação em Saúde

Os processos de implementação de segurança da informação em saúde são aqueles processos derivados do ciclo PDCA de um Sistema de Gestão de Segurança da Informação, notadamente os processos “Planejar e Estabelecer o SGSI” e “Monitorar e Revisar o SGSI”.

De acordo com a norma ISO/IEC 27001:2005, o objetivo do processo “Planejar e Estabelecer” do ciclo PDCA, é estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação, para produzir resultados de acordo com as políticas e objetivos de uma organização.

“Planejamento” é essencial para o sucesso de qualquer projeto (CALDER, 2009). Para fins de desenvolvimento deste trabalho, os processos do ciclo de gestão do SGSI escolhidos para análise foram os processos “Planejar e Estabelecer o SGSI” e “Monitorar e Revisar o SGSI”.

De acordo com o *Project Management Institute* (PMI), o processo de planejamento e o de manutenção são os mais importantes e críticos no ciclo de gestão porque eles garantem que as atividades sejam definidas, seqüenciadas e executadas de acordo com o cronograma e qualidade.

Os principais processos a serem examinados estão descritos a seguir:

1. Definir o escopo do SGSI
2. Conduzir o *gap analysis*
3. Definir a política do SGSI
4. Analisar os riscos do SGSI
5. Selecionar os controles para o SGSI

6. Declarar a aplicabilidade

Os processos são examinados tomando como ponto de partida os processos de implementação e manutenção do ciclo PDCA, e também, são analisados de acordo com os seguintes critérios empregados pelo *Project Management Institute* (PMI) para descrição de processos e atividades:

- Identificação do **objetivo** do processo: esse critério visa identificar e documentar o objetivo que processo pretende atingir;
- E**ntradas** para do processo: esse critério visa pesquisar as principais entradas (por exemplo: saídas de outros processos) para um determinado processo;
- Levantamento das **atividades** do processo: esse critério visa definir as atividades que compõem o processo ou subprocesso;
- **Ordenamento:** esse critério via agrupar as atividades no mesmo nível de detalhe, identificar as principais áreas envolvidas e estabelecer a sequência das atividades;
- **Saídas** do processo: esse critério visa pesquisar as principais saídas do processo;

O primeiro processo a ser examinado é o processo “definir o escopo do SGSI”, por se tratar do processo que inicia todo ciclo PDCA e é critico porque a organização necessita definir antes os limites que se deseja prover à segurança da informação.

3.1.1 Definir o escopo do SGSI

O processo “definir o escopo do SGSI” é um dos seis processos-chave para o sucesso do SGSI. É um processo crítico porque a organização de saúde precisa conhecer e definir antes as fronteiras organizacionais e os ativos para planejar a implementação de segurança, e também porque é um dos requerimentos da norma ISO 27799:2008.

Quadro 2 – Definição de escopo do SGSI

Processo 1 – Definir o escopo do SGSI		
Objetivo:		
Definir o escopo e os limites do SGSI nos termos das características da organização de saúde, a organização, sua localização, ativos e tecnologia, incluindo detalhes e justificativas para quaisquer exclusões do escopo.		
Entradas	Atividades/Ferramentas	Saídas
1. Requerimentos legais de segurança, regulatórios e normativos da organização de saúde 2. Inventário dos ativos de informação de saúde a proteger 3. Definição dos limites (abrangência) da organização e do S-RES 4. Análise das características da organização de saúde, da localização, dos ativos e das tecnologias	5. Técnicas de *Delphi* (análises das características da organização de saúde, da localização, dos ativos e das tecnologias) 6. Técnicas de *brainstorm* e debates com a gerência 7. Aplicação de questionário, realização de entrevistas e revisão de documentos de entrada	8. Documento de definição e declaração formal escopo 9. Documento com detalhes e justificativas de exclusão de escopo 10. Base de dados de inventário de ativos

Fonte: Resultado da pesquisa

O objetivo do processo “definir o escopo do SGSI” é definir o escopo e os limites do SGSI nos termos das características da organização de saúde, a organização, sua localização, ativos e tecnologia, incluindo detalhes e justificativas para quaisquer exclusões do escopo (ISO/IEC, 2005a, p. 4). Este processo apresenta as seguintes entradas, atividades, ferramentas e saídas, conforme descritos a seguir:

1. **Requerimentos legais de segurança, regulatórios e normativos da organização de saúde**: Estes requerimentos derivam da regulamentação geral para o segmento de saúde e são referenciados no Capítulo 2.3 do presente estudo. Tais requerimentos permitem estabelecer o foco sobre quais sistemas e informações os requerimentos poderão trazer impacto legal ou normativo direto. Os critérios para definição do escopo de conformidade vêm do conjunto de requerimentos identificados e analisados pela organização de saúde.
2. **Inventário dos ativos de informação de saúde a proteger**: O processo de definição de escopo é um processo difícil porque muitas vezes a complexidade da organização dificulta da localização desses ativos. O inventário dos ativos é essencial para a organização de saúde porque permite identificar quais ativos

físicos ou de informações do S-RES pretende-se proteger e quais não serão protegidos antes de se decidir quais são as proteções apropriadas.

3. **Definição dos limites (abrangência) da organização e do S-RES**: A norma ISO/IEC 27001:2005 requer que seja identificado e explicitado o que está fora do escopo do SGSI, bem como, que seja justificada essa exclusão. Isso tem o objetivo de garantir que durante a implementação do processo obtenha-se visibilidade dos limites (CALDER, 2009). Como exemplo de definição de limite, podemos citar "os sistemas de TI que suportam o S-RES".
4. **Análise das características da organização de saúde, da localização, dos ativos e das tecnologias**: Nesta atividade são analisadas todas as entradas do processo utilizando técnicas que permitam envolver outros departamentos da organização para contribuir com a decisão do escopo de SGSI.
5. **Técnicas de Delphi**: O método Delphi é um método que permite obter consenso entre os membros do projeto. É um metodo sistemático e interativo de estimativa que se baseia na experiência independente de vários membros de um processo ou projeto. Os membros são cuidadosamente selecionados pela sua experiência e respondem a um questionário em um ou mais ciclos. Após cada ciclo, um facilitador provê um sumário anônimo das estimativas de cada membro no ciclo, bem como as razões sobre as quais cada um baseou sua estimativa. (PMI, 2004, p. 248)
6. **Técnicas de *brainstorm* e debates com a gerência**: De acordo com o *Project Management Institute*, "*brainstorm*" é uma técnica para coletar informações dentre vários membros de equipes multidisciplinares na organização (PMI, 2004, p. 110);
7. **Aplicação de questionário, realização de entrevistas e revisão de documentos de entrada**: Essas são atividades executadas no processo que devem ser conduzidas pela organização.
8. **Documento de definição e declaração formal escopo**: Documento gerado com detalhes do escopo das informações pessoais de saúde a serem protegidas. Tal documento é parte integrante do sistema de gestão e pode ser submetido a auditorias no processo "CHECK" do ciclo do SGSI.
9. **Documento com detalhes e justificativas de exclusão de escopo**: Este documento registra detalhes sobre quais ativos estão fora do escopo do SGSI e

suas respectivas justificativas. Esse documento é parte integrante do sistema de gestão e está sujeito a auditorias durante a fase do ciclo “CHECK” do SGSI.

10. **Base de dados de inventário de ativos**: Essa base de dados (pode ser uma planilha eletrônica ou uma outra base estruturada de informações) é uma relação dos ativos lógicos e físicos que compõem o sistema S-RES e que faz parte do escopo do SGSI a ser protegido.

3.1.2 Conduzir o *gap analysis*

Uma vez tendo estabelecido o escopo, o próximo estágio do processo é conduzir o *gap analysis*, no qual uma avaliação é realizada para comparar o atual estado dos controles de segurança com o estado desejado dos controles de segurança. O foco do *gap analysis* reside na responsabilidade, na implementação, na documentação e na evidência de existência de controles. Isto é claramente consistente com as práticas na área de saúde nas quais habilidades, registros e procedimentos apropriados são importantes. (ISO, 2008, p. 19).

A realidade é que muitas organizações de saúde que desejam implementar um SGSI já possuem um determinado número mínimo de controles de segurança da informação aplicados (exemplo: senhas, cópias de segurança etc.) (CALDER, 2009). Os processos do SGSI necessitam garantir que os controles que já existem sejam adequados e apropriados e que controles adicionais requeridos pela norma sejam implementados, ou seja, uma análise do “*gap*” do que existe implementado e o que será requerido, que deverá ser realizada.

Quadro 3 – Conduzir o *gap analysis*

Processo 2 - Conduzir o *gap analysis*		
Objetivo:		
Realizar uma análise do “gap” com objetivo de identificar os controles de segurança já existentes na organização de saúde (ou S-RES) e os controles que serão requeridos para o SGSI.		
Entradas	Atividades/Ferramentas	Saídas
1. Inventário dos ativos de informação de saúde a proteger 2. Documento de definição e declaração formal escopo	3. Realizar análise de *gap bottom-up* 4. Ferramenta de produtividade (software) para *gap analysis*	5. Matriz de análise de *gaps*

Fonte: Resultado da pesquisa

O objetivo do processo “conduzir o *gap analysis*” é realizar uma análise do “*gap*” (lacuna) para identificar os controles de segurança já existentes na organização de saúde (ou no S-RES) e os controles que são requeridos para o SGSI (ISO/IEC, 2005a, p. 5). Este processo apresenta as seguintes entradas, atividades, ferramentas e saídas conforme descritos a seguir:

1. **Inventário dos ativos de informação de saúde a proteger**: Esta entrada do processo é o mesmo inventário já realizado na entrada do processo 1.2 durante a definição do escopo. O inventário permite que a análise tenha como foco somente os ativos relevantes para proteção dentro da organização de saúde.
2. **Documento de definição e declaração formal escopo**: Esta entrada do processo é o mesmo documento já produzido na saída do processo 1.7 durante a definição do escopo. A declaração de escopo do SGSI permite que a análise tenha como foco somente dentro dos limites definidos no sistema.
3. **Realizar análise de *gap bottom-up*:** A análise *bottom-up* baseia-se em levantar informações em todos os controles existentes na organização e depois verificar se eles estão adequados ou não, e também verificar contra os requerimentos de controles previstos na norma ISO/IEC 27002:2005 e listados no Anexo A desse trabalho.
4. **Ferramenta de produtividade (software) para *gap analysis*:** Existem ferramentas de *software* que servem como ferramentas de produtividade para realizar a análise de *gap* de forma automatizada. Essas ferramentas ajudam a organização a tomar uma abordagem estruturada e sistemática para a análise gerando resultados mais consistentes.
5. **Matriz de análise dos gaps**: Matriz (planilha ou saída da ferramenta automatizada) com a lista de todos os controles já implementados na organização (de acordo com o escopo) e se estão ou não adequados de acordo com os requerimentos da declaração de aplicabilidade e dos requerimentos de controle.

O resultado do *gap analysis* também permite sugerir uma classificação inicial das prioridades para implementar os controles requeridos.

Uma declaração formal de escopo precisa ser produzida nesse processo e convém que a declaração seja divulgada amplamente dentro da organização pelo gestor do SGSI, com

objetivo de comunicar a alta gerência da organização sobre o escopo formal da segurança. É essencial que a declaração do escopo defina a fronteira da atividade de conformidade em termos de pessoas, processos, lugares, plataformas e aplicações.

