

# DESENVOLVIMENTO DE SISTEMAS DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO ATRAVÉS DA INTEGRAÇÃO DAS NORMAS ISO/IEC 27001:2006 E ISO/IEC 21827 (SSE-CMM)

Josiane Kroll<sup>1</sup>, Marcos C. d'Ornellas<sup>2</sup>, Lisandra Manzoni Fontoura<sup>3</sup>

**Sumário:** 1. Introdução. 2. O Desenvolvimento de Sistemas de Gestão da Segurança da Informação (SGSI). 3. Normas da Segurança. 3.1. Norma ISO/IEC 27001:2006. 3.2. Norma ISO/IEC 21827 (SSE-CMM). 4. Análise das Normas Apresentadas. 5. Combinação das Normas De Segurança ISO/IEC 27001:2006 E ISO/IEC 21827 (SSE-CMM). 5.1. Um modelo de referência para o desenvolvimento de SGSI. 5.2. A integração das normas ISO/IEC 27001:2006 e ISO/IEC 21827 (SSE-CMM). 5.3 A abrangência das normas de segurança no contexto organizacional. 6 Conclusão. 7.References.

**Resumo:** As organizações estão cada vez mais buscando implementar sistemas de gestão da segurança da informação que estejam atrelados às normas de segurança. No entanto, se desconhece a relação existente entre as normas de segurança propostas pela literatura, e se essas podem ser usadas em conjunto de forma a trazer maiores garantias de proteção. Neste artigo serão analisadas duas normas de segurança, a ISO/IEC 21007:2006 e a ISO/IEC 21827, que são recomendadas para o desenvolvimento da gestão da segurança da informação. Cada norma será descrita e discutida com o intuito de encontrar evidências que forneçam as organizações uma visão conjunta do propósito de implantação de cada norma. O artigo relaciona e integra as normas de forma a auxiliar as organizações no estabelecimento e manutenção de sistemas de gestão da segurança da informação que possam atender as necessidades organizacionais. Também será discutida a Instrução Normativa GSI Nº 1, de 13 de junho de 2008, que trata disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, a fim de relacioná-la com a utilização das normas de segurança.

**Palabras clave:** 1. Gestão da Segurança da Informação. 2. ISO/IEC 27001:2006. 3. ISO/IEC 21827. 4. ISO/IEC 17799:2005. 5. Normas de Segurança. 6. Instrução Normativa GSI Nº 1.

**Abstract:** Organizations are increasingly looking to implement systems for managing information security that are tied to safety standards. However, if you know the relationship between safety standards proposed in the literature, and these can be used together in order to bring greater assurance of protection. In this article, we analyze two security standards, ISO / IEC 21007:2006 and ISO / IEC 21827, which are recommended for the development of the management of information security. Each standard is described and discussed in order to find evidence that the organizations provide a comprehensive view of the purpose of implementation of each standard. The article relates and integrates the standards in order to assist organizations in establishing and maintaining management systems for information security that can meet organizational needs. He will also discuss GSI Instruction No. 1, June 13, 2008, which is subject to Security Management of Information and Communications in the Federal Public Administration, directly or indirectly, to relate it to the use of safety.

**Keywords:** 1. Management of Information Security. 2. ISO / IEC 27001:2006. 3. ISO / IEC 21827. 4. ISO / IEC 17799:2005. 5. Safety Standards. 6. GSI Instruction No. 1.

---

<sup>1</sup> Programa de Pós-Graduação em Engenharia de Produção (PPGEP) - Universidade Federal de Santa Maria (UFSM)- Santa Maria, RS - Brasil, josi.unc@gmail.com

<sup>2</sup> Laboratório de Computação Aplicada (LaCA) – Universidade Federal de Santa Maria (UFSM) Santa Maria, RS - Brasil, marcosdornellas@gmail.com

<sup>3</sup> Laboratório de Computação Aplicada (LaCA) – Universidade Federal de Santa Maria (UFSM) Santa Maria, RS - Brasil, lisandramf@gmail.com

## **1 Introdução**

Há inúmeras razões para se desenvolver sistemas de gestão da segurança da informação (SGSI), dentre elas garantir a continuidade dos negócios, a boa reputação, a proteção dos ativos, o cumprimento de leis e regulamentações, o fortalecimento dos objetivos do negócio, a minimização dos riscos entre outras (WIANDER, 2007). Sem o SGSI, as organizações podem sofrer as consequências de violações causadas pela falta de segurança.

A falta de segurança produz o descontentamento tanto dos clientes como dos próprios funcionários da organização, gerando danos financeiros e morais que em muitas situações são irreparáveis. Para o desenvolvimento das organizações e de suas soluções, a implementação da gestão da segurança da informação é um elemento fundamental para o sucesso (BEZERRA; NAKAMURA; RIBEIRO, 2006).

As organizações que buscam desenvolver um SGSI procuram suporte nas documentações de segurança. Há várias ferramentas, métodos, checklists e normas para a construção de sistemas de gerenciamento da segurança da informação (WIANDER, 2007). A norma ISO/IEC 27001:2006 é uma referência para o desenvolvimento de SGSI e se estabelece como um guia para a organização (ABNT NBR ISO/IEC 27001, 2006). Outra norma que também é usada para o desenvolvimento de SGSI é ISO/IEC 21827 (SSE-CMM) que é voltada ao projeto de engenharia da segurança, sendo de grande valia para implementação de processos de segurança (SSE-CMM, 2003). Ambas as normas, são distintas e se desconhece a relação que uma norma de segurança possui com a outra e como ambas podem contribuir para garantir e fortalecer a segurança das informações.

