Avaliação de Segurança da Informação Usando o Modelo ITMark

Marcelo Pereira da Silva
Instituto SENAI de Tecnologia
Londrina, Paraná, Brasil

Jacques Duilio Brancher
Universidade Estadual de Londrina
Londrina, Paraná, Brasil

***Abstract* — The implementation of quality models has become common practice in micro and small software companies of the Brazil. Supported by funding programs and improvement projects, these companies obtained benefits for organizing their development processes. Now, these companies seek alternatives to ensure quality in the other organization's processes. One of these is the Information Security, which has become in recent years a major concern for companies. This paper presents the ITMark model highlighting its assessment of the security process, reports the first certifications in Brazil, analyzes of these evaluations and shows that the model to be viable for micro and small companies.**

***Index Terms* — Information Security, ITMark, Software Certification.**

***Resumo* — A implantação de modelos de qualidade se tornou prática comum nas micro e pequenas empresas de software brasileiras. Apoiadas por programas de financiamento e projetos de melhoria, essas empresas obtiveram benefícios por organizarem seus processos de desenvolvimento. Agora, essas empresas buscam alternativas para garantir qualidade nos outros processos da organização. Um destes é a Segurança da Informação, que se tornou nos últimos anos uma grande preocupação das empresas. Este artigo apresenta o modelo ITMark destacando sua avaliação do processo de segurança, relata as primeiras certificações no Brasil, faz uma análise destas avaliações e mostra que o modelo por ser viável para empresas deste porte.**

***Palavras-chave* — Segurança da Informação, ITMark, Certificação de Software.**

I.INTRODUÇÃO

Para muitas empresas brasileiras desenvolvedoras de software, a implantação dos modelos de melhoria de processos é 'demasiadamente pesada'. Assim, somente o implementam por necessidade do mercado[21].

Para atender a necessidade das empresas brasileiras foi criado pela Associação para Promoção da Excelência do Software Brasileiro (SOFTEX), em 2003, o modelo de maturidade denominado MR-MPS-SW [19].

Segundo dados disponibilizados na página da SOFTEX [19], até Dezembro de 2014 já haviam sido feitas 596 avaliações de empresas de software. Isso mostra uma estabilidade no modelo de maturidade para o desenvolvimento de software.

Atingida essa maturidade, as empresas deste segmento estão buscando modelos de qualidade para outros processos internos como Gestão Estratégica e Segurança da Informação (SI).

Entre 2013, empresas brasileiras participaram do projeto RELAIS (Rede Latino Americana da Indústria do Software), o qual um dos objetivos foi a difusão tanto do modelo MR- MPS-SW, no México, Colômbia e Peru quanto o modelo MoProSoft no Brasil, Colômbia e Peru [18].

As cinco primeiras empresas de cada país que concluíram exitosamente o projeto foram contempladas com a avaliação sem custos do modelo internacional ITMark, de acordo com os critérios definidos pelo RELAIS.

O ITMark é um sistema de certificação especialmente concebido para as micro e pequenas empresas (MPEs) contemplando não só o processo de desenvolvimento de software como também a gestão de negócios e a segurança das informações.

Este artigo apresenta um estudo das avaliações do ITMark em quatro empresas brasileiras, já certificadas com outros modelos de qualidade, mostrando que o modelo também pode ser uma solução para o problema de implantação de modelos em conjunto citado por Pardo [15].

Para tal, o presente artigo foi assim estruturado: na Seção 2 apresenta uma fundamentação teórica do trabalho e a caracterização do problema. Também na Seção 2 é apresentado o modelo ITMark, com destaque para a avaliação da SI.

A Seção 3 relata a avaliação feita em quatro empresas brasileiras. Na Seção 4 são comentados os resultados das avaliações. As conclusões e os trabalhos sugeridos para disseminar o modelo no Brasil estão na Seção 5.

II. FUNDAMENTAÇÃO TEÓRICA

Proteger informação tornou-se uma grande preocupação para muitas empresas que, com a dependência cada vez mais do uso da tecnologia, estão expostas a um número crescente de ameaças e vulnerabilidades.

Torna-se então necessário às empresas terem um sistema de gestão de SI eficiente [13], que contemple políticas, processos e gerenciamento dos riscos que envolvem seus ativos de informação.

Hoje em dia, o acesso a informações confiáveis tornou-se um fator essencial que leva ao sucesso nos negócios. A este respeito, a segurança adequada das informações e dos sistemas que a processam é fundamental para o funcionamento de todas as empresas.

Por isso as organizações devem compreender e melhorar o estado atual da sua SI, a fim de garantir a continuidade dos negócios [3]. Para tal, é necessário preservação as três propriedades da SI:

- Confidencialidade: propriedade em que a informação não é revelada para as entidades do sistema se antes não ter sido autorizada.
- Integridade: propriedade em que a informação não é alterada, destruída ou perdida de forma não autorizada ou acidental.

- Disponibilidade: propriedade de um sistema ou recurso do sistema de ser acessível e usável por uma entidade autorizada do sistema segundo as especificações de desempenho do sistema.

A segurança dainformação