ESTUDO SOBRE A CONFORMIDADE DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO DO HEMOSC COM NORMA ISO 27001:2013

Mônica Meller Nunes[1]

Resumo: Este artigo trata do estudo sobre a conformidade da gestão da segurança da informação do Hemosc, com relação à Norma ISO 27001:2013. São estudados alguns conceitos relacionados à segurança da informação, à Norma ISO 27001:2013, e a forma com que a norma trata a segurança da informação. Também é realizada a avaliação da gestão da segurança da informação do Hemosc, de acordo com cada requisito estabelecido pela Norma ISO 27001:2013, definido a conformidade de cada item e identificado de que forma os requisitos são atendidos. Seu principal objetivo é diagnosticar a gestão da segurança da informação do Hemosc à luz da Norma ISO 27001:2013.

Palavras-chave: Tecnologia da Informação. Segurança da Informação. ISO 27001:2013.

1 INTRODUÇÃO

O Centro de Hematologia e Hemoterapia de Santa Catarina – Hemosc, apesar de depender fortemente de suas informações e de seus sistemas informatizados para conseguir realizar seus processos e dessa forma atingir seus objetivos estratégicos, ainda não possui um Sistema de Gestão de Segurança da Informação formalmente estabelecido, baseado em padrões e metodologias.

Esta situação torna-se preocupante à medida que a instituição expande sua área de atuação, aperfeiçoa seus processos e implanta novas tecnologias, sempre com envolvimento da Tecnologia de Informação como meio para viabilização dos projetos.

Outro fator a ser ponderado é a ampliação e renovação do quadro de colaboradores tanto na área de Tecnologia da Informação, quanto na gestão organizacional, fato este que requer que o conhecimento e as normas estabelecidas nos processos de trabalho, sejam compartilhados com todos e considerados patrimônio da organização e não das pessoas que ocupam as posições estratégicas.

[1] Bacharel em Ciências da Computação – UFSC/1988. Cursando Especialização de Governança de Tecnologia de Informação-Unisul. Assessora de Informática do Centro de Hematologia e Hemoterapia de Santa Catarina

Diante da situação, a necessidade é fazer uma investigação, identificando os processos existentes e seu nível de maturidade e os processos faltantes, tendo como norteador do estudo uma norma ou padrão reconhecido no mercado, com o objetivo de realizar uma avaliação do Sistema de Gestão da Segurança da Informação do Hemosc à luz da metodologia escolhida.

Após o estudo de várias metodologias e padrões relacionados ao gerenciamento da segurança da informação e considerando que o Hemosc possui certificação ISO 9001, optou-se por adotar a norma NBR ISO 27001:2013, a qual é o padrão e a referência internacional para a gestão da Segurança da Informação, assim como a ISO 9001 é a referência Internacional para a certificação de gestão de Qualidade e ambas são compatíveis.

O objetivo geral deste trabalho é investigar se a Gestão da Segurança da Informação do Hemosc está em conformidade com a norma ISO 27001:2013. Seus objetivos específicos são: avaliar a Gestão da Segurança da Informação do Hemosc, de acordo com cada requisito da norma NBR/ISO 27001:2013, identificar o nível de conformidade de cada item e apontar pontos fortes e pontos críticos da gestão da segurança da informação.

O presente estudo foi realizado com base na documentação oficial NBR/ISO 27001:2013 e levantamento bibliográfico, buscando informações e dados disponíveis em publicações da produção científica relacionados à questão de implementação e certificação de Sistemas de Gestão da Segurança da Informação.

A metodologia aplicada neste trabalho, quanto à natureza, foi a pesquisa aplicada, pois os conhecimentos adquiridos serão utilizados para aplicação prática, voltados para a solução de problema.

Quanto à forma de abordagem foi utilizada a pesquisa qualitativa, na qual o pesquisador participa, compreende e interpreta os dados coletados. E a subjetividade do sujeito não pode ser traduzida em números e não requer o uso de técnicas e métodos estatísticos.

Após o levantamento bibliográfico e estudo da norma NBR/ISO 27001:2013, foi realizado um *check-list* com os requisitos da norma. Para avaliação da conformidade de cada item foi verificado a documentação existente bem como foram realizadas entrevistas com profissionais envolvidos com a Segurança da Informação e com a Gestão da Qualidade do Centro de Hematologia e Hemoterapia de Santa Catarina. Para cada requisito observado foi definido se está conforme, não conforme, parcialmente conforme ou não se aplica e, ainda se procede alguma observação ou oportunidade de melhoria.