Neste artigo serão descritas e analisadas as normas ISO/IEC 27001:2006 e a ISO/IEC 21827(SSE-CMM) buscando relacioná-las de forma que se possa compreender o processo de implementação e estabelecimento de cada uma. O objetivo é verificar como essas normas podem ser integradas para o desenvolvimento de um SGSI que forneça maiores garantias de proteção. Também será analisada a abordagem e a estrutura que cada uma fornece para o seu desenvolvimento. Ainda serão evidenciados os benefícios que podem obtidos através da integração de normas de segurança.

Este artigo está organizado da seguinte forma: na seção 2, são apresentados os aspectos de desenvolvimento de um SGSI. Na seção 3, são apresentadas as normas ISO/IEC 27001:2006 e ISO/IEC 21827 com suas estruturas e abordagens de implantação. Na seção 4, as normas são analisadas, discutidas e relacionadas. Na seção 5, é mostrado como as normas descritas podem ser integradas, quais os benefícios provenientes dessa combinação e também é feita uma discussão sobre a metodologia definida pela Instrução Normativa GSI N° 1. Por fim, a seção 6 traz as conclusões obtidas com o desenvolvimento do estudo.

## **2 O Desenvolvimento de Sistemas de Gestão da Segurança da Informação (SGSI)**

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

componentes de segurança requeridos para um sistema ser implementado cuidadosamente, evitando o ataque de ameaças e a exposição a riscos, é chamado de SGSI (DEY, 2007).

O desenvolvimento de um SGSI não é uma tarefa fácil (DEY, 2007). As organizações devem analisar e projetar 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 projeto de SGSI é 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 dado 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, 2007). Sem a implementação adequada dos controles ou sem o apoio das normas de segurança, um SGSI pode não atender às necessidades de segurança organizacionais.

### **3 Normas da Segurança**

As normas de segurança fornecem uma abordagem de gerenciamento sistemática adotada para 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 (DEY, 2007).

Nesta seção serão apresentadas duas normas de segurança, a ISO/IEC 27001:2006 recomendada pela Instrução Normativa GSI N° 1 e a ISO/IEC 21827 indicada para a melhoria dos processos de segurança organizacionais. Essas normas terão descritos seus propósitos e estruturas de desenvolvimento.

#### **3.1 Norma ISO/IEC 27001:2006**

A norma ISO/IEC 27001:2006 foi construída baseada na norma britânica BS7799 e na ISO/IEC 17799 (ABNT NBR ISO/IEC 27001, 2006). Seu objetivo é proporcionar um modelo para o estabelecimento, implementação, funcionamento, acompanhamento, revisão, manutenção e melhoria de um SGSI documentado dentro do contexto dos riscos de negócio globais da organização (FENZ et al, 2007). Ela pode ser aplicada em todos os tipos de organizações como por exemplo, empreendimentos comerciais, agências governamentais, organizações sem fins lucrativos, 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 (ABNT NBR ISO/IEC 27001, 2006).

O SGSI projetado 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 27001:2006 são encontrados na norma ISO/IEC 17799:2005. A norma

ISO/IEC 17799:2005 está contida na ISO/IEC 27001:2006, ou seja, a norma ISO/IEC 27001:2006 fornece um processo definido de implantação dos controles da norma ISO/IEC 17799:2005.

A norma ISO/IEC 27001:2006 aplica um sistema de processos dentro de uma organização, junto com a identificação e interações destes processos. Essa abordagem de processos enfatiza a importância dos seguintes aspectos:

- Entendimento dos requisitos de segurança da informação de uma organização e da necessidade de estabelecer uma política e objetivos para a segurança de informação;
- Implementação e operação de controles para gerenciar os riscos de segurança da informação de uma organização no contexto dos riscos de negócio globais da organização;
- Monitoração e análise crítica do desempenho e eficácia do SGSI; e
- Melhoria contínua baseada em medições objetivas.

A norma ISO/IEC 27001:2006 incorpora o ciclo Plan-Do-Check-Act (PDCA), que é adotado em toda a estrutura dos processos do SGSI. O ciclo PDCA baseia-se no ciclo de melhoria contínua que consiste em planejar (Plan – P), fazer (Do – D), checar (Check – C) e agir (Act – A). O ciclo PDCA é uma ferramenta importante para a análise e melhoria dos processos organizacionais contribuindo pra a tomada de decisões gerenciais e para o alcance das metas e objetivos da organização (KAJAVA et al, 2006).

### 3.2 Norma ISO/IEC 21827 (SSE-CMM)

A norma ISO/IEC 21827 ou modelo SSE-CMM (Systems Security Engineering Capability Maturity Model) foi desenvolvida pelo ISSEA (International Systems Security Engineering Association) em 1999. Esta norma descreve as características essenciais que um processo de engenharia da segurança da informação deve possuir para assegurar a boa segurança (SSE-CMM, 2003).

A norma ISO/IEC 21827 não prescreve uma sequência ou um processo particular, mas captura as práticas que são geralmente observadas na indústria. Esta norma é designada para todos os tipos de organizações, sendo usada para a melhoria e avaliação da capacidade de maturidade dos processos de segurança (SG-SBP, 2008).