No caso das organizações da área de saúde, convém que esta declaração seja amplamente divulgada, revisada, e adotada pela área de comunicação da organização, de clínicas e consultórios e grupos de governança corporativa. É importante documentar também de que forma o escopo definido vem ao encontro aos interesses da organização de saúde em buscar aderência aos aspectos legais e regulatórios sobre a proteção e segurança das informações pessoais de saúde.

3.1.3 Definir a política do SGSI

De acordo com a norma ISO 27799:2008, a política do SGSI é considerada um documento maior da política de segurança da informação. Estas políticas podem estar descritas em um único documento a ser produzido nesse processo.

Quadro 4 – Definir política do SGSI

Processo 3 - Definir a política do SGSI		
Objetivo:		
Definir uma política do SGSI com as características da organização de saúde, sua localização, seus ativos e tecnologia que compõem o S-RES e estabelecer o Fórum de Gestão de Segurança da Informação da organização de saúde.		
Entradas	Atividades/Ferramentas	Saídas
1. Requerimentos legais de segurança, regulatórios e normativos da organização de saúde 2. Representantes da organização de saúde: TI, RH, auditoria, Qualidade	3. Alinhar com o contexto estratégico de gestão de riscos da organização de saúde 4. Estabelecer o Fórum Gestão de Segurança da Informação da organização de Saúde 5. Submeter a aprovação da Gerência da organização de saúde	6. Política de segurança do SGSI 7. Aprovação da Gerência da organização de saúde. 8. Fórum FGSI estabelecido

Fonte: Resultado da pesquisa

O objetivo do processo “definir a política do SGSI” é definir uma política do SGSI com as características da organização de saúde, sua localização, seus ativos e a tecnologia que

compõem o S-RES e estabelecer o Fórum de Gestão de Segurança da Informação da organização de saúde (ISO/IEC, 2005a, p. 7). Este processo apresenta as seguintes entradas, atividades, ferramentas e saídas conforme descritos a seguir:

1. **Requerimentos legais de segurança, regulatórios e normativos da organização de saúde:** Estes requerimentos derivam da regulamentação geral para o segmento de saúde e estão referenciados no Capítulo 2.3 desse estudo. Tais requerimentos permitem estabelecer o foco sobre quais sistemas e informações de saúde as requerimentos trazem impacto legal ou normativo direto. Os critérios para definição da política do SGSI conformidade advêm do conjunto requerimentos identificados que norteiam a organização de saúde.
2. **Representantes da organização de saúde: TI, RH, auditoria, Qualidade**: Esta entrada se refere a representantes da organização de vários departamentos (*cross* organizacional e *cross* funcional) que compõem o escopo do SGSI. A partir de técnicas de *brainstorm* (conforme citado no processo 1) é possível estimular e chegar a consenso sobre as políticas internas.
3. **Alinhar com o contexto estratégico de gestão de riscos da organização de saúde:** As políticas de segurança devem estar alinhadas com o perfil de riscos da organização de saúde. Esse perfil de risco é determinado no processo “analisar riscos do SGSI”.
4. **Estabelecer o Fórum Gestão de Segurança da Informação da organização de Saúde:** De acordo com a norma ISO 27799:2008, um Fórum de Gestão de segurança da informação (FGSI) apropriado para a organização de saúde deve ser estabelecido para supervisionar e administrar a segurança da informação. Estruturar o fórum pode ser desafiador, com muitos pontos de vista de *stakeholders* a serem considerados e obrigações regulatórias a serem cumpridas. Enquanto as funções do FGSI não puderem ser delegadas ou dispersadas sem a perda de efetividade, a criação do FGSI não pode ser tida como um mandato para criar ‘ainda mais um comitê’. A fim de explorar sinergias entre os departamentos, é melhor ampliar o foco de um comitê já existente na organização, como um que endereça riscos ou é responsável pela governança da informação, para que o mesmo lidere o FGSI.
5. **Submeter a aprovação da Alta Gerência da organização de saúde**: A política de segurança é a força motriz do SGSI (CALDER, 2009, p. 53). Ela deve ser um

documento pequeno que deve incorporar o direcionamento da alta gerência, realidade organizacional, atender os requerimentos legais (entrada 1) como também os requerimentos da Norma. A alta gerência da organização de saúde deve endossar e apoiar a política, portanto, a política deve ser emitida e comunicada em nome de sua autoridade.

6. **Política de segurança do SGSI**: Documento final e resumido que deve incorporar o direcionamento da alta gerência, a realidade organizacional, atender os requerimentos legais como também os requerimentos da Norma ISO 27799:2008.
7. **Aprovação da Alta Gerência da organização de saúde**: Aprovação final alta gerência da organização de saúde.
8. **Fórum FGSI estabelecido:** Fórum constituído com respectivos membros e atas das reuniões registradas.

O fórum precisa cobrir a abrangência das funções de segurança e governança da informação, assim como representantes das diferentes comunidades de usuários e representantes das funções-chave de suporte. Representantes de Recursos Humanos e Auditoria Interna também devem estar presentes.

A partir uma abordagem de governança da informação, a natureza crítica da segurança da informação é enfatizada e também permite um processo integrado na organização, com a inserção da análise de risco, que diretamente alimenta também o processo de governança clínica. Uma vez definida a política, o próximo passo é analisar os riscos de segurança da informação que expõem a organização de saúde e as informações de seus pacientes.

3.1.4 Analisar os riscos do SGSI

A proposta para o processo “analisar os riscos do SGSI” tem o objetivo de identificar e avaliar os riscos de segurança da informação da organização de saúde dentro do escopo determinado pelo SGSI.

A norma ISO/IEC 27001:2005 e a norma ISO/IEC 27005:2008 definem os elementos de análise de riscos como sendo os seguintes:

1. Identificar os ativos dentro do escopo definido do SGSI e os proprietários destes ativos.
2. Identificar as ameaças para os ativos dentro do escopo definido do SGSI e os proprietários e usuários destes ativos.
3. Identificar as vulnerabilidades que podem ser exploradas pelas fontes de ameaças aos ativos dentro do escopo definido do SGSI.
4. Identificar e avaliar os impactos que as perdas de confidencialidade, integridade e disponibilidade podem causar aos ativos dentro do escopo definido do SGSI.
5. Avaliar a probabilidade real da ocorrência de impactos aos ativos dentro do escopo do SGSI.
6. Estimar os níveis de risco da organização dentro do escopo definido do SGSI.

Neste estudo, os elementos do macro processo “analisar os riscos do SGSI” propostos pelas normas ISO/IEC 27001:2005 e ISO/IEC 27005:2008 são especificados nas próximas Seções em subprocessos detalhados, com as respectivas entradas, atividades e saídas pesquisadas em várias referências bibliográficas. É fundamental salientar que a efetiva avaliação de risco de segurança da informação na área de Saúde requer a disponibilidade das seguintes habilidades e conhecimentos de pessoas que devem realizar a análise:

- Conhecimento de processos clínicos e de enfermagem, incluindo protocolos e caminhos do cuidado;
- Conhecimento dos formatos de dados clínicos e a capacidade de uso impróprio destes dados;
- Fatores do ambiente externo que podem exacerbar ou diminuir os níveis de qualquer ou de todos os componentes de risco descritos previamente;
- Características de atributos e desempenho ou falha de dispositivos médicos e de TI;
- Conhecimento sobre histórias de incidentes e cenários de impacto de casos atuais;
- Conhecimentos detalhados de arquiteturas de sistemas; e
- Familiaridade com programas de gerenciamento de mudanças que possam modificar qualquer ou todos os níveis dos componentes de risco.

A avaliação de risco é apenas um meio para alcançar um objetivo e não pode ser um objetivo por si próprio, embora freqüentemente termine desta maneira (HANASHIRO, 2007).

Isto é verdadeiro especialmente em ambientes com limitação de recursos, tais como encontrados em diversas organizações da área de saúde. O gerenciamento de riscos responde à avaliação identificando quais controles podem ser implementados, quais já estão e quais controles adicionais a organização precisa implementar para reduzir o nível de risco residual a um nível aceitável.

A seguir são apresentados e detalhados os subprocessos que foram identificados em várias fontes e referências mencionadas e que são propostos para analisar os riscos do SGSI em saúde.

3.1.4.1 Identificar os ativos do SGSI

O objetivo do subprocesso descrito no Quadro 5 é identificar os ativos dentro do escopo definido do SGSI e os proprietários destes ativos (ISO, 2008).

Quadro 5 – Subprocesso para identificar os ativos

Processo 4 – Analisar os riscos do SGSI		
Sub processo 4.1: Identificar os ativos		
Objetivo: Identificar os ativos dentro do escopo do SGSI e os proprietários destes ativos (ISO 27799:2008)		
Entradas	Atividades/Ferramentas	Saídas
1. Documento de definição e declaração formal escopo 2. Lista de usuários do sistema S-RES 3. Lista de hardware 4. Lista de software 5. Interfaces do sistema S-RES (ex. conectividade interna e externa) 6. Dados e informações de saúde 7. Missão do sistema: 8. Crititicidade do sistema e dos dados.	9. Aplicar questionário 10. Realizar entrevistas 11. Revisar documentos de entrada 12. Utilizar ferramenta automatizada de auditoria	13. Matriz de ativos identificados 14. Detalhamento dos sistemas de TI que compõem o S-RES 15. Delineamento das fronteiras (limites) dos sistemas

Fonte: Resultado da pesquisa

1. **Documento de definição e declaração formal escopo**: Esta entrada do processo é o mesmo documento já produzido na saída do processo 1.7 durante a definição do escopo. A declaração do escopo do SGSI permite que a análise tenha como foco somente os limites definidos no sistema.

2. **Lista de usuários do sistema S-RES**: Lista contendo os nomes dos usuários que utilizam o sistema S-RES, bem como os nomes das pessoas que fazem a manutenção e suporte ao sistema (GARY *et al*., 2003, p. 10).
3. **Lista de hardware**: Lista detalhada com o inventário dos equipamentos de TI que compõem a infraestrutura do sistema S-RES (GARY *et al*., 2003, p. 10).
4. **Lista de software**: Relação detalhada e atualizada de todos os softwares que compõem a solução S-RES com suas respectivas versões e atualizações aplicadas (GARY *et al*., 2003, p. 10).
5. **Interfaces do sistema S-RES (Ex.: conectividade interna e externa)**: Desenho em alto nível das interfaces e conexões lógicas do S-RES para troca de informações. Todas as conectividades lógicas internas e externas devem ser possíveis de serem visualizadas nessa documentação. O padrão TISS foi criado pela ANS, especialmente para as operadoras de planos de saúde e prestadores de assistência em saúde, que são obrigados a trocar informações usando o padrão TISS.
6. **Dados e informações de saúde**: Sãos dados e informações de saúde conforme descritos no referencial teórico no Capítulo 2, Seção 2.2.1, desse estudo.
7. **Missão do sistema: (ex. prover cadastro de atendimento na clínica médica)**: Documento de declaração de missão do sistema S-RES. Por exemplo: prover cadastro de atendimento na clínica médica.
8. **Crititicidade do sistema e dos dados**: Documento com o nível de valor e importância do sistema S-RES em relação à integridade, confidencialidade e disponibilidade de informações.
9. **Aplicar questionário**: Esse questionário pode ser distribuído e aplicado a todo pessoal técnico e não técnico (exemplo: enfermeiros, clínica médica, etc.) que especificam, que apoiam e que utilizam o sistema S-RES. Esse questionário também pode ser utilizado para entrevista em visita a setores internos da organização de saúde.
10. **Realizar entrevistas**: Entrevistas com as pessoas que utilizam, apoiam e operam o sistema S-RES devem ser realizadas para identificar informações e ativos. Ex:. como o sistema é operado e mantido. As visitas para entrevistas também permitem coletar informações sobre as condições de segurança física do ambiente.