Como resultado da análise de dados será possível identificar o nível de conformidade da gestão da segurança da informação do Hemosc frente à norma NBR ISO 27001:2013, e quais ações serão necessárias para adequar a gestão aos requisitos da norma.

A seguir será apresentada a fundamentação teórica, envolvendo conceitos de Informação, Segurança da Informação e ISO 27001, os dados analisados através de uma lista de verificação e os resultados obtidos.

2 GESTÃO DA SEGURANÇA DA INFORMAÇÃO

A informação, ativo cada vez mais valorizado, impacta diretamente na continuidade dos negócios das organizações e na sua credibilidade. Por conta disso, tem-se buscado cada vez mais, meios que garantam a proteção da informação. A Gestão da Segurança da Informação abrange a criação de processos voltados ao monitoramento contínuo da integridade das informações, à prevenção de ataques e ao furto dos dados, assegurando o pronto restabelecimento dos sistemas e acesso seguro, em casos emergenciais.

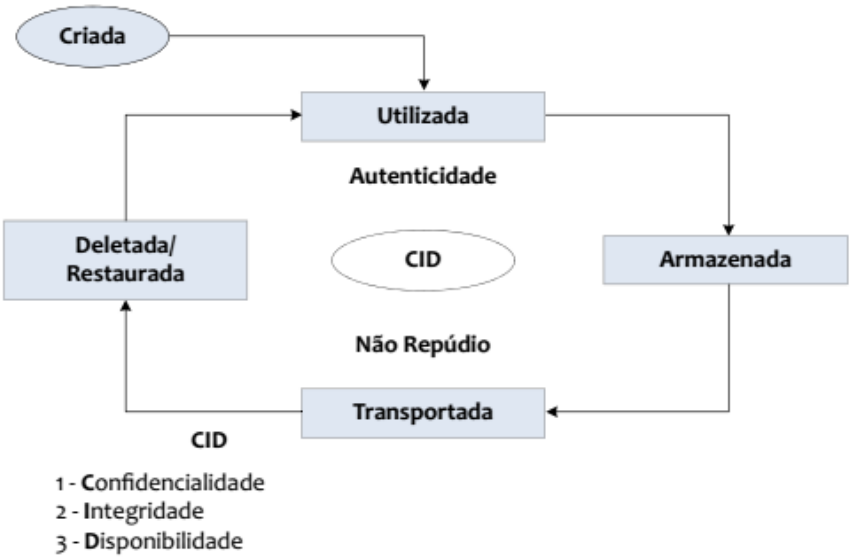
2.1 INFORMAÇÃO

De acordo com Siqueira (2005), as informações devem ser disponibilizadas de acordo com o público que precisa ter acesso.

Com isso, Peixoto (2006) define que as informações podem ser de acesso público ou interno e particular ou confidencial.

Campos (2007) divide o ciclo de vida da informação em cinco fases: a criação, transporte, publicação, armazenagem e descarte. A Figura 1 representa esse ciclo:

Figura 1– Ciclo de Vida da Informação



Fonte: Baseado em, Lento (2011, página 103)

Para Sêmola (2003) as informações possuem um ciclo de vida dividido em quatro etapas:

- **Manuseio:** Situação de criação e manipulação da informação, podendo acontecer ao percorrer papéis, autenticar-se para ter acesso a um determinado ambiente, entre outros.
- **Armazenamento:** Situação em que as informações são arquivadas, podendo ser em mídias como disquetes (sendo guardadas no ambiente de trabalho) ou ainda em banco de dados compartilhados, entre outros.
- **Transporte:** Situação em que a informação é movimentada, podendo ocorrer por meio de comunicação por telefone (de informações confidenciais) ou ainda por ferramentas eletrônicas (como com troca de e-mail).
- **Descarte:** Situação em que a informação é excluída, podendo esta ser física (um material impresso) sendo jogada em uma lixeira ou ainda uma informação digital podendo ser descartada de um computador (ou outro meio eletrônico).

2.2 SEGURANÇA DA INFORMAÇÃO

Para Peixoto (2006), a segurança da informação é construída pelos seguintes pilares básicos:

- **Confidencialidade:** Garantia de que as informações serão de acesso apenas aos usuários autorizados.
- **Integridade:** Garantia de que nenhuma alteração aconteça na informação durante o seu percurso (caminho entre remetente e destinatário), assegurando a veracidade da mesma.
- **Disponibilidade:** Garantia de que as informações estarão disponíveis num sistema computacional (para usuários autorizados) sempre que requisitadas.