A estrutura de desenvolvimento da norma ISO/IEC 21827 é dada por 22 PAs (Process Areas), divididas em dois grupos, Práticas Base de Segurança e Práticas Base Organizacionais e do Projeto. A estrutura de distribuição das PAs em seus grupos correspondentes pode ser vista na Tabela 1:

Tabela 1- Estrutura de distribuição da PAs da norma ISO/IEC 21827.

| <b>Categorias</b>          | <b>PAs (Process Áreas)</b>                |
|----------------------------|---|
| Práticas Base de Segurança | PA01 - Administrar controles de segurança |
|                            | PA02 - Avaliar impacto                    |
|                            | PA03 - Avaliar riscos de segurança        |
|                            | PA04 - Avaliar ameaças                    |
|                            | PA05 - Avaliar vulnerabilidades           |
|                            | PA06 - Construir argumentos de segurança  |
|                            | PA07 - Coordenar a segurança              |
|                            | PA08 - Monitorar a postura da segurança   |
|                            | PA09 - Estabelecer a entrada de segurança |

|  |  |
|--|--|
|  | PA10 - Especificar necessidades de segurança                       |
|  | PA11 - Verificar e validar a segurança                             |
|  | PA12 - Assegurar qualidade   |
|  | PA13 - Gerenciar a configuração                                    |
|  | PA14 - Gerenciar riscos do projeto                                 |
|  | PA15 - Monitorar e controlar esforço técnico                       |
|  | PA16 - Planejar esforço técnico                                    |
|  | PA17 - Definir processos de engenharia de sistemas da organização  |
| Práticas Base Organizacionais e do Projeto | PA18 - Melhorar processos de engenharia de sistemas da organização |
|  | PA19 - Gerenciar evolução da linha do produto                      |
|  | PA20 - Gerenciar ambiente de suporte a engenharia de sistemas      |
|  | PA21 - Promover habilidade e conhecimento progressivo              |
|  | PA22 - Coordenar com fornecedores                                  |

A norma ISO/IEC 21827 também define níveis de maturidade dos processos de segurança da organização que são ampliados após o estabelecimento e cumprimento das práticas da segurança (BATISTA, 2007). O processo mais "maduro" define uma organização cujos processos são melhores definidos e conduzidos. São seis níveis de maturidade definidos, onde cada um desses níveis consiste de um número de Práticas Genéricas - GP (Generic Practices) que suportam o desempenho das PAs. Os níveis de maturidade atribuídos pela norma ISO/IEC 21827 são:

- Nível 0 - Práticas base não são realizadas;
- Nível 1 - Práticas base são realizadas informalmente;
- Nível 2 - Práticas base são planejadas e monitoradas;
- Nível 3 - Práticas base estão bem definidas;
- Nível 4 - Práticas base são controladas quantitativamente;
- Nível 5 - Práticas base estão em contínua melhoria.

O processo de melhoria e maturidade organizacional da norma ISO/IEC 21827 é realizado por meio do modelo IDEAL que foi desenvolvido pelo SEI - Software Engineering Institute e é usado para definir ações que capacitem as organizações a melhorar seus processos. O modelo IDEAL serve como um guia para iniciar, planejar e implementar ações de melhoria. A palavra IDEAL é um acrônimo do inglês para Iniciar (initiating), Diagnosticar (diagnosing), Estabelecer (establishing), Agir (acting) e Aprender (learning). O modelo IDEAL forma uma infra-estrutura de cinco fases para guiar organizações no planejamento e na implementação de um efetivo programa de melhoria de processos (SSE-CMM, 2003).

## 4 Análise das Normas Apresentadas

Para que se possa compreender a relação entre as normas ISO/IEC 27001:2006 e ISO/IEC 21827 foram realizadas duas comparações. Na primeira comparação, as características da norma ISO/IEC 27001:2006 são comparadas com as normas ISO/IEC 21827. Na segunda comparação, são identificados os controles da norma ISO/IEC 17799:2005 que correspondem as PAs da norma ISO/IEC 21827. As informações para critério de comparação foram obtidas dos documentos ABNT NBR ISO/IEC 27001:2006 (ABNT NBR 27001, 2006), ABNT NBR ISO/IEC 17799:2005 (NBR ISO/IEC 17799, 2005) e Systems Security Engineering Capability Maturity Model (SSE-CMM) Model Description Document version 3.0 (SSE-CMM, 2003).

Com resultado da primeira comparação, foi observado que as normas apresentam duas visões que estão permanentemente presentes antes e depois do SGSI ser implementado: a visão funcional e a visão de processos. A visão funcional é representada pela norma ISO/IEC 27001:2006 que fornece uma estrutura de recomendações que deve ser seguida para o desenvolvimento de um SGSI. Já a norma ISO/IEC 21827 representa uma visão de processos, que fornece as práticas que devem ser implementadas para a construção de um SGSI.

Com relação ao ciclo de melhoria, que indica uma ferramenta de qualidade para o desenvolvimento da norma, verifica-se que a ISO/IEC 27001:2006 utiliza o ciclo de melhoria PDCA para a análise e melhoria dos processos organizacionais, enquanto a ISO/IEC 21827 utiliza o modelo IDEAL. Ambos os modelos consistem em um ciclo de atividades modelado para guiar a melhoria contínua e para desenvolvimento adequado de cada norma.