11. **Revisar documentos de entrada**: Nesta atividade todos os documentos de entrada deste subprocesso são revisados a fim de identificar quaisquer ativos físicos ou de informações do sistema S-RES.
12. **Utilizar ferramenta automatizada para auditoria**: Métodos proativos e técnicos de inventário dos ativos podem ser utilizados. Como exemplo, uma ferramenta de software para mapeamento de rede pode identificar os serviços que são executados nos servidores do sistema S-RES.
13. **Matriz de ativos identificados**: A principal saída deste subprocesso é uma matriz completa e detalhada, identificando todos os ativos e tipos identificados que compõem o S-RES.
14. **Detalhamento dos sistemas de TI que compõem o S-RES**: Todos os itens identificados nesse subprocesso, como usuários do sistema, arquitetura do sistema, topologia de rede do sistema, interfaces do sistema e fluxo de informações etc.
15. **Delineamento das fronteiras (limites) dos sistemas**: Documento que descreve os limites e as fronteiras do sistema com o objetivo de manter o controle sobre os ativos e informações identificados de acordo com o escopo definido do S-RES.

A identificação dos ativos que são valiosos para organização é uma atividade crítica e exaustiva no processo (CALDER, 2009, p. 58). Ao final do processo é importante certificar-se que todos os ativos identificados estão dentro do escopo do SGSI, da política de segurança do SGSI e registrados no sistema de inventários de ativos da organização de saúde.

Uma vez identificados os ativos da organização, o subprocesso seguinte é a identificação das ameaças para esses ativos de acordo com o escopo definido.

3.1.4.2 Identificar as ameaças do SGSI

Após a identificação dos ativos no subprocesso anterior, prossegue-se com a identificação das ameaças para cada ativo. De acordo com Gary *et al.* (2003, p. 12), uma ameaça é o potencial de uma fonte de ameaça específica (iniciado acidentalmente ou intencionalmente) suceder ao explorar uma vulnerabilidade específica. O objetivo do subprocesso descrito no Quadro 6 é identificar as ameaças para cada ativo identificado.

Quadro 6 – Subprocesso para identificar as ameaças

Processo 4 – Analisar os riscos do SGSI		
Sub processo 4.2: Identificar as ameaças		
Objetivo: Identificar as ameaças para os ativos dentro do escopo do SGSI e os proprietários e usuários destes ativos (ISO/IEC 27001:2005)		
Entradas	Atividades/Ferramentas	Saídas
1. Matriz de ativos identificados 2. Identificar fontes de ameaças 3. Identificar as motivações 4. Detalhamento dos sistemas de TI que compõem o S-RES 5. Histórico de ataques internos e externos ao sistema S-RES 6. Dados de agências de inteligência 7. Notícias na imprensa	8. Identificar as ameaças	9. Matriz das ameaças identificadas que podem explorar as vulnerabilidades nos ativos do SGSI de saúde

Fonte: Resultado da pesquisa

A seguir é apresentada uma descrição detalhada das entradas, ferramentas e saídas deste subprocesso:

1. **Matriz de ativos identificados**: A principal entrada para este subprocesso é uma matriz detalhada com a identificação de todos os ativos e tipos que compõem o S-RES. Podem ser necessárias também as saídas do processo 4.1: “detalhamento dos sistemas de TI que compõem o S-RES” e “delineamento das fronteiras (limites) dos sistemas”.
2. **Identificar fontes de ameaças**: O objetivo dessa atividade é identificar as potenciais fontes de ameaças e compilar uma matriz que lista as fontes de ameaças e que são aplicáveis aos sistemas de TI e que compõem o S-RES em avaliação. De acordo com Calder (2009), uma fonte de ameaça é definida como qualquer circunstância ou evento com o potencial de causar um dano ao sistema de TI. As fontes de ameaças mais comuns podem ser de ordem natural, humana ou do ambiente.
3. **Identificar as motivações**: Realizar o mapeamento das motivações, recursos e competências que são necessários para realizar um ataque “com sucesso” pelos potencias atacantes. Essa atividade vem em seguida à identificação das fontes de ameaças e contribui para a identificação da probabilidade.
4. **Detalhamento dos sistemas de TI que compõem o S-RES**: Essa é a saída do subprocesso anterior 4.1 e constitui todos os itens identificados naquele subprocesso, tais como usuários do sistema, arquitetura do sistema, topologia de rede do sistema, interfaces do sistema e fluxo de informações etc.

5. **Histórico de ataques internos e externos ao sistema S-RES**: Essa atividade refere-se a levantar os incidentes de segurança ocorridos no passado na organização de TI Tais incidentes podem ser coletados na área de suporte de TI, abertura e atendimento de chamados, relatórios de auditorias internas, *logs* e registros de sistemas operacionais ou de redes.
6. **Dados de agências de inteligência:** São dados que podem ser coletados em agencias de inteligência e de segurança da informação. Geralmente esses dados e relatórios de pesquisas são divulgados periodicamente. Exemplo: Polícia Federal, CERT.BR - Centro de Estudos, Resposta e Tratamento de Incidentes, *SecurityFocus* etc.
7. **Notícias na imprensa**: São informações na forma de notícias, sobre ameaças que podem ser coletadas em sítios de notícias especializados em segurança da informação. Essas notícias podem revelar incidentes de segurança da informação que estão ocorrendo nas organizações, e permitem, a partir da análise desses incidentes, identificar as ameaças que podem impactar nos sistemas de TI.
8. **Identificar as ameaças**: Esse é o processo principal de identificação, avaliação e documentação (matriz) de todas as ameaças ao S-RES. Com base nas entradas identificadas, uma análise criteriosa deve ser realizada usando técnicas de *brainstorm* com algumas pessoas nomeadas entre os departamentos da organização de saúde.
9. **Matriz das ameaças identificadas que podem explorar as vulnerabilidades nos ativos do SGSI de saúde**: A principal saída desse subprocesso é uma matriz de ameaças identificadas e que podem explorar as vulnerabilidades nos ativos do S-RES da organização de saúde.

As ameaças estão sempre presentes nos sistemas e ativos de uma organização porque tais ativos apresentam valor, portanto, podem apresentar valor também para um outro elemento externo à organização. As situações identificadas de ameaças devem ser tratadas com confidencialidade dentro da organização de saúde.

O Anexo B do presente trabalho apresenta uma visão geral das várias ameaças humanas, suas motivações e os métodos ou ações pelas quais elas podem se manifestar. Essa informação poderá ser útil para auxiliar na modelagem deste subprocesso, como trabalho futuro.

Uma vez mapeadas as ameaças aos ativos da organização, o subprocesso a seguir propõe a identificação das vulnerabilidades para esses ativos, de acordo com o escopo definido.

3.1.4.3 Identificar as vulnerabilidades do SGSI

O objetivo do subprocesso exibido no Quadro 7 a seguir é mapear uma lista das vulnerabilidades identificadas (falhas ou deficiências) nos ativos ou sistemas do escopo do SGSI e que podem ser exploradas por potenciais fontes de ameaças. De acordo com Gary *et al*. (2003, p. 15), vulnerabilidade é uma falha ou deficiência nos procedimentos de segurança, no desenho, na implementação ou nos controles que podem ser explorados (acidentalmente ou intencionalmente), sendo o resultado uma quebra de segurança ou violação da política de segurança do sistema.

Quadro 7 – Subprocesso para identificar as vulnerabilidades

Processo 4 – Analisar os riscos do SGSI		
Sub processo 4.3: Identificar as vulnerabilidades		
Objetivo: Identificar as vulnerabilidades que podem ser exploradas pelas fontes de ameaças aos ativos dentro do escopo do SGSI. (ISO/IEC 27001:2005)		
Entradas	Atividades/Ferramentas	Saídas
1. Matriz de ativos identificados 2. Detalhamento dos sistemas de TI que compõem o S-RES 3. Delineamento das fronteiras (limites) dos sistemas 4. Relatórios de análise de riscos anteriores 5. Relatório de auditoria interna ou externa 6. *Checklist* de requerimentos de segurança 7. Relatório de testes automatizados anteriores (ex. *penetration test*) 8. Questionário para aplicação de teste do NIST SP 800-53 - *Guide for Assessing the Security Controls in Federal Information Systems - Building Effective Security Assessment Plans*), disponível em: http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf	9. Aplicar questionário 10. Realizar entrevistas 11. Revisar documentos de entrada 12. Utilizar ferramenta de busca automatizada de vulnerabilidades técnicas (ex. *scanners nessus*, disponível em http://www.nessus.org/nessus/)	13. Matriz com a lista de vulnerabilidades no sistema S-RES que podem ser exploradas pelas fontes de ameaças.

Fonte: Resultado da pesquisa

A seguir é apresentada uma descrição detalhada das entradas, ferramentas e saídas deste subprocesso:

1. **Matriz de ativos identificados**: A principal entrada para esse subprocesso é uma matriz detalhada identificando todos os ativos e tipos identificados que compõem o S-RES. Podem ser necessárias também as saídas do processo 4.1 respectivamente: “detalhamento dos sistemas de TI que compõem o S-RES” e “delineamento das fronteiras (limites) dos sistemas”.
2. **Detalhamento dos sistemas de TI que compõem o S-RES**: Essa é a saída do subprocesso anterior 4.1, e constitui todos os itens identificados naquele subprocesso, tais como usuários do sistema, arquitetura do sistema, topologia de rede do sistema, interfaces do sistema e fluxo de informações etc.
3. **Delineamento das fronteiras (limites) dos sistemas**: Essa é a saída do subprocesso 4.1 anterior e se refere a todos os itens identificados naquele subprocesso, que delimitam as fronteiras do S-RES.
4. **Relatórios de análise de riscos anteriores**: Toda fonte documental de vulnerabilidades identificadas no ambiente TI, como relatórios de análises de riscos, relatórios de auditorias anteriores, relatórios de anomalias de sistemas, relatórios de revisão de segurança e relatórios de testes e avaliação dos sistemas (GARY *et al*., 2003).
5. **Relatório de auditoria interna ou externa**: Toda fonte documental de vulnerabilidades identificadas no ambiente TI, como relatórios de auditorias anteriores internas e externas realizadas anteriormente (GARY *et al*., 2003).
6. ***Checklist* de requerimentos de segurança**: Essa é uma lista para verificação de vulnerabilidades a partir de uma base de dados pública conhecida, como exemplo, a *National Vulnerability Database*, NIST I-CAT disponível em http://icat.nist.gov.
7. **Relatório de testes automatizados**: Relatório de testes de vulnerabilidades automatizados realizados anteriormente no ambiente de TI do S-RES.
8. **Questionário**: Um questionário para aplicação de teste de vulnerabilidades do NIST SP 800-53 (*Guide for Assessing the Security Controls in Federal Information Systems - Building Effective Security Assessment Plans*), disponível em http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf.
9. **Aplicar questionário**: Aplicar o questionário de teste de vulnerabilidade durante as sessões de identificação de vulnerabilidades junto aos donos dos sistemas de TI que compõem o S-RES.