Podendo ainda incluir-se mais dois pilares:

- **Não repúdio e autenticidade:** Estes tem como finalidade comprovar a identidade e autenticidade de um acesso garantindo a integridade de origem.

A área da segurança da informação conforme Sêmola (2003, página 43), é voltada a proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou a sua indisponibilidade. Para ele segurança da informação é um termo dúbio, podendo ser visto como:

> - **Segurança como "meio":** A segurança da informação visa garantir a confidencialidade, integridade e disponibilidade da informação, a impossibilidade de que agentes participantes em transações ou na comunicação repudiem a autoria de suas mensagens, a conformidade com a legislação vigente e a continuidade dos negócios.
> - **Segurança como "fim":** A segurança da informação é alcançada por meio de práticas e políticas voltadas a uma adequada padronização operacional e gerencial dos ativos, e processos que manipulam e executem a informação.

O tema Segurança da Informação, não está ligado somente à ação de hackers, anti-vírus ou atualização de servidores, envolve diversas áreas, tais como: segurança física, infraestrutura tecnológica, aplicações e conscientização organizacional, cada uma delas com

seus próprios riscos, ameaças e controles aplicáveis e soluções de segurança que podem minimizar a exposição do maior patrimônio da organização: a informação.

Quando for discutida a Segurança da Informação, deve se tomar sempre em consideração os pilares básicos: Confidencialidade, Integridade e Disponibilidade.

Segundo a norma ISO 27001:2006, Sistema de Gestão da Segurança da Informação (SGSI) é a "parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação."

A implantação de um SGSI em uma organização é estratégico para o seu negócio, pois através dele é possível aprimorar a gestão da segurança da informação. Em todo SGSI existem três partes fundamentais: avaliação, correção e registro. Estas três atividades compõem as partes mais importantes do Ciclo PDCA(*Plan, Do, Check, Act*), favorecido nos sistemas de gestão ISO. Quando uma parte fica de fora do ciclo, a gestão da segurança torna-se impossível.

2.3 ISO 27001:2013

A ISO 27001 é uma norma internacional publicada pela Internacional Standardization Organization (ISO), com o objetivo de prover um modelo para o estabelecimento, implementação, operação, monitoramento, revisão, manutenção e melhoria de um Sistema de Gestão de Segurança da Informação.

A versão mais recente desta norma foi publicada em 2013, e seu título completo é ISO/IEC 27001:2013. A primeira versão foi publicada em 2005, e foi desenvolvida com base na Norma Britânica BS 7799-2.

Segundo a norma NBR ISO/IEC 17799:2005, 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 oportunidade de negócios. Ainda segundo a NBR ISO/IEC 17799:2005 a segurança da informação é caracterizada pela preservação dos três atributos básicos da informação: confidencialidade, integridade e disponibilidade.

O foco da ISO 27001 é proteger a confidencialidade, integridade e disponibilidade da informação de uma organização. E tem como princípio geral a adoção, pela organização, de um conjunto de requisitos, processos e controles com o objetivo de mitigar e gerir adequadamente o risco da organização. Isto é realizado através da identificação de potenciais problemas que possam ocorrer com a informação e o que deve ser feito para prevenir que tais problemas ocorram. Desta forma, a principal filosofia da ISO 27001 é a baseada na gestão de riscos: descobrir onde os riscos estão e tratá-los sistematicamente.

2.4 *CHECK-LIST* REQUISITOS ISO 27001:2013

A lista de verificação a seguir descreve os requisitos especificados nos itens 4 a 10 da norma ISO/IEC 27001:2013, os quais devem ser atendidos pela organização que reivindica conformidade com a norma.

A avaliação poderá ser considerada: C- Conforme, NC-Não Conforme, PC-Parcialmente Conforme ou NA-Não se Aplica.

Quadro 1 - Requisitos especificados nos itens 4 a 10 da norma ISO/IEC 27001:2013

Lista de verificação Gestão da Segurança da Informação do Hemosc		
Requisito	Aval.	Observação
4 Contexto da Organização	-	
4.1 Entendendo a organização e seu contexto	NC	O Hemosc não possui esta definição.
4.2 Entendendo as necessidades e as expectativas das partes interessadas	C	As partes interessadas e seus requisitos estão definidas do Manual da Qualidade do Hemosc..
4.3 Determinando o escopo do sistema de gestão da segurança da informação	NC	O Hemosc não possui esta definição.
4.4 Sistema de gestão de segurança da informação	NC	O Hemosc não possui um sistema de gestão de segurança de informação implantado.
5. Liderança	-	