Tanto a norma ISO/IEC 27001:2006 como a norma ISO/IEC 21827 podem ser adotadas por qualquer tipo de organização, seja ela de pequeno ou grande porte. Isso indica que não há restrições quanto ao uso das normas e a escolha de aderir a uma ou a outra norma de segurança, deve ser direcionada ao atendimento dos objetivos de segurança organizacionais.

O desenvolvimento da norma ISO/IEC 27001:2006 está baseada na implementação dos controles de segurança contidos na ISO/IEC 17799:2005. Dessa forma, a ISO/IEC 27001:2006 implementa a ISO/IEC 17799:2005. Na ISO/IEC 21827 não há um documento de segurança complementar para o seu desenvolvimento. Ela é implantada por meio da implementação das PAs e é avaliada pelo método SSAM (SSE-CMM Appraisal Method).

Uma característica importante da ISO/IEC 21827 é o uso das métricas para avaliar os processos de segurança e estabelecer níveis de maturidade. Essa característica está voltada ao gerenciamento da segurança. Já a norma ISO/IEC 27001:2006 foi projetada para permitir a uma organização alinhar ou integrar seu SGSI com requisitos de sistemas de gestão relacionados.

As características da norma ISO/IEC 27001:2006 e da norma ISO/IEC 21827 mencionadas anteriormente podem ser vistas no quadro comparativo da Tabela 2:

Tabela 2 - Quadro comparativo de características das normas ISO/IEC 27001:2006 e ISO/IEC 21827

| Principais características      | Normas   |   |
|---------------------------------|--|---|
|                                 | ISO/IEC 27001:2006   | ISO/IEC 21827   |
| Propósito da norma              | Estabelecer, revisar, implementar, acompanhar, manter e melhorar um SGSI | Descrever características de segurança de um processo |
| Ferramenta de qualidade         | PDCA   | IDEAL   |
| Organização que podem fazer uso | Todas  | Todas   |
| Norma de complemento            | ISO/IEC 17799:2005   | Não apresenta   |
| Recursos de gerenciamento       | Controles da ISO/IEC 17799:2005  | Métricas  |
| Visão de implementação          | Controles de segurança   | Processos de segurança                                |
| Base de implementação           | Controles da ISO/IEC 17799:2005  | Áreas do Processo (PAs)                               |
| Pré-condição de implementação   | Não apresenta  | Não apresenta   |
| Principal característica        | Fornecimento de um conjunto de recomendações de segurança                | Melhoria dos processos de segurança                   |

A segunda comparação foi realizada entre as normas ISO/IEC 21827 e ISO/IEC 17799:2005. A norma ISO/IEC 17799:2005 está contida na norma ISO/IEC

27001:2006, sendo que as recomendações de segurança da norma ISO/IEC 27001:2006 implicam na implementação dos controles da ISO/IEC 17799:2005.

Para essa comparação foram selecionadas 11 PAs referentes as Práticas Base de Segurança da norma ISO/IEC 21827 e foram selecionados controles da norma ISO/IEC 17799:2005. O critério adotado para identificar os controles relacionados com as PAs foi baseado no atendimento dos objetivos e requisitos (Base Practice - BP) de cada PA. Também foi usado como critério de comparação a literatura relacionada as normas e nas publicações oficiais da ABNT e do SEI. Na Tabela 4 são apresentados os controles da ISO/IEC 17799:2005 que estão relacionados com as PAs da ISO/IEC 21827:

| <b>ISO/IEC 27001</b>                            | <b>ISO/IEC 17799:2005</b>   |
|---|---|
| Descrição das PAs                               | Controles relacionados  |
| PA01 – Administração dos controles de segurança | Documento da política de segurança da informação;<br>Atribuição de responsabilidades para a segurança da informação;<br>Processo de autorização para os recursos de processamento da informação;<br>Recomendações para classificação;<br>Rótulos e tratamento da informação;<br>Papéis e responsabilidades;<br>Responsabilidades da direção;<br>Consientização, educação e treinamento em segurança da informação;<br>Documentação dos procedimentos de operação;<br>Gestão de mudanças;<br>Gerenciamento de mudanças para serviços terceirizados;<br>Procedimentos para tratamento de informação;<br>Gerenciamento de privilégios;<br>Gerenciamento de senha do usuário;<br>Sistema de gerenciamento de senha;<br>Prevenção de mau uso de recursos de processamento da informação; |
| PA02 - Avaliação do impacto                     | Apresentado no item 4 referente à Introdução da norma ISO/IEC 17799:2005;   |
| PA03 - Avaliação dos riscos de segurança        | Identificação dos riscos relacionados com partes externas;<br>Inventário dos ativos;<br>Proprietário dos ativos;<br>Uso aceitável dos ativos;<br>Apresentado no item 4 referente à Introdução da norma ISO/IEC 17799:2005;  |
| PA04 - Avaliação de ameaças                     | Apresentado no item 4 referente à Introdução da norma ISO/IEC 17799:2005;   |
| PA05 - Avaliação de vulnerabilidades            | Apresentado no item 4 referente à Introdução da norma ISO/IEC 17799:2005;   |
| PA06 - Construção de argumentos de garantia     | Identificando a segurança da informação, quando tratando com os clientes;   |
| PA07 - Coordenação da segurança                 | Acordos de confidencialidade;<br>Identificando segurança da informação nos acordos com terceiros;<br>Segregação de funções;<br>Acordos para a troca de informações;<br>Procedimentos para controle de mudanças;<br>Conformidade com as políticas e normas de segurança da informação;   |
| PA08 - Monitoração da postura da segurança      | Comprometimento da direção com a segurança da informação;<br>Coordenação da segurança da informação;<br>Contato com autoridades;  |