10. **Realizar entrevistas**: Realizar entrevistas junto aos gestores internos e entre as áreas e departamentos da organização de saúde, conforme identificadas no escopo, com objetivos de identificar vulnerabilidades percebidas por esses gestores e donos de sistemas.
11. **Revisar documentos de entrada**: Revisar todos os documentos e informações de entrada desse processo para garantir que a análise seja realizada com suficiência de fonte de informações e a qualidade da avaliação.
12. **Utilizar ferramenta**: Deve-se considerar a utilização de ferramentas automatizadas (software de testes) como ferramenta de produtividade, bem como, para garantir a melhor qualidade do resultado avaliação.
13. **Matriz com a lista de vulnerabilidades**: Essa é a principal saída desse processo e refere-se a uma matriz detalhada com a lista de todas as vulnerabilidades identificadas no ambiente do sistema S-RES que podem ser exploradas pelas fontes de ameaças.

As atividades estudadas nesse processo visam identificar todas as potenciais vulnerabilidades de cada ativo para cada fonte de ameaça. As vulnerabilidades podem deixar os sistemas S-RES expostos a ataques das ameaças identificadas. Como exemplo, para a ameaça de incêndio, uma vulnerabilidade seria a presença de material inflamável na sala dos computadores do sistema S-RES.

O Anexo C do presente trabalho de pesquisa apresenta uma visão resumida das vulnerabilidades e suas várias fontes de ameaças. Essa informação pode ser útil para auxiliar na modelagem deste subprocesso em trabalhos futuros.

O subprocesso a seguir visa avaliar os impactos decorrentes das ameaças e vulnerabilidades identificadas por meio de magnitudes qualitativas ou quantitativas.

3.1.4.4 Avaliar os impactos

O objetivo deste subprocesso é identificar e avaliar possíveis impactos que a exploração bem sucedida das vulnerabilidades pelas ameaças terá sobre a disponibilidade, a confidencialidade e a integridade das informações e ativos de saúde (e dos pacientes). Todos

esses impactos devem, sempre que possível, ter associados um valor monetário, usando faixas de valor monetário (exemplo: menor que 10 mil, entre 10 mil e 50 mil, maior que 50 mil) que reflita o tamanho da organização de saúde e o custo total (direto e indireto) do incidente (CALDER, 2009, p. 59). O **Error! Reference source not found.** a seguir apresenta as entradas, atividades, ferramentas e saídas mapeados para este subprocesso.

Quadro 8 – Subprocesso para avaliar os impactos

Processo 4 – Analisar os riscos do SGSI		
Sub processo 4.4: Avaliar os impactos		
Objetivo: Identificar e avaliar os impactos que as perdas de confidencialidade, integridade e disponibilidade podem causar aos ativos dentro do escopo do SGSI. (ISO/IEC 27001:2005)		
Entradas	Atividades/Ferramentas	Saídas
1. Relatório BIA (*Business Impact Analysis*) caso exista na organização de saúde 2. Lista de processos realizados pelo sistema S-RES 3. Criticidade do sistema e dos dados. Ex. Nível de valor e importância do sistema S-RES em relação a integridade, confidencialidade e disponibilidade. (*entrada do processo 4.1*)	4. Revisar documentos de entrada 5. Determinar a magnitude dos impactos	6. Matriz com a magnitude de impacto classificados em alto, médioe baixo.

Fonte: Resultado da pesquisa

A seguir é apresentada uma descrição detalhada das entradas, ferramentas e saídas desse subprocesso:

1. **Relatório BIA**: Utilizar aqui o último relatório do processo BIA (*Business Impact Analysis*) realizado na organização. O processo BIA identifica quais processos e ativos da organziação requerem o nível mais alto de proteção; inclui recomendações sobre possíveis estratégias e alternativas de recuperação, como também fornece dados financeiros para ajudar a selecionar os níveis apropriados de investimento para proteção do negócio (KOVACICH, 2006).
2. **Lista de processos**: Mapeamento de todos os processos apoiados pelos sistemas de TI do S-RES. Esses processos podem ser conhecidos pelas áreas usuárias e também pela área de qualidade da organização de saúde.
3. **Criticidade do sistema e dos dados**: Mapeamento e classificação da criticidade, do valor e da importância dos dados (exemplo: informações de pacientes) e sistemas de TI que compõe o S-RES para o suporte aos objetivos da organização de saúde.

4. **Revisar documentos de entrada**: Revisar todos os documentos e informações de entrada desse processo para garantir que a análise de impacto seja realizada com suficiência de fonte de informações e com qualidade satisfatória.
5. **Determinar a magnitude dos impactos**: Realizar a análise detalhada dos dados de entrada para determinar a magnitude de impacto utilizando métodos de quantitativos e qualitativos de avaliação (conforme apresentado no Quadro 9).
6. **Matriz com a magnitude de impacto**: Essa é a principal saída desse processo e refere-se a uma matriz detalhada com a magnitude de impactos classificados por meio dos métodos quantitativos ou qualitativos. As categorias de impactos são sugeridas por Gary *et al*. (2003, p. 9), como sendo: os impactos sob perdas de integridade da informação, perdas de confidencialidade e perda de disponibilidade.

Alguns impactos tangíveis podem ser medidos quantitativamente em perdas financeiras, custo de repor os sistemas ou o esforço requerido para corrigir e restaurar os serviços de saúde interrompidos pelas ameaças. Impactos como: perda de confiança pública, perda de credibilidade e danos ao interesse pela organização de saúde, não podem ser medidos em unidades monetárias, entretanto, podem ser qualificados em termos de magnitude: alto, médio ou baixo.

Para realizar esse subprocesso, deve-se considerar as vantagens e as desvantagens da avaliação quantitativa em contraste com avaliação qualitativa (DEY, 2007). O Quadro 9 apresenta uma sugestão de magnitudes de impactos qualitativa e suas respectivas definições.

Quadro 9 – Magnitude e definição de impactos

Magnitude do impacto	Definição do Impacto
Alta	A exploração da vulnerabilidade pode: (1) resultar em altíssima perda financeira ou de ativos ou recursos; (2) violar significativa, causar danos ou impedir a missão da organização, reputação, imagem ou interesse; (3) resultar em perdas humanas (mortes).
Média	A exploração da vulnerabilidade pode: (1) resultar em perda financeira ou de ativo ou recurso; (2) violar, causar danos ou impedir a missão da organização, reputação ou interesse; (3) resultar em ferimentos humanos.
Baixa	A exploração da vulnerabilidade pode: (1) resultar em alguma perda de ativo tangível ou recurso; (2) afetar a organização de forma perceptível

Fonte: Resultado da pesquisa

Uma vez identificados e analisados os impactos quantitativos e/ou qualitativos, o subprocesso seguinte tem objetivo de avaliar as probabilidades de ocorrência também por meio de um sistema de classificação descrito a seguir.

3.1.4.5 Avaliar a probabilidade da ocorrência de eventos

O objetivo deste subprocesso é avaliar a probabilidade de um evento ocorrer, usando um sistema de classificação definido: uma vez a cada dois anos, uma vez a cada ano, uma vez a cada seis meses etc. (DEY, 2007). Exemplo: um ataque por vírus (software malicioso) pode ser classificado como: uma vez por dia. Dessa forma, permite identificar o nível de risco (alto, médio ou baixo), e então concluir para cada risco, se ele é aceitável ou qual controle é requerido.

O Quadro 10 apresenta de forma detalhada as entradas, as atividades, as ferramentas e as saídas deste subprocesso:

Quadro 10 – Subprocesso para avaliar a probabilidade

Sub processo 4.5: Avaliar a probabilidade		
Objetivo: Avaliar a probabilidade real da ocorrência de impactos aos ativos dentro do escopo do SGSI. (ISO/IEC 27001:2005)		
Entradas	Atividades/Ferramentas	Saídas
1. Matriz de motivação das fontes da ameaças 2. Capacidade das ameaças 3. Natureza das vulnerabilidades 4. Matriz de controles já existentes no S-RES	5. Determinar as probabilidades	6. Matriz de classificação de probabilidades e ocorrências em alto, médio e baixo.

Fonte: Resultado da pesquisa

A seguir é apresentada uma descrição detalhada das entradas, das ferramentas e das saídas desse subprocesso:

1. **Matriz de motivação**: Conforme entrada do processo 4.2 “Identificar as ameaças”, essa matriz contém o mapeamento das motivações, recursos e competências que são necessários para realizar um ataque “com sucesso” pelos potencias atacantes. Essa atividade ocorre em seguida à identificação das fontes de ameaças e ajuda na identificação da probabilidade.

2. **Capacidade das ameaças**: Idem ao item 1, incluindo a análise das capacidades e recursos associados e disponíveis às fontes das ameaças e suas motivações.
3. **Natureza das vulnerabilidades**: Essa é a saída do subprocesso 4.3 “Identificar uma matriz com a lista de vulnerabilidades no sistema S-RES que podem ser exploradas pelas fontes de ameaças” e é uma matriz detalhada, identificando todos tipos de vulnerabilidades identificados ao S-RES.
4. **Matriz de controles existentes**: A fim de se chegar a um índice geral que indica a probabilidade que uma potencial vulnerabilidade pode ser explorada, considerando o ambiente de ameaças, essa entrada identifica os controles já existentes no ambiente de TI do S-RES, que servem para atenuar ou aumentar o índice de probabilidade final.
5. **Determinar as probabilidades**: Essa é a principal atividade deste subprocesso e refere-se a realizar todas as análises com os dados e informações de entrada.
6. **Matriz de classificação de probabilidades**: Essa é a saída principal desse subprocesso e refere-se à produção de uma matriz de classificação das probabilidades e ocorrências em alto, médio e baixo. (GARY *et al*., 2003).

O Quadro 11 exibe os níveis de probabilidade em função das definições de impactos possíveis, de forma a permitir ao avaliador de riscos uma escala para situar as probabilidades e impactos.

Quadro 11 – Nível de probabilidade e suas definições

Nível de Probabilidade	Definição do Impacto
Alto	A fonte de ameaça está altamente motivada e é suficientemente capaz, e os controles para prevenirem as vulnerabilidades de serem exploradas são ineficientes.
Médio	A fonte de ameaça esta motivada e é capaz, entretanto controles estão presentes que podem impedir o sucesso da exploração da vulnerabilidade.
Baixo	Não há motivação para a fonte de ameaça ou competência; os controles estão presentes que impedem que as vulnerabilidades sejam exploradas

Fonte: Resultado da pesquisa

Com as probabilidades de ocorrência devidamente identificadas e avaliadas, é necessária a avaliação dos níveis de riscos que os ativos do ambiente de TI do S-RES estão expostos.

O subprocesso a seguir (estimar os níveis de risco) visa gerar uma estimativa dos riscos considerando os níveis de probabilidades identificados nesse subprocesso.

3.1.4.6 Estimar os níveis de risco

O objetivo deste subprocesso é estimar e avaliar o nível de risco o qual os ativos definidos no escopo do SGSI da organização de saúde estão expostos. A determinação do nível de um risco em função de uma ameaça ou vulnerabilidade em particular pode ser expressada da seguinte forma:

- A probabilidade de uma determinada ameaça explorar uma vulnerabilidade;
- A magnitude do impacto caso a ameaça consiga explorar uma vulnerabilidade;
- A adequação dos controles existentes.

Para avaliar os riscos, uma escala de riscos e uma matriz com os níveis de risco precisam ser desenvolvidos e acordados a fim de possibilitar o entendimento uniforme entre as varias áreas da organização.

O Quadro 12 a seguir apresenta, de forma detalhada, as entradas, as atividades, as ferramentas e as saídas desse subprocesso.