5.1 Liderança e comprometimento	PC	Apesar se o Hemosc não possuir um sistema de gestão de segurança de informação implantado, a alta direção, através das ferramentas da gestão da qualidade, demonstra sua preocupação com a segurança da informação.
5.2 Política	C	FLN.05.01 – Política de Segurança de Informática da Hemorrede de Santa Catarina.
5.3 Autoridades, responsabilidades e papéis organizacionais	C	A Assessoria de Informática é responsável pela gestão da segurança da informação.
6 Planejamento	-	
6.1 Ações para contemplar riscos e oportunidades	-	
6.1.1 Geral	NC	O Hemosc não possui sistema de gestão de riscos e oportunidades.
6.1.2 Avaliação de riscos de segurança da informação	NC	O Hemosc não possui sistema de gestão de riscos e oportunidades.
6.1.3 Tratamento de riscos de segurança da informação	NC	O Hemosc não possui sistema de gestão de riscos e oportunidades. Porém realiza alguns controles previstos no Anexo A.
6.2 Objetivo de segurança da informação e planejamento para alcançá-lo	NC	O Hemosc não possui sistema de gestão de riscos e oportunidades.
7 Apoio	-	
7.1 Recursos	C	No orçamento do Hemosc existe uma conta específica para Tecnologia da Informação.
7.2 Competência	C	Hemosc possui funcionários competentes e fornecedores de serviços de tecnologia da informação especializados.
7.3 Conscientização	C	Os colaboradores tomam ciência da Política de Informática logo de iniciam da instituição.
7.4 Comunicação	NC	Não existe um processo formal de comunicação.
7.5 Informação documentada	-	
7.5.1 Geral	NC	O Hemosc não possui sistema de gestão da segurança da informação.
7.5.2 Criando e Atualizando	NC	O Hemosc não possui sistema de gestão da segurança da informação.
7.5.3 Controle da informação documentada	PC	Apesar de o Hemosc não possui sistema de gestão da segurança da informação, a documentação existente referente aos controles realizados do Anexo A, possuem controle através do controle de documentação previsto na ISO 9001.
8 Operação	-	

8.1 Planejamento operacional e controle	NC	O Hemosc não possui sistema de gestão de riscos e oportunidades.
8.2 Avaliação de riscos de segurança da informação	NC	O Hemosc não possui sistema de gestão de riscos e oportunidades.
8.3 Tratamento de riscos de segurança da informação	NC	O Hemosc não possui sistema de gestão de riscos e oportunidades.
9 Avaliação de desempenho	-	
9.1 Monitoramento, medição, análise e avaliação	NC	O Hemosc não possui sistema de gestão da segurança da informação.
9.2 Auditoria interna	PC	O Hemosc possui consolidado o processo de auditoria interna em função do Sistema de Gestão da Qualidade, porém somente alguns processos da Tecnologia da Informação são auditados e não o sistema de gestão de segurança de informação, visto que não existe.
9.3 Análise crítica pela direção	PC	A Alta Direção avalia criticamente os processos auditados em função da Sistema de Gestão da Qualidade
10	-	
10.1 Não conformidade e ação corretiva	C	Realizada através do Sistema de Gestão da Qualidade do Hemosc
10.2 Melhoria contínua	PC	Realizada através do Sistema de Gestão da Qualidade do Hemosc nos processos existentes.

Fonte: (Dados da pesquisa, 2015)

Após avaliar e responder cada ítem do *check-list*, foi verificado que todos os requisitos na norma são aplicáveis à gestão da segurança da informação do Hemosc, dos quais foram identificados 7(sete) ítens Conforme, 5(cinco) itens Parcialmente Conforme e 14(quatorze) ítens Não Conforme. Sendo que as não-conformidades estão relacionadas principalmente à ausência do sistema de gestão de riscos e oportunidades e ao fato de não existir um sistema de gestão da segurança da informação estabelecido formalmente, e as conformidades estão relacionadas a existência do Sistema de gestão da Qualidade e certificação ISO 9001.

3 CONCLUSÃO

O objetivo deste estudo, que se propôs a realizar um diagnóstico da gestão da segurança da informação do Hemosc, visando contribuir com informações para desencadear as ações de melhoria dos seus processos, foi atingido.

Embora ainda não possua um sistema de gestão de segurança da informação formalmente estabelecido, a Assessoria de Informática do Hemosc, vem realizando vários procedimentos relevantes para a garantia da confidencialidade, integridade e disponibilidade das informações da instituição.

Através da lista de verificação foi possível evidenciar vários pontos a serem implantados ou melhorados principalmente no que diz respeito à sistematização dos processos diretamente relacionados ao gerenciamento de riscos.