|   |   |
|---|---|
|   | <p>Análise crítica independente de segurança da informação;<br/> Gestão de capacidade;<br/> Controles contra códigos maliciosos;<br/> Controles contra códigos móveis;<br/> Registros de auditoria;<br/> Monitoramento do uso do sistema;<br/> Proteção das informações dos registros (<i>log</i>);<br/> Registros (<i>log</i>) de administrador e operador;<br/> Registros (<i>log</i>) de falhas;<br/> Vazamento de informações;<br/> Controle de vulnerabilidades técnicas;<br/> Controles de auditoria de sistemas de informação;</p>   |
| PA09- Fornecer a entrada segurança              | <p>Documento da política de segurança da informação;<br/> Análise crítica da política de segurança da informação;<br/> Processo disciplinar;<br/> Políticas e procedimentos para troca de informações;<br/> Política de controle de acesso;<br/> Registro de usuário;<br/> Restrição de acesso à informação;<br/> Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação;</p>  |
| PA10 - Especificar as necessidades de segurança | <p>Segurança da documentação dos sistemas;<br/> Uso de senhas;<br/> Autenticação para conexão externa do usuário;<br/> Procedimentos seguros de entrada no sistema (<i>log-on</i>);<br/> Identificação e autenticação de usuário;<br/> Análise e especificação dos requisitos de segurança;<br/> Integridade de mensagens;<br/> Incluindo segurança da informação no processo de gestão da continuidade de negócio;<br/> Continuidade de negócios e análise/avaliação de riscos;<br/> Estrutura do plano de continuidade do negócio;<br/> Identificação da legislação vigente;<br/> Direitos de propriedade intelectual;<br/> Proteção de dados e privacidade de informações pessoais;<br/> Proteção de ferramentas de auditoria de sistemas de informação;</p> |
| PA11 - Verificação e validação da segurança     | <p>Entrega de serviços;<br/> Monitoramento e análise crítica de serviços terceirizados;<br/> Cópias de segurança das informações;<br/> Análise crítica dos direitos de acesso de usuário;<br/> Validação dos dados de entrada;<br/> Controle do processamento interno;<br/> Validação de dados de saída;<br/> Testes, manutenção e reavaliação dos planos de continuidade do negócio;<br/> Verificação da conformidade técnica.</p>   |

Foi observado que nem todos os controles da ISO/IEC 17799:2005 possuem uma relação direta com as PAs da ISO/IEC 21827. Os controles manuseio de mídias, serviço de comércio eletrônico, controles criptográficos, computação móvel e de trabalho remoto e alguns outros, não estão contidos na Tabela 3 por não terem ligação aparentemente direta com o objetivos da PAs.

No entanto, a implementação de um projeto de SGSI recomendado pela norma ISO/IEC 27001:2006 está condicionado as necessidades de segurança organizacionais e portanto, nem todos os controles de segurança tem obrigatoriedade de

implementação. Na norma ISO/IEC 21827, as PAs também são selecionadas objetivando atender as necessidades de segurança organizacionais e podem ser selecionadas PAs tanto da categoria de Práticas Base de Segurança como do grupo Práticas Base Organizacionais e do Projeto.

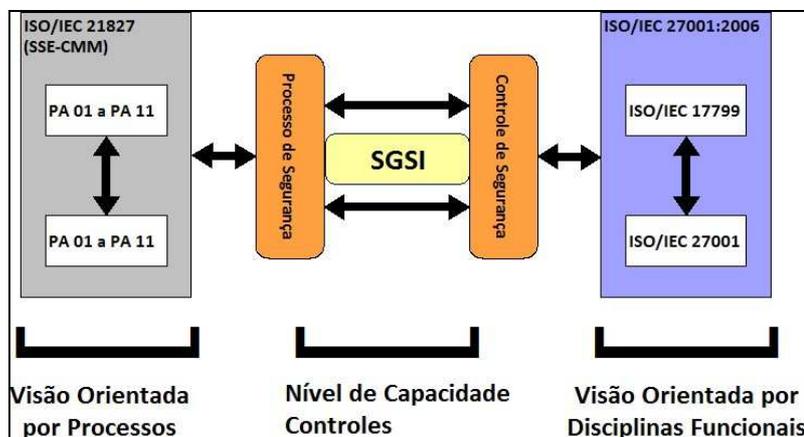
## 5 Combinação das Normas De Segurança ISO/IEC 27001:2006 E ISO/IEC 21827 (SSE-CMM)

### 5.1 Um modelo de referência para o desenvolvimento de SGSI

A Figura 1 apresenta a integração da norma ISO/IEC 27001:2006 e a norma ISO/IEC 21827 no modelo de referência, onde se pode observar:

- Visão orientada por disciplinas funcionais: no modelo diferenciam-se seis disciplinas funcionais incluindo a segurança fundamental, segurança ambiental e de infraestrutura, segurança dos sistemas, segurança em comunicações e redes, segurança física e segurança pessoal;
- Visão orientada por processos: no modelo estão identificados oito sub-processos de segurança incluindo a gestão estratégica da segurança, cumprimento legal e padrões aplicáveis, identificação, classificação e avaliação de ativos, análise e avaliação de riscos de segurança, tratamento e gestão de riscos de segurança, gestão da segurança operacional, segurança das operações – condições normais e segurança das operações – condições anormais;
- Segurança Fundamental: Observando a Tabela 4, podemos observar que a mesma contém um conjunto de controles e sub-processos definidos em ambas as normas ISO/IEC 21827 e ISO/IEC 27001:2006 que são imprescindíveis para que o processo de segurança exista não só na melhoria da sua capacidade, mas também das necessidades específicas de segurança em áreas concretas do negócio. Os controles e sub-processos indicados neste nível são comuns para o resto das áreas funcionais.

Figura 1: Integração da norma ISO/IEC 27001:2006 com a norma ISO/IEC 21827 no modelo de referência (HUMPHREYS, 2007).



Este modelo, em que se integram ambas as visões de segurança, deriva-se da base de conhecimentos Theoretical and Practical Knowledge Base (TPKB) produzida pelo International Systems Security Professional Certification Scheme (ISSPCS), o qual colabora com o International Systems Security Engineering Association (ISSEA).

| Processo de Segurança nas Organizações | 1. Gestão Estratégica da Segurança | 2. Concordância e Normas Aplicáveis                                 | 3. Identificação, Classificação e Avaliação de Ativos                   | 4. Análise e Avaliação de Riscos de Segurança | 5. Tratamento e Gestão de Riscos de Segurança     | 6. Gestão da Segurança Operacional | 7. Segurança em Operações – Normais                                     | 8. Segurança em Operações – Anormais                              |  |
|--|------------------------------------|---|---|---|---|------------------------------------|---|---|--|
| Disciplinas Funcionais                 | Segurança Fundamental              | A5 (completo)<br>A6.1 (1,2,3,7)<br>PA 06 07<br>PA 09 10<br>PA 11 10 | A 15.1<br>A 5.1.5<br>A 6.2.3<br>A 8.1.1.3<br>A 10.8.2<br>PA 10<br>PA 11 | A 7 (completo)<br>PA 02<br>PA10               | A 6.2.1<br>A 14.1.2<br>PA 02 03<br>PA 04<br>PA 05 | A 6.1.8<br>A 6.2.2<br>PA 03        | A 9.1<br>A 10 (1,2,3)<br>A 11.2<br>A 11.6<br>PA 01 07<br>PA 08<br>PA 11 | A 6.1 (4,6,7)<br>A 10 (4,5,6)<br>A10 (7,8,9)<br>PA 07 09<br>PA 10 | A 13 (completo)<br>A 14 (completo)<br>PA 06<br>PA 10 |
|  | Ambiental e Infraestrutura         | PA 06 07<br>PA 09 10<br>PA 11 10<br>PA 02                           | PA 10 11<br>PA 02   | PA 02 PA 10<br>PA 09                          | PA 02 03<br>PA 04 05<br>PA 09                     | PA 03<br>PA 09<br>PA 10            | A 9.2<br>PA 01 07<br>PA 08<br>PA 11                                     | PA 07 09<br>PA 10   | PA 06 10<br>PA 07<br>PA 09                           |
|  | Segurança dos Sistemas             | A 12.1<br>PA 06 07<br>PA 09 10<br>PA 11                             | A 15.2<br>A 15.3<br>PA 10<br>PA 11                                      | PA 02 PA 10                                   | PA 02 03<br>PA 04<br>PA 05                        | A 12.2<br>A 12.3<br>PA 03          | A 11.5<br>A 11.7<br>A 12.4<br>A 12.5<br>PA 01 07<br>PA 08<br>PA 11      | A 12.6<br>PA 07 09<br>PA 10                                       | PA 06<br>PA 10                                       |
|  | Comunicações e Operações           | PA 06 07<br>PA 09 10<br>PA 10 11<br>PA 01<br>PA 08                  | PA 10 11<br>PA 02   | PA 02 PA 10                                   | PA 02 03<br>PA 04<br>PA 05                        | PA 03                              | A 11.4<br>PA 01 07<br>PA 08 11<br>PA 09<br>PA 10                        | A 10.10<br>PA 07 09<br>PA 10                                      | PA 06 07<br>PA 10                                    |
|  | Segurança Física                   | PA 06 07<br>PA 09 10<br>PA 11                                       | PA 10<br>PA 11  | A 9 (completo)<br>PA 02 PA 10                 | PA 02 03<br>PA 04<br>PA 05                        | PA 03                              | PA 01 07<br>PA 08<br>PA 11  | A 6.2 (1,2)<br>PA 07 09<br>PA 10                                  | PA 06<br>PA 10                                       |
|  | Segurança Pessoal                  | PA 06 07<br>PA 09 10<br>PA 11                                       | PA 10<br>PA 11  | PA 02 PA 10                                   | A 8.1<br>PA 02 03<br>PA 04<br>PA 05               | A 8.2<br>PA 03                     | A 11.3<br>PA 01 07<br>PA 08<br>PA 11                                    | A 8.3<br>PA 07 09<br>PA 10  | PA 06<br>PA 10                                       |

## 5.2 A integração das normas ISO/IEC 27001:2006 e ISO/IEC 21827 (SSE-CMM)

A relação da norma ISO/IEC 27001:2006 com a ISO/IEC 21827 está baseada no estabelecimento de maiores garantias de proteção. Cada norma fornece meios para assegurar o desenvolvimento da segurança de forma sistemática e contínua.