Quadro 12 – Subprocesso para estimar os níveis de risco

Processo 4 – Analisar os riscos do SGSI		
Sub processo 4.6: Estimar os níveis de risco		
Objetivo: Estimar os níveis de risco da organização do escopo do SGSI. (ISO/IEC 27001:2005)		
Entradas	Atividades/Ferramentas	Saídas
1. Matriz de classificação de probabilidades de ocorrência em alto, médio e abaixo. 2. Matriz com a magnitude de impacto classificados em alto,médioe baixo 3. Matriz de controles já existentes no S-RES	4. Estimar níveis de risco	5. Matriz de níveis de risco classificados em alto, médio e baixo.

Fonte: Resultado da pesquisa

A seguir é apresentada uma descrição detalhada das entradas, das atividades, das ferramentas e das saídas desse subprocesso:

1. **Matriz de classificação de probabilidades**: Essa é a saída principal do subprocesso 4.6 “avaliar probabilidades” e refere-se à produção de uma matriz de classificação das probabilidades e ocorrências em alto, médio e baixo (GARY *et al*., 2003).
2. **Matriz com a magnitude de impacto**: Idem ao item 1. A magnitude de impacto esta incluída na matriz principal de classificação de probabilidades
3. **Matriz de controles existentes**: Essa é a entrada do subprocesso anterior 4.6 “avaliar probabilidades”, e refere-se ao mapeamento de todos os controles já existentes no ambiente de TI do S-RES.
4. **Estimar níveis de risco**: Essa é a principal atividade deste subprocesso e refere-se à realização de todas as análises subjetivas com os dados e informações de entrada, a fim de se obter as estimativas quantitativas e qualitativas dos níveis de riscos existentes no ambiente de TI do S-RES.
5. **Matriz de níveis de risco classificados**: Essa é a principal saída desse subprocesso e refere à produção de uma matriz de níveis de risco classificados nas categorias de alto, médio e baixo (GARY *et al*., 2003)..

O Quadro 13 a seguir apresenta as escalas de riscos e ações necessárias. Essa escala pode ser utilizada elaboração da matriz de níveis de risco, conforme a saída 5 do presente subprocesso.

Quadro 13 – Escalas de riscos e ações necessárias

Nível de Risco	Descrição do risco e das ações necessárias
Alto	Se um risco é avaliado como ALTO, então há forte necessidade de medidas corretivas. O sistema existente pode continuar a operar, mas um plano de ação corretivo necessita ser iniciado o mais rápido possível.
Médio	Se um risco é avaliado como médio, então ações corretivas são necessárias um plano necessita ser desenvolvido para incorporar essas ações dentro de um período razoável de tempo.
Baixo	Se um risco é avaliado como BAIXO, então o dono do sistema pode determinar se alguma ação corretiva é necessário ou decidir aceitar o risco.

Fonte: Resultado da pesquisa

O processo “Analisar os riscos do SGSI” foi detalhadamente examinado e desdobrado em seis subprocessos pesquisados e descritos nos itens anteriores.

O próximo processo apresentado é “Selecionar os controles do SGSI”.

3.1.5 Selecionar os controles do SGSI

Os objetivos de controle e os controles devem ser selecionados e implementados para atender aos requisitos identificados pela análise e avaliação dos riscos, como também pelo processo de tratamento de riscos. Esta seleção deve considerar os critérios para aceitação de riscos como também os requisitos legais, regulatórios e contratuais da organização de saúde.

Quadro 14 – Processo para selecionar os controles do SGSI

5 – Selecionar os controles do SGSI		
Objetivo:		
Selecionar os objetivos de controle e os controles para o tratamento dos riscos identificados no processo anterior.		
Entradas	Atividades/Ferramentas	Saídas
1. Norma ISO/IEC 27002:2005 2. Relatório de avaliação dos riscos do SGSI	3. Selecionar os controles	4. Plano de tratamento de riscos

Fonte: Resultado da pesquisa

O objetivo do processo “selecionar os controles do SGSI” é selecionar os objetivos de controle e os controles para o tratamento dos riscos identificados no processo anterior (ISO/IEC, 2005a, p. 8). Este processo apresenta as seguintes entradas, atividades, ferramentas e saídas conforme descritos a seguir:

1. **Norma ISO/IEC 27002:2005**: Os objetivos de controle e os controles da Norma ISO/IEC 27002:2005 devem ser selecionados como parte da entrada deste processo, como adequados para cobrir os requisitos identificados. Os controles listados na norma ISO/IEC 27002:2005 não são exaustivos, e objetivos de controles e controles adicionais podem também ser selecionados. Os usuários da norma ISO 27799:2008 são direcionados para a norma ISO/IEC 27002:2005 como um ponto de partida para a seleção de controles, para assegurar que nenhuma opção de controle importante seja negligenciada.
2. **Relatório de avaliação dos riscos do SGSI**: Somente os controles que estão relacionados e são apropriados devem ser selecionados para os atuais riscos identificados no SGSI da organização, de maneira que não haja um acúmulo desnecessário de controles. A norma ISO/IEC 27002:2005 contém uma lista de todos os controles que podem ser considerados em relação a todo potencial de riscos.

3. **Selecionar os objetivos de controle**: Deve-se selecionar os controles que estão relacionados, são apropriados e proporcionais ao nível atual de riscos que a organização está exposta. A norma ISO/IEC 27002:2005 contém uma lista de melhores práticas de controles que podem ser considerados em relação ao nível de riscos. Alguns controles contidos nessa norma podem não ser necessários na organização.
4. **Plano de tratamento de riscos:** A fim de diferenciar entre o processo de análise de riscos como um todo e o ato de tratar os riscos identificados, a norma Australiana AS/NZ 4360 introduziu o conceito de “tratamento de risco”. Este conceito foi subseqüentemente adotado pela norma ISO/IEC 27001:2005. O rótulo “tratamento de risco” destaca a atividade de reduzir o risco a níveis aceitáveis (reconhecendo que recursos suficientes nunca estarão disponíveis para permitir sequer uma tentativa de completa evasão do risco). O tratamento de risco é particularmente adequado para organizações da área de saúde, trazendo consigo seus conceitos de “ameaça, transferência ou tolerância” em relação às estratégias adotadas frente aos riscos. A definição do que é aceitável é e deve permanecer individual para a organização e seu pessoal. Isto deve refletir o apetite da organização por risco e deve ser utilizado para garantir que os gastos no aperfeiçoamento da segurança da informação sejam justificados e representados de forma demonstrável do bom uso de recursos financeiros escassos.

O processo de análise de riscos está no centro do SGSI (CALDER, 2009, p. 61). Pode-se afirmar que os controles selecionados pela organização estão todos contidos no SGSI. A maioria do esforço dos processos do SGSI é investida no desenho, implantação, teste e revisão de controles apropriados que são destinados a endereçar os riscos identificados. De acordo com Calder (2009, p. 61), os controles são maneiras de gerenciar os riscos, incluindo políticas, procedimentos, guias, práticas ou arranjos organizacionais, que ainda podem ser do tipo administrativo, técnico, gerencial ou de natureza legal.

3.1.6 Declarar a aplicabilidade

O processo de declaração de aplicabilidade pode ser entendido como a elaboração de um resumo executivo do estado da segurança da informação na organização de saúde (de

acordo com o escopo definido), da interpretação da organização quantos aos requisitos de segurança e sobre como implementar os controles de forma mais adequadas.

A Declaração de Aplicabilidade (DA) deve ser mantida por um administrador da organização em nome do Fórum de Gestão de Segurança da Informação (FGSI). Este documento deve ser fornecido às funções de governança corporativa e de clínica para formar uma parte-chave do conjunto de documentações de governança. Seu formato também é tipicamente adaptável para o uso como uma ferramenta de avaliação ou evidência em suporte à auditoria externa, garantia de segurança clínica e outras inspeções regulatórias.

Quadro 15 – Processo para declarar a aplicabilidade do SGSI

6 – Declarar aplicabilidade do SGSI		
Objetivo:		
Elaborar uma declaração de aplicabilidade para o Sistema de Gestão de Segurança da Informação da organização de saúde.		
Entradas	Atividades/Ferramentas	Saídas
1. Matriz de objetivos de controles selecionados 2. Matriz de controles atualmente implementados 3. Matriz de exclusão dos objetivos de controle e controles da norma ISO/IEC 27002	4. Elaborar documento de declaração de aplicabilidade	5. Documento de declaração de aplicabilidade (DA)

Fonte: Resultado da pesquisa

O objetivo do processo “declarar aplicabilidade do SGSI” é elaborar uma declaração de aplicabilidade para o Sistema de Gestão de Segurança da Informação da organização de saúde (ISO, 2008, 25). Este processo apresenta as seguintes entradas, atividades, ferramentas e saídas conforme descritos a seguir:

1. **Matriz de objetivos de controles selecionados:** Os objetivos de controle, os controles selecionados em e as razões para sua seleção.
2. **Matriz de controles atualmente implementados:** Os objetivos de controle e os controles atualmente implementados
3. **Matriz de exclusão dos objetivos de controle e controles da norma ISO/IEC 27002:2005**: A exclusão de quaisquer objetivos de controle e controles da norma ISO/IEC 27002:2005 e a justificativa para sua exclusão

4. **Elaborar documento de declaração de aplicabilidade:** A declaração de aplicabilidade (DA) estará completa somente quando todos os riscos identificados tenham sido avaliados e a aplicabilidade de todos os controles identificados tenham sido considerados e documentados. Em geral, o processo de declaração é iniciado antes que qualquer controle seja implementado e concluído quando o controle final é estabelecido.
5. **Documento de declaração de aplicabilidade (DA):** A Declaração de Aplicabilidade provê um resumo das decisões relativas ao tratamento de riscos. A justificativa das exclusões provê uma verificação cruzada de que nenhum controle foi omitido inadvertidamente

Normalmente, a declaração de aplicabilidade é uma lista de todos os controles identificados na ISO/IEC 27002:2005, junto com uma declaração da existência e ou não daqueles controles, um a um, aplicados na organização de saúde (CALDER, 2009, 65).

Se determinado controle é aplicado, então a DA descreve como ele é aplicado e identifica as políticas e procedimentos inerentes a esse controle. Se determinado controle não é aplicado, então a DA explica por que não é aplicado e provê boas razões.

Tomando como base a norma ISO 27799:2008, estudou-se até o momento, os processos de implementação da segurança da informação em uma organização de saúde. Verificou-se o desdobramento dos processos em vários outros subprocessos necessários e presentes nas implementações da norma ISO/IEC 27001:2005.

Na próxima Seção, os processos examinados são os destinados à manutenção e à perenidade da segurança dentro da organização de saúde.

3.2 Processos de Manutenção da Segurança da Informação

O Sistema de Gestão de Segurança da Informação (SGSI) deve ser monitorado continuamente e revisado ciclicamente. É uma premissa que o monitoramento é parte integrante dos processos de manutenção dos diversos controles identificados durante o processo de implementação do SGSI, os quais, uma vez implementados, podem servir de base

para estabelecer indicadores de acordo com o requisito especificado na seção 4.2.3 da norma ISO 27799:2008.

Conforme mencionado anteriormente, um erro comumente cometido é descrever a conformidade com a norma como sendo uma questão de adoção de um *checklist*. Para estarem verdadeiramente em conformidade, as organizações de saúde precisam ser capazes de demonstrar que um Sistema de Gestão de Segurança da Informação está operacional e que existem processos apropriados de planejamento e manutenção do sistema.