A existência do sistema de gestão da qualidade e da certificação ISO 9001 contribuem muito fortemente para o cumprimento de vários requisitos da Norma ISO 27001:2013, uma vez que algumas exigências desta estão previstas também na Norma NBR ISO 9001:2008 e já são aplicadas na Tecnologia da Informação.

Para que se possa atingir um maior nível de conformidade com a norma, será necessária a criação de um sistema de gestão de riscos e oportunidades e posteriormente um sistema de gestão de segurança da informação.

Considerando que o Hemosc já possui alguns controle e objetivos de controles definidos no Anexo A da Norma NBR ISO 27001:2013, uma alternativa viável será iniciar a implantação do sistema de gestão de segurança da informação pela definição de todos os processos requeridos no referido anexo, para na sequência definir as atividades necessárias para atendimento dos requisitos da norma.

STUDY ON THE CONFORMITY OF HEMOSC INFORMATION SECURITY MANAGEMENT WITH STANDARD ISO 27001: 2013

ABSTRACT: This article deals with the study aboutr the information security management of Hemosc with respect to ISO 27001: 2013. Studies are carried out about some concepts related to information security, the ISO 27001: 2013, and the way in which the norm comes to information security. It is also performed an evaluation of the information security management of Hemosc, according to each requirement established by ISO 27001: 2013, defined the compliance of each item and identified how the requirements are met. Its main objective is to diagnose the information security management of Hemosc according to ISO 27001: 2013.

Keywords: Information Technology. Information Security. ISO 27001:2013.

REFERÊNCIAS

27001 Academy. **O que é a ISO 27001?** Disponível em <http://www.iso27001standard.com/pt-br/o-que-e-a-iso-27001/>. Acesso em: 24 fev. 2015.

CALDER, Alan. Nine **Steps to Success: An ISO 27001:2013 Implementation Overview**. United Kingdon. 2. ed. 2013. Disponível em <https://books.google.com.br/books?id=9eRgAgAAQBAJ&printsec=frontcover&dq=iso+27001&hl=pt-BR&sa=X&ei=cG_7VOL0F4OrgwSzpIKgDA&ved=0CDoQ6AEwAzgK#v=onepage&q=iso%2027001&f=false>. Acesso em 06 mar. 2015.

CAMPOS, André. **Sistema de Segurança da informação**. 2ª edição. Florianópolis: Visual Books, 2007.

INTEGRITY. **ISO 27001 Sistema de Gestão de Segurança da Informação.** Disponível em <https://www.27001.pt/>. Acesso em: 08 mar. 2015.

KOSUTIC, Dejan**. A lógica básica da ISO 27001: Como a segurança da informação funciona?** 2014. Disponível em <http://www.profissionaisti.com.br/2014/05/a-logica-basica-da-iso-27001-como-a-seguranca-da-informacao-funciona/>. Acesso em 07 mar. 2015.

LENTO, Luíz Otávio Botelho**. Governança e Gestão da Segurança de Informação**. Palhoça: UnisulVirtual, 2011.

NBR ISO 27001:2013 - **Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos.**

NOGUEIRA, Ligia Casagrande. **Proposta para acreditação do Laboratório de Sorologia/Teste de Amplificação do Ácido Nucléico (NAT) da Hemorrede de Santa Catarina conforme padrões da organização Nacional de Acreditação (ONA), em nível de excelência.** Belo Horizonte, 2012.

PEIXOTO, Mário C. P. **Engenharia Social e Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006.

SÊMOLA, Marcos. **Gestão da segurança da Informação: uma visão executiva**. Rio de Janeiro: Campus, 2003.

SIQUEIRA, Marcelo Costa. **Gestão Estratégica da Informação**. Rio de Janeiro: Brasport, 2005.

SILVA, Rosemery Quadra e; MELLO, Lívia Rejane de. **MELHORIA DE PROCESSOS EM UMA PEQUENA UNIDADE ORGANIZACIONAL APLICANDO A NORMA ISO/IEC 29110**. 2014. 109 f. TCC (Graduação) - Curso de Sistemas de Informação, Universidade do Sul de Santa Catarina, Palhoça, 2014.

SOUZA, Ranieri Marinho de. **Implantação de ferramentas e técnicas de segurança da informação em conformidade com as normas ISO 27001 e ISO 17799.** Campinas, 2007. Disponível em: <http://www.bibliotecadigital.puc-campinas.edu.br/tde_arquivos/10/TDE-2008-03-14T122330Z-1418/Publico/raniere%20marinho%20de%20souza.pdf.>. Acesso em 07 mar. 2015.