A norma ISO/IEC 17799:2005 que fornece os controles recomendados pela norma ISO/IEC 27001:2006 foi comparada com as PAs da ISO/IEC 21827 para se verificar a similaridade de processos. A partir dessa comparação nota-se que alguns controles não estão diretamente ligados com a ISO/IEC 21827. Com isso, pode ser observado que a ISO/IEC 21827 é mais indicada para o gerenciamento de processos de segurança e não para a sua definição dos processos (controles) que serão implementados.

A definição dos controles de segurança que serão implementados pelo SGSI seguem a estrutura de segurança organizacional, podendo alguns controles serem selecionados e outros não. O mesmo acontece com as PAs da ISO/IEC 21827, onde nem todas as PAs são selecionadas e procura-se fazer a seleção de acordo com a necessidade de segurança organizacional. Dessa maneira, os controles que são selecionados da ISO/IEC 17799:2005 recomendados pela ISO/IEC 27001:2006 podem ganhar níveis de maturidade por meio da implementação da ISO/IEC 21827.

A integração das normas está no desenvolvimento em conjunto das normas. Ganhando níveis de maturidade, os controles da ISO/IEC 17799:2005 podem ser gerenciados e monitorados assegurando o aprimoramento da segurança organizacional. Cada organização pode definir seus objetivos de segurança selecionando controles e determinando níveis de maturidade que atendam suas necessidades de segurança.

A integração das normas ISO/IEC 27001:2006 e ISO/IEC 21827 pode trazer benefícios para as organizações, onde se pode observar:

- Melhoria nos aspectos de definição da segurança fundamental: em uma organização que não tenha definido o processo global de segurança, a primeira etapa deveria ser defini-lo, levando em consideração os sub-processos de segurança e controles que são propostos no modelo de referência;
- Desenvolvimento de projetos SGSI específicos: em organizações científicas como laboratórios ou empresas de desenvolvimento de software com processos de negócio especializado os projetos de SGSI poderiam ser desenvolvidos com o objetivo de aprofundar as relações da norma ISO/IEC 21827. Este conhecimento é importante tanto para conhecer melhor as necessidades de segurança requisitadas por estes setores da economia, como também, as dificuldades inerentes aos setores facilitando a criação de padrões para o desenvolvimento de soluções de segurança setoriais;
- Determinação de níveis de maturidade para os processos de segurança: em um projeto de SGSI, deve-se exigir que o processo global de segurança projetado e implementado possa ser avaliado como nível maior de maturidade. Um SGSI de nível 1 teria deficiências. Com a utilização da ISO/IEC 21827 é possível estipular o nível de capacidade que se deseja alcançar;
- Atendimento dos requisitos legislativos: uma vez que tanto as leis quanto seus regulamentos levam em consideração os processos de segurança da informação, os projetos poderiam revisar as próprias leis conforme a visão de processos de segurança assim como identificar as falhas que a norma pode apresentar para compreendê-las, melhorá-las e aplicá-las;
- Redução de custos: com a implementação de controles monitorados pela ISO/IEC 21827, pode-se assegurar a redução de falhas de segurança e conseqüentemente a diminuição de recursos financeiros aplicados para reparação de danos;
- Definição de estratégias de segurança: o gerenciamento dos processos de segurança fornece uma visão do quadro de segurança atual da organização,

fornecendo subsídios para a implementação de medidas preventivas que assegurem o bem estar organizacional;

- Reconhecimento organizacional: a certificação por normas reconhecidas no ambiente de segurança garante maior confiabilidade por parte de clientes, colaboradores e terceiros.

### 5.3 *A abrangência das normas de segurança no contexto organizacional*

Desenvolver um SGSI que forneça garantias de segurança não está atrelado apenas ao uso de uma norma. Uma norma de segurança pode satisfazer inúmeros requisitos de segurança, mas não pode abranger todos os aspectos que asseguram proteção.

A Instrução Normativa GSI Nº 1, de 13 de junho de 2008 que trata disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, têm o propósito de manter seguras as informações e orientar a condução de políticas de segurança da informação e comunicações pelos órgãos da Administração Pública Federal, direta e indireta. Cumprindo o art. 3 da Instrução Normativa GSI Nº 1, o Gabinete de Segurança Institucional da Presidência da República-GSI ficou responsável por orientar a condução da Política de Segurança da Informação e Comunicações. Ficou então definido pelo GSI, que a metodologia de gestão de segurança da informação e comunicações deve basear-se no processo de melhoria contínua, denominado ciclo “PDCA” (Plan-Do-Check-Act), estabelecido pela norma ISO/IEC 27001:2006 e todos os órgãos da Administração Pública Federal, direta e indireta, devem adotá-la. A escolha realizada pelo GSI levou em consideração três critérios:

- Simplicidade do modelo;
- Compatibilidade com a cultura de gestão de segurança da informação em uso nas organizações públicas e privadas brasileiras; e
- Coerência com as práticas de qualidade e gestão adotadas em órgãos públicos brasileiros.