Pode-se afirmar que os processos de análises críticas e as auditorias são processos de refinamento dos controles, ou seja, de forma geral, são ferramentas que o gestor dispõe para demonstrar aderência de seus sistemas de segurança.

Os processos “monitorar e analisar” (*Check*) e “manter e melhorar” (*Act*) são baseados no ciclo do modelo PDCA (*Plan-Do-Check-Act*) da norma ISO/IEC 27001:2005 e compõem a base dos processos de manutenção do sistema de segurança para demonstrar aderência com os controles contidos na norma.

3.2.1 Processos para monitorar e analisar o sistema

A norma ISO 27799:2008 estabelece três processos principais para atender ao processo “*Check*” do ciclo PDCA que são: auditoria externa ou interna, monitoramento e análise crítica.

3.2.1.1 Auditoria externa e interna

Os processos de auditoria podem ser externos ou internos. Uma auditoria interna é uma auto-avaliação, geralmente realizada por um departamento interno da organização de saúde independente, que verifica a adequação, a eficiência e eficácia do sistema de gestão de segurança em relação aos seus objetivos e ao comportamento frente às políticas de segurança definidas em seu escopo.

As auditorias internas são algumas vezes chamadas de auditoria de primeira parte, e são conduzidas pela própria organização interna, com fins específicos internos para viabilizar uma auto-declaração de conformidade da organização de saúde. (BASTOS; CAUBIT, 2009).

A auditoria externa geralmente é realizada por uma organização externa e independente que avalia a existência, a adequação e eficácia dos requisitos da norma, avaliando ou não a aderência à referida norma, que pode resultar em um certificado de aderência, renovável em períodos determinados. As auditorias externas podem ser ainda classificadas como “auditoria de segunda” ou de “terceira parte”, de acordo com os interesses das partes pela organização de saúde (BASTOS; CAUBIT, 2009, p. 124).

As auditorias de segunda parte são aquelas realizadas pelas partes externas que têm um interesse pela organização, tais como clientes. As auditorias de terceira parte são realizadas por organizações externas que fornecem certificados ou registro de conformidade.

São basicamente três os fatores que motivam a necessidade de uma organização realizar uma auditoria em seu sistema de gestão de segurança: a necessidade de compará-lo com o padrão internacional (exemplo: ISO 27799:2008), testando sua conformidade e eficácia; a avaliação de um terceiro fornecedor de serviços críticos da sua cadeia de valor e que compõem um processo produtivo; e o cumprimento dos aspectos regulatórios e normativos que opera o setor de saúde. Assim, os principais objetivos de uma auditoria do sistema de gestão de segurança são: determinar sua conformidade, frente ao padrão ISO 27799:2008; determinar a eficácia do SGSI implementado; detectar oportunidades de melhoria do sistema; atender aos aspectos mandatórios para obter certificação e atender aos aspectos regulatórios do setor em que opera.

3.2.1.2 Monitoramento

O monitoramento do SGSI é a forma mais eficaz de garantir o funcionamento adequado e a manutenção da segurança dentro da organização (BASTOS; CAUBIT, 2009, p. 124). O processo de monitoração dos controles tem por objetivo detectar quaisquer atividades não autorizadas, falhas e o uso inadvertido dos recursos de informação. Para um monitoramento efetivo, os dispositivos de gestão devem ser inseridos e constantemente

monitorados de forma a permitir a integridade do fluxo das informações e garantir que possíveis desvios sejam corrigidos, assegurando que os riscos sejam reduzidos a um nível aceitável pela organização.

O processo de monitoramento deve ser formalmente definido e publicado, contendo os procedimentos de monitoramento do SGSI e assegurando que sejam analisados criticamente de forma regular.

3.2.1.3 Análise crítica

O processo de análise crítica do SGSI representa a disposição de revisão do sistema pela alta administração da organização por meio da avaliação dos indicadores do SGSI: resultado das auditorias anteriores, retornos das partes interessadas (terceiros, pacientes, fornecedores, entidades reguladoras etc.) sobre o desempenho do sistema ou possíveis falhas.

A análise crítica encerra o processo do ciclo PDCA que é o "*check*", ou seja, verificação do sistema, que contribui para a manutenção e perenidade do sistema de gestão de segurança na organização de saúde.

3.2.1.4 Abordagem dos processos

O Quadro 16 consolida, com base no estudo dos itens anteriores, os principais processos de monitoramento e análise do sistema de segurança descritos anteriormente, bem como apresenta seus objetivos e resultados.

Quadro 16 – Principais processos de monitoramento e análise do sistema de segurança

Processos: monitorar e analisar	Objetivos
Monitor e revisar procedimentos e controles	a) Detectar proativamente erros nos resultados e saídas do sistema; b) Detectar proativamente as tentativas e as ocorrências de brechas de segurança da informação ou incidentes; c) Permitir à alta administração da organização de saúde determinar se as atividades de segurança delegadas às pessoas ou implementadas pelos sistemas ou tecnologias estão desempenhando como esperado; d) Permitir detectar os eventos de segurança e prevenir os incidentes de segurança por meio do uso de indicadores; e) Determinar se as ações tomadas para resolver a brechas de segurança são efetivas
Realizar revisões regulares	Realizar revisões regulares da efetividade do SGSI (incluindo a política, os objetivos e os controles) levando em consideração os resultados das auditorias, incidentes, medidas de efetividade, sugestões e *feedbacks* de todas as partes interessadas.
Medir a efetividade dos controles	Medir a efetividade dos controles com objetivo de garantir que os objetivos dos controles de segurança foram atingidos.
Revisar as análises de riscos	Revisar as análises de riscos em intervalos planejados e revisar o nível de risco residual identificando os riscos aceitáveis tendo em consideração as seguintes mudanças: a) na organização de saúde; b) na tecnologia c) objetivos da organização e processos d) ameaças identificadas e) efetividade dos controles implementados f) fatores externos e eventos, como mudanças no ambiente regulatório e normativo do setor de saúde
Conduzir a auditorias internas e externas	Conforme descritos na Seção 3.2.1.1 deste trabalho.
Submeter à revisão da alta administração	Submeter periodicamente à revisão da alta administração do SGSI para garantir que o escopo (conforme descrito na Seção 3.1.2, “definir o escopo do SGSI”) permaneça adequado.
Registrar e/ou atualizar os planos	Registrar ou atualizar a documentação levando em conta os elementos detectados durante o monitoramento e revisão das atividades.
Registrar e/ou atualizar ações	Registrar ou atualizar as ações e os eventos que podem impactar a efetividade e a performance do SGSI.

Fonte: Resultado da pesquisa

Os processos para monitorar e analisar o sistema são processos que, em última análise, permitem a manutenção de um sistema de segurança na organização de saúde por meio dos subprocessos granulares e complementares identificados ao longo desse estudo.

3.2.2 Processos para manter e melhorar o sistema

O processo de manutenção e melhoria do SGSI refere-se ao processo "*Act*" do ciclo de gestão PDCA, no qual os controles implementados pela organização podem vir a ser melhorados. Para realizar a melhoria de desempenho do SGSI, deve-se levar em consideração os indicadores de desempenho estabelecidos pelos processos de implementação estudados anteriormente. As melhorias podem advir de ações corretivas e ações preventivas (BASTOS; CAUBIT, 2009, p. 162).

Uma ação corretiva é uma ação implementada para eliminar a causas de uma não-conformidade, de um defeito ou outra situação indesejável existente a fim de prevenir a sua repetição. As ações corretivas precisam ser registradas de forma a evidenciar sua execução por meio de um processo formal. As ações corretivas devem apresentar abordagem sistêmica e buscar a solução da situação de não conformidade, visando os processos e não somente a falha ocorrida (BASTOS; CAUBIT, 2009, p. 163)

A ação preventiva tem o objetivo de eliminar a causa de uma possível não conformidade, prevenindo sua ocorrência. Tal como nas ações corretivas, as ações preventivas de ser registradas para evidenciar sua execução por meio de um processo formal.

A partir da mesma filosofia da melhoria dos processos, que afirma que os executores são os responsáveis pelos bons resultados de eficiência e eficácia dos processos, o sucesso da manutenção de um SGSI não depende das organizações que o aplicam, mas das pessoas que cumprem as políticas, as normas e os procedimentos de segurança da informação no seu dia-a-dia dentro da organização de saúde (CALDER, 2009).

3.2.2.1 Abordagem dos processos

O Quadro 17 consolida, com base no estudo dos itens anteriores, os principais processos para “manter e melhorar” o sistema de segurança descritos anteriormente, bem como apresenta seus objetivos e resultados.

Quadro 17 – Principais processos para manter e melhorar o sistema de segurança

Processos: manter e melhorar	Objetivos
Implementar as melhorias identificadas	Implementar todas as melhorias identificadas durante a revisão do SGSI
Tomar ações preventivas e corretivas	Tomar ações preventivas e corretivas apropriadas. Aplicar as lições aprendidas das experiências de outras organizações em segurança, como também, da própria organização;
Medir a efetividade dos controles	Medir a efetividade dos controles com objetivo de garantir que os objetivos dos controles de segurança foram atingidos;
Comunicar ações e melhorias	Comunicar apropriadamente as ações e as melhorias para todas as partes interessadas com nível de detalhes apropriado as circunstancias e relevante
Certificar atingimento dos objetivos	Certificar-se que as melhorias propostas atingiram os objetivos da organização de saúde

Fonte: Resultado da pesquisa

Os processos para manter e melhorar o sistema são processos que, em última análise, encerram o ciclo PDCA e permitem a manutenção do sistema de segurança na organização de saúde por meio da execução dos subprocessos granulares identificados ao longo desse estudo.

4. CONSIDERAÇÕES SOBRE OS PROCESSOS DE SEGURANÇA DA INFORMAÇÃO EM SAÚDE

Em um ambiente inseguro para as informações das organizações de saúde, a norma ISO 27799:2008 oferece processos, que quando implementados, monitorados e mantidos, podem dar aos pacientes, médicos e enfermeiros a tranquilidade de que a segurança da informação nos sistemas de informação da organização é gerenciada. A efetiva adoção dos processos em linha com um padrão internacional de segurança da informação é um passo fundamental para a efetividade da governança da organização de saúde.

Nos últimos anos, tem havido mudanças no cenário regulatório e normativo com respeito à segurança e a privacidade da informação no setor de saúde no Brasil, o que tem exigido das organizações cuidados específicos com o tema para atender a esses aspectos. A normatização para o setor de saúde baseia-se em resoluções normativas do Conselho Federal de Medicina (CFM), em resoluções da Agência Nacional em Saúde Complementar (ANS), além das leis do próprio Código Penal brasileiro.

As resoluções normativas e as normas para setor influenciam diretamente a gestão e a governança das informações de pacientes no setor de saúde, a medida que a aderência a elas, pode se tornar obrigatória por entidades regulatórias. A segurança da informação e a aderência aos aspectos regulatórios e normativos do setor de saúde pode ser um problema mais sério para organizações maiores do que para as organizações menores, a medida que a complexidade e distribuição dos ativos e informações pela organização dificulta sua gestão.

Os processos examinados neste estudo apresentam de forma estruturada, com base nas normas internacionais, um roteiro de implementação e manutenção do SGSI em organizações de saúde. A implementação de um Sistema de Gestão de Segurança da Informação em uma organização de saúde é executada como um conjunto de atividades relacionadas, com seus respectivos processos, entradas, saídas, escopo, tempo e propriamente a gestão de riscos, conforme práticas e orientação do padrão do PMI – *Project Management Institute*. Como todo projeto, deverá haver um plano de preparação para implementação na organização de saúde com a aprovação da alta administração da organização de saúde, constando a definição da estrutura organizacional do projeto bem como a aprovação documentação da Administração.