No entanto, o GSI não leva em consideração que as organizações possuem necessidades de segurança diferentes. O que pode ser adaptado consideravelmente bem para uma organização, pode não ser tão bem adaptado para outra.

Definir uma metodologia para a gestão da segurança da informação baseada na aplicação de apenas uma norma pode deixar lacunas na segurança, resultando em futuras falhas de segurança, danos financeiros e sociais.

Além disso, uma norma não pode ser recomendada para todo e qualquer tipo de organização. As organizações são diferentes, possuem necessidades de segurança específicas e estão em outro contexto cultural. Em muitos casos, a relação de uma organização com uma norma de segurança não se completa. Isso ocorre não pela inconsistência da segurança fornecida por uma norma, mas pelo fato da organização possuir objetivos vinculados as necessidades de segurança próprias.

A utilização de uma única norma de segurança pode trazer benefícios agregando mais proteção a organização, mas de fato, ela não preenche e nem se enquadra a todos os aspectos de segurança necessários para fornecer controle sobre todos os aspectos de segurança organizacional.

As normas de segurança se complementam, de forma a fornecer maiores garantias de segurança. Com a integração das normas de segurança as organizações podem focar seus objetivos de proteção, prevenindo que incidentes de segurança ocorram. A integração das normas que se dá pela combinação da segurança pode adequar-se a maioria das organizações e se enquadrar em um contexto específico.

## 6 Conclusão

O presente trabalho discutiu o desenvolvimento de um SGSI através da integração das normas ISO/IEC 27001:2006 e ISO/IEC 21827. Buscou-se verificar como essas normas podem ser integradas de modo proporcionar maiores garantias de segurança as organizações.

Pode-se observar que a norma ISO/IEC 27001:2006 fornece uma estrutura bem definida para a implementação de um SGSI, enquanto a norma ISO/IEC 21827 pode ser usada para assegurar que os processos de segurança sejam desenvolvidos e mantidos em conformidade com a segurança, adquirindo níveis de maturidade. Neste sentido, a integração das normas ISO/IEC 27001:2006 e ISO/IEC 21827 pode ser utilizada com um modelo de referência para o desenvolvimento de processos de SGSI.

Com a existência de vários documentos de segurança, destes incluem o NIST, CSE, BS 7799, ISO/IEC 13335 entre outros, a ISO/IEC 21827 pode ser entendida como um sistema para a descrição das características essenciais do processo de engenharia de segurança da organização, que sempre deve existir para assegurar a boa engenharia de segurança. As organizações de segurança podem usar o ISO/IEC 21827 para avaliar e refinar as práticas de engenharia de segurança; os clientes podem usá-lo para avaliar o recurso de engenharia de segurança de um dado sistema; e as organizações de avaliação de engenharia, para estabelecer valores organizacionais com base nos recursos.

A ISO/IEC 21827 deve ser usada pelas organizações para examinar a maturidade de um processo de segurança de tecnologia da informação implementado em uma organização em comum acordo com a ISO/IEC 27007:2006 ou um dos documentos acima citados. Desta forma, a ISO/IEC 21827 pode e deve ser usada em conjunto com qualquer documento de segurança.

## 7 References

BATISTA, Carlos F. A., 2007. Métricas de Segurança de Software. Dissertação do Programa de Pós-graduação em Informática do Departamento de Informática da PUC-Rio. Universidade Pontifícia Católica, Rio de Janeiro.

BEZERRA, Edson K.; NAKAMURA, Emílio T.; RIBEIRO, Sérgio L., 2006. Maximizando Oportunidades com Gestão de Segurança e Gerenciamento de Riscos. Disponível em [www.cpqd.com.br/file.upload/6-sic-1-artigoforum-riscos.pdf](http://www.cpqd.com.br/file.upload/6-sic-1-artigoforum-riscos.pdf). Acessado em junho de 2009.

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

FENZ, Stefan; GOLUCH, Gernot; EKELHART, Andreas; RIEDL, Bernhard; WEIPPL, Edgar, 2007. Information Security Fortification by Ontological Mapping of the ISO/IEC

27001 Standard. 13th IEEE International Symposium on Pacific Rim Dependable Computing.

HANAHIRO, Maíra, 2007. Metodologia para Desenvolvimento de Procedimentos e Planejamento de Auditorias de TI Aplicadas à Administração Pública Federal. Dissertação de mestrado em engenharia elétrica. Universidade de Brasília-UnB.

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

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

KAJAVA, Jorma; ANTTILA, Juhani; VARONEN, Rauno; SAVOLA, Reijo; RONING, Juha, 2006. Information Security Standards and Global Business. Industrial Technology, 2006. ICIT 2006. IEEE International Conference.

NBR ISO/IEC 17799, 2005. Tecnologia da Informação. Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro.

NBR ISO/IEC 27001, 2006. Tecnologia da Informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos. Associação Brasileira de Normas. Rio de Janeiro.

SG-SBP, 2008. Recommendation for Creating a Comprehensive Framework for Risk Management and Compliance in the Financial Services and Insurance Industries. Information Technology Industry Council (ITI). Disponível em < [www.incits.org/tc\\_home/sbp.htm](http://www.incits.org/tc_home/sbp.htm)> Acessado em junho de 2009.

WIANDER, Timo, 2007. ISO/IEC 17799 Standard's Intended Usage and Actual Use by the Practitioners. 18th Australasian Conference on Information Systems. Toowoomba, 5-7.