Torna-se importante ressaltar que as normas específicas de Segurança da Informação, ISO/IEC 27001 e ISO/IEC 27002, respectivamente, são normas gerais e suas aplicações são independente do setor de atividade organizacional, enquanto que, a norma de referência do setor de Saúde (ISO 27799:2008), é específica e é apoiada nas normas ISO/IEC 27001 e ISO/IEC 27002.

Entretanto, a norma ISO 27799:2008, como padrão de segurança da informação para o setor de saúde, não apresenta as atividades operacionais e as outras atividades especificas de um SGSI; ela cobre os conceitos sobre como desenhar os processos e as atividades que resultarão em um SGSI implementado. Esse trabalho examinou as atividades operacionais e outras específicas concernentes à implementação e a manutenção do SGSI não cobertas na norma ISO 27799:2008. Como resultado dessa análise, procurou-se identificar e documentar esses processos, permitindo assim, que trabalhos futuros tratem de modelar os processos dentro de uma estrutura metodológica e possa ser empregada por qualquer organização de saúde que deseje implementar e manter um SGSI.

- Ao implementar e manter a norma ISO 27799:2008 com base nos processos examinados neste estudo, a organização de saúde pode desenvolver um sistema de segurança da informação orientado a processos, fornecendo aos gestores da organização o caminho para que os riscos às informações sejam constantemente avaliados e mantidos dentro de um nível aceitável conforme definido no escopo do SGSI. De acordo com a norma ISO 27799:2008 os principais processos de um sistema de gestão de segurança da informação são: Política de Segurança da Informação, Organizando a Segurança da Informação, Gestão de Ativos, Segurança em Recursos Humanos, Segurança Física e do Ambiente, Gestão das Operações e Comunicações, Controle de Acessos, Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação, Gestão de Incidentes de Segurança da Informação, Gestão de Continuidade do Negócio e Conformidade.

A manutenção de um sistema de gestão de segurança da informação para o segmento de saúde esta fundamentalmente apoiada em uma política de segurança, no processo de realização periódica de análise e avaliação de riscos em relação aos processos e informações em Saúde, considerando também, as constantes mudanças de cenários, de tecnologias, de demandas regulatórias e de processos organizacionais, dentre outros, na organização de saúde.

5. CONCLUSÕES

A utilização de dados e de informações de saúde de pacientes está no centro das atividades profissionais e do processo decisório nas organizações de saúde. Os registros de informações de pacientes, dentre os quais o mais importante é o prontuário médico, nos últimos anos eram representados por documentos em papel e mantidos por meio de uma miríade de formatos, conteúdos, e locais de armazenamento diferentes dentro da organização de saúde.

O desenvolvimento e a evolução dos Sistemas de Registros Eletrônicos de Saúde (S-RES) possibilitaram a criação e manutenção de registros de saúde de pacientes que abarcam toda a vida do indivíduo, e a criação de bases de dados digitais que contém informações agregadas clínicas e administrativas. Esse fato trouxe um grande impacto e melhorias de performance para as organizações de saúde, principalmente devido aos avanços e a disponibilidade de soluções tecnológicas e de telecomunicações as quais as organizações de saúde passaram a adotar e transformar a forma em que são criadas, mantidas, e recuperadas as informações de saúde, clínicas e administrativas, referentes aos pacientes.

Essas soluções tecnológicas e de telecomunicações são complexas e introduzem riscos relacionados à segurança, a confidencialidade, a integridade e a disponibilidade das informações nos sistemas S-RES que capturam, armazenam e trafegam informações pessoais de saúde, e em última análise, podem expor os pacientes e a organização de saúde a riscos.

Nesse contexto, o surgimento da norma ISO 27799:2008 permitiu oferecer às organizações de saúde, orientação, apoio e referências sobre a gestão da segurança, da confidencialidade, da integridade e da disponibilidade das informações pessoais de saúde por meio da implementação de um Sistema de Gestão de Segurança da Informação (SGSI). A norma internacional ISO 27799:2008 trata as necessidades e peculiaridades específicas de gerenciamento da segurança do setor de saúde e seus vários ambientes organizacionais e ela esta apoiada em outras duas importantes normas (ISO/IEC 27001:2005 e ISO/IEC 27002:2005) de Segurança da Informação.

As normas de segurança disponíveis não oferecem uma visão estruturada e detalhada dos processos e dos subprocessos de implementação e manutenção de um SGSI para o setor de saúde, e a principal contribuição desse estudo foi no sentido de apresentar uma proposta de

processos e subprocessos estruturados e sistematizados que orientam e direcionam para a implementação e manutenção do sistema de segurança em organizações de saúde. Esse estudo examinou os processos necessários para a implementação e manutenção de um sistema de segurança da informação para o setor de saúde de acordo com a norma ISO 27799:2008.

O resultado do estudo apresentado nesse trabalho traz detalhamentos, descrições e explicações sobre os processos de segurança para uma organização de saúde que deseje implementar segurança. Entretanto, ele não especifica qualquer requerimento novo, e é destinado a ser utilizado em conjunto com a norma ISO 27799:2008, portanto não é destinado a modificar ou reduzir os processos, requerimentos ou recomendações especificados na norma original.

O fator humano nas organizações de saúde é um fator que merece atenção, à medida que as pessoas constituem o elo mais fraco em um sistema de segurança. As pessoas (assistentes, médicos, enfermeiros, auxiliares, administrativo, etc.) estão presentes em todos os processos operacionais de uma organização de saúde, como por exemplo: recepção, atendimento, operação de sistemas e muitos outros. É importante ressaltar que as organizações de saúde somente se beneficiarão da implementação e manutenção de um sistema de gestão de segurança da informação se tiverem o verdadeiro apoio e comprometimento da alta administração, além disso a implementação de políticas de segurança, treinamento e conscientização são elementos críticos no dia a dia para assegurar que o risco do fator humano seja efetivamente gerenciado nas organizações de saúde.

5.1 Sugestões para trabalhos futuros

Como sugestão para trabalhos futuros, propõe-se a modelagem dos processos e elaboração de uma metodologia para a implementação e a manutenção de Sistema de Gestão de Segurança da Informação com base na norma ISO 27799:2008.

Destaca-se também a necessidade de analisar, em trabalhos futuros, os processos necessários para obtenção de aprovação para implementação do SGSI junto à alta administração da organização de saúde, bem como para os processos de planejamento do projeto.

6. REFERÊNCIAS

ABNT. **ISO/TR 20514. Informática em saúde – Registro eletrônico de saúde – Definição, escopo e contexto**. Associação Brasileira de Normas. Rio de Janeiro: 2005.

ABNT **ISO/IEC 27005**. **Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação**, ISO NBR, 2005

ALVES, G. A. **Segurança da Informação: Uma Visão Inovadora da Gestão**. Rio de Janeiro: Ed. Ciência Moderna, 2006.

BASTOS, Alberto; CAUBIT, Rosângela. **ISO 27001 e ISO 27002: Gestão de Segurança da Informação – Uma Visão Prática**. Porto Alegre: Souk, 2009.

BEZERRA, Edson K.; NAKAMURA, Emílio T.; RIBEIRO, Sérgio L.. **Maximizando Oportunidades com Gestão de Segurança e Gerenciamento de Riscos**. 2006. Disponível em www.cpqd.com.br/file.upload/6-sic-1-artigoforum-riscos.pdf. Acesso em: 17 Jan 2010.

BOSWORTH, M. H. **Ohio University: Data Breach Central?** Consumeraffairs.com, 2006. Disponível em http://www.consumeraffairs.com/news04/2006/05/ohio_u_data_theft.html. Acesso em: 23 Jan 2010.

BRASIL. Ministério da Saúde. Secretaria-executiva. Secretaria de gestão de trabalho e da educação na saúde. **Glossário temático: Gestão do trabalho e da educação na saúde**. Brasília: Editora do Ministério da Saúde, 2009.

CALDER, Alan. **Nine steps to sucess. An ISO 27001 implementation overview**. IT Governance Publishing, 2009.

CONSELHO FEDERAL DE MEDICINA. Resolução CFM 1.638/2002. 2002. Disponível em http://www.portalmedico.org.br/resolucoes/cfm/2002/1638_2002.htm Acesso em: 18 outubro 2003.

DEY, Manik. Information Security Management - A Practical Approach. **AFRICON 2007**, 2007, p. 1-6.

FERREIRA, F. N. F. **Segurança da Informação**. Rio de Janeiro: Ed. Ciência Moderna, 2006.

GARY, Stoneburner, ALICE Goguen, ALEXIS Feringa. **NIST Special Publication 800-30. Risk Management Guide for Information Technology Systems**. Recommendations of the National Institute of Standards and Technology, September, 2003. Disponível em http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf. Acesso em: 15 Dez 2009

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. São Paulo. Atlas, 1991.

HANASHIRO, Maíra. **Metodologia para Desenvolvimento de Procedimentos e Planejamento de Auditorias de TI Aplicadas à Administração Pública Federal**. Dissertação (Mestrado) Engenharia Elétrica. Universidade de Brasília, Brasília, 2007.

HERRERA, Sven S. Information Security Management Metrics Development. Security Technology, 2005. CCST '05. **39th Annual 2005 International Carnahan Conference**, 2005, p. 51–56.

HUMPHREYES, Edward. **Implementing the ISO/IEC 27001 Information Security Management System Standard**. Artech House, Inc. Norwood, MA, USA, 2007.

INTERNATIONAL MEDICAL INFORMATICS. **Information Security Risk Management for Healthcare Systems**. Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC), paper, 2007. 18 p.

ISO. **ISO 27799:2008. Health informatics — Information security management in health using ISO/IEC 27002**, ISO, 2008.

ISO/IEC. **ISO/IEC 27001:2005**. **Information technology -- Security techniques -- Information security management systems** – Requirements, ISO, 2005

ISO/IEC. **ISO/IEC 27002:2005**. **Information technology -- Security techniques -- Code of practice for information security management**, ISO, 2005

KOVACICH, G. L. **The Information Systems Security Officer's Guide: Establishing and Managing an Information Protection Program**. Ed. Butterworth Heinemann, 2006.

LEÃO B, COSTA C, FORMAN J, GALVÃO D. **Manual de Certificação para Sistemas de Registro Eletrônico em Saúde – versão 3.1**. Disponível em: http://www.sbis.org.br/certificacao/Manual_Certificcao_SBIS_CFM_Fase2_v3.1_Consulta_Publica.pdf, 2008.

MARTINS, Gilberto de Andrade. **Manual para elaboração de monografias e dissertações**. São Paulo: Atlas, 1994.

MASSAD, E.; MARIN, H. F.; AZEVEDO, R. S. **O Prontuário do Paciente na Assistência, Informação e Conhecimento Médico**. São Paulo. USP, 2003.

NIST. **National Vulnerability Database Home**. Disponível em: http://icat.nist.gov. Acesso em: 20 Mar 2010.

PMI. Project Management Institute. **PMBok® Terceira edição: Project Management Body of Knowledge**. PMI, 2004.

PONEMOM INSTITUTE LLC. **Electronic Health Information at Risk - A Study of IT Practitioners**. Ponemon Institute© Research Report. October 15, 2009 Disponível em: http://loglogic.com/resources/analyst-reports/ponemon-electronic-health-info-at-risk/. Acesso em: 19 Jan 2010.

RÖTZSCH, Jussara Macedo Pinho. Troca De Informações Em Saúde Suplementar. **Seminário Internacional de Avaliação do Impacto Sócio-Econômico do TISS**. Brasília, 2009. Disponível em: http://anstabnet.ans.gov.br/data/files/jussara08062009_TISS.pdf. Acesso em 10 Mar 2010.

ROSS, R. *et al*. **Guide for assessing the security controls in Federal Information Systems**. **Building Effective Security Assessment Plans**. NIST Special Publication 800-53A. NIST, 2008. Disponível em: http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf. Acesso em: 20 Mar 2010.

SALVADOR, V.; FILHO, F. Aspectos Éticos e de Segurança do Prontuário Eletrônico do Paciente. **II Jornada do Conhecimento e da Tecnologia**, UNIVEM, Marília, SP, 2005. Disponível em: http://galileu.fundanet.br/jornada/artigos/computacao/Valeria_Farinazzo.pdf. Acesso em: 19 jan 2010.

SILVA, Edna Lúcia da., MENEZES, Estera Muszkat. **Metodologia da Pesquisa e Elaboração de Dissertação**. 3ª Ed. Florianópolis: Laboratório de Ensino a Distância da UFSC, 2001.

WASHINGTON D.C. **Federal Coordinating Council for Science. Office of Science and Technology Policy. High performancecomputing & communications: toward a national information infrastructure**. Washington D.C., 1994. 176 p.

Anexo A – Controles da Norma ISO/IEC 27002:2005

Controles da ISO/IEC 27002:2005		
Cláusula	Seção	Objetivo do Controle/Controle
Política de Segurança da Informação	5,1	Política de Segurança da Informação
	5.1.1	Documento de política de segurança da informação
	5.1.2	Revisão do documento de política de segurança da informação
Organizando a Segurança da Informação	6,1	Organização Interna
	6.1.1	Comprometimento gerencial
	6.1.2	Coordenação
	6.1.3	Atribuição de responsabilidades
	6.1.4	Processo de autorização para meios de processamento de informação
	6.1.5	Acordos de confidencialidade
	6.1.6	Contato com autoridades
	6.1.7	Contato com grupos de interesses especiais
	6.1.8	Revisão independente de segurança da informação
	6,2	Entidades Externas
	6.2.1	Identificação de riscos relacionados a entidades externas
	6.2.2	Endereçando a segurança ao tratar dos clientes
	6.2.3	Endereçando a segurança em acordos com entidades terceirizadas
Gestão de Ativos	7,1	Responsabilidade pelos ativos de informação de saúde
	7.1.1	Inventario dos ativos
	7.1.2	Custodiante designado para ativos de infomação de saúde
	7.1.3	Regras para o uso aceitável desses ativos
	7,2	Classificação de informação de saúde
	7.2.1	Diretrizes de classificação
	7.2.2	Manuseio e rotulagem da informação

Segurança em Recursos Humanos	8,1	Antes do emprego
	8.1.1	Papéis e responsabilidades
	8.1.2	Seleção
	8.1.3	Termos e condições de emprego
	8,2	Durante o emprego
	8.2.1	Responsabilidades de gerência
	8.2.2	Conscientização, educação e treinamento em segurança da informação
	8.2.3	Processo disciplinar
	8,3	Desligamento ou mudança de emprego
	8.3.1	Responsabilidades do desligamento
	8.3.2	Retorno dos ativos
	8.3.3	Remoção dos direitos de acesso
Segurança Física e de Ambiente	9,1	Áreas Seguras
	9.1.1	Perímetro de segurança física
	9.1.2	Controles de entrada física
	9.1.3	Assegurando escritórios, salas e aparelhos
	9.1.4	Protegendo contra ameaças ambientais e externas
	9.1.5	Trabalhando em áreas seguras
	9.1.6	Áreas de acesso público, carga e descarga
	9,2	Segurança de equipamentos
	9.2.1	Localização e proteção de equipamentos
	9.2.2	Utilitários de suporte
	9.2.3	Segurança de cabeamento
	9.2.4	Manutenção de equipamentos
	9.2.5	Segurança de equipamentos fisicamente externos
	9.2.6	Descarte ou reutilização segura de equipamento
	9.2.7	Remoção de propriedade
Gestão de comunicações e operações	10,1	Responsabilidades e procedimentos operacionais
	10.1.1	Procedimentos operacionais documentados
	10.1.2	Gestão de mudanças
	10.1.3	Segregação de função
	10.1.4	Separação de meios de desenvolvimento, ensaios e operações
	10,2	Gestão de entrega de serviços terceirizados
	10.2.1	Entrega de serviços
	10.2.2	Monitoramento e revisão de serviços terceirizados

	10.2.3	Gestão de mudanças de serviços terceirizados
	10,3	Aceitação e planejamento de sistema
	10.3.1	Gestão de capacidade
	10.3.2	Aceitação de sistema
	10,4	Proteção contra código malicioso e código movel
	10.4.1	Controle contra código malicioso
	10.4.2	Controles contra código movel
	10,5	Back-Up - Cópia de segurança de informação de saúde
	10.5.1	Cópia de segurança de informação de saúde
	10,6	Gestão de segurança da rede
	10.6.1	Controles de rede
	10.6.2	Segurança de serviços de rede
	10,7	Manuseio de mídia
	10.7.1	Gestão de mídia removivel de computador
	10.7.2	Descarte de mídia
	10.7.3	Procedimentos de manuseio de informação
	10.7.4	Segurança de documentação do sistema
	10,8	Troca de informação
	10.8.1	Políticas e procedimentos de troca de informação de saúde
	10.8.2	Acordos de troca
	10.8.3	Mídia física em trânsito
	10.8.4	Mensagens eletrônica
	10.8.5	Sistemas de informação de saúde
	10,9	Serviços de informação de saúde eletronicos
	10.9.1	Comércio eletrônico
	10.9.2	Transações on-line
	10.9.3	Informação de saúde disponível publicamente
	10,10	Monitoramento
	10.10.1	Registro de auditoria
	10.10.2	Monitorando o uso do sistema
	10.10.3	Proteção de informação do registro
	10.10.4	Registros de administrador e operador
	10.10.5	Registro de falhas
	10.10.6	Sincronização de relógio
Controle de Acesso	11,1	Requisitos para controle de acesso na saúde
	11.1.1	Política de controle de acesso

	11,2	Gerencia de acesso do usuário
	11.2.1	Registro de usuário
	11.2.2	Gerenciamento de privilégio
	11.2.3	Gerenciamento de senha de usuário
	11.2.4	Revisão de direitos de acesso do usuário
	11,3	Responsabilidades do usuário
	11.3.1	Uso de senhas
	11.3.2	Equipamentos de usuários desatendidos
	11.3.3	Politica de mesa e tela limpas
	11,4	Controle de acesso a rede
	11.4.1	Politica de uso de serviços de rede
	11.4.2	Autenticação de usuários para conexões externas
	11.4.3	Identificação de equipamentos na rede
	11.4.4	Diagnoticos remote e configuração de proteção de portas
	11.4.5	Separação da redes
	11.4.6	Controle de conexão de redes
	11.4.7	Controle de roteamento em redes
	11,5	Controle de Acesso dos Sistemas Operacionais
	11.5.1	Procedimentos de Log-on seguro
	11.5.2	Identificação e autenticação de usuário
	11.5.3	Sistema de gestão de senhas
	11.5.4	Uso de sistemas utilitários
	11.5.5	Tempo de sessão
	11.5.6	Limitação do tempo de conexão
	11,6	Controle de acesso a aplicação
	11.6.1	Restrição de acesso a informação
	11.6.2	Isolação de sistemas sensíveis
	11,7	Computação móvel e trabalho a distancia
	11.7.1	Computação móvel e trabalho a distancia
	11.7.2	Trabalho a distancia
Aquisição, desenvolvimento e manutenção de sistema de informação	12,1	Requisitos de segurança de sistemas de informação
	12.1.1	Analise e especificação de requisitos de segurança
	12,2	Processamento correto de aplicações
	12.2.1	Validação de entrada de dados
	12.2.2	Controle de processamento interno
	12.2.3	Integridade de mensagem

	12.2.4	Validação de dados de saída
	12,3	Controle criptográficos
	12.3.1	Política de uso de controle criptográficos
	12.3.2	Gerenciamento das chaves
	12,4	Segurança de sistemas de arquivos
	12.4.1	Controle de software operacional
	12.4.2	Proteção de dados de teste de sistema
	12.4.3	controle de acesso a bibliteca de código fonte
	12,5	Segurança no Desenvolvimento e Processos de Suporte
	12.5.1	Procedimentos de controle de mudança
	12.5.2	Revisão técnica das aplicações
	12.5.3	Restrição de mudançca em pacotes de software
	12.5.4	Vazamneto de informação
	12.5.5	Desenvolvimento de software por terceiros
	12,6	Gestão de vulnerabilidades técnicas
	12.6.1	Controle de vulnerabilidades técnicas
Gerenciamento de incidentes de segurança da informação	13,1	Reporte de eventos e vulnerabilidades de segurança
	13.1.1	Reporte de eventos de segurança da informação
	13.1.2	Reporte de vulnerabilidades
	13,2	Gestão de incidentes de segurança e melhorias
	13.2.1	Responsabilidades e procedimentos
	13.2.2	Aprendizado dos incidentes de segurança da informação
	13.2.3	Coleção de evidências
Gestão de Continuidade de negócios	14,1	Aspectos de segurança da informação em continuidade de negócios
	14.1.1	Incluindo segurança da informação no processo de continuidade de negóci
	14.1.2	Continuidade de negocios e avaliação de riscos
	14.1.3	Desenvolvendo plano de continuidade de negócios
	14.1.4	Estrutura de desenvolvimento do plano de continuidade de negócios
	14.1.5	Testes e manutenção dos planos de continuidades de negocios

Conformidade	15,1	Conformidade com requisitos legais
	15.1.1	Identificação de legislação aplicável
	15.1.2	Direito de propriedade intelectual
	15.1.3	Proteção de registros
	15.1.4	Proteção de dados e privacidade de informação pessoal
	15.1.5	Prevenção de abuso das facilidades de processamento de informação
	15.1.6	Regulação de controles criptográficos
	15,2	Conformidade com políticas e padrões de seg. e conformidade técnica
	15.2.1	Conformidade com políticas de segurança
	15.2.2	Checagem técnica de conformidade
	15,3	Considerações sobre auditoria de sistemas
	15.3.1	Controles de auditoria de sistemas de informação
	15.3.2	Proteção da informações das ferramentas de auditoria

Fonte: Norma ISO/IEC 27002:2005

Anexo B – Fontes de Ameaças, Motivações e Ações

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

Fonte: GARY et al, 2003, p14

Anexo C – Relacionamento entre Vulnerabilidades e Fontes de Ameaças

Vulnerability	Threat-Source	Threat Action
Terminated employees' system identifiers (ID) are not removed from the system	Terminated employees	Dialing into the company's network and accessing company proprietary data
Company firewall allows inbound telnet, and *guest* ID is enabled on XYZ server	Unauthorized users (e.g., hackers, terminated employees, computer criminals, terrorists)	Using telnet to XYZ server and browsing system files with the *guest* ID
The vendor has identified flaws in the security design of the system; however, new patches have not been applied to the system	Unauthorized users (e.g., hackers, disgruntled employees, computer criminals, terrorists)	Obtaining unauthorized access to sensitive system files based on known system vulnerabilities

Fonte: Gary *et al*., 2003, p. 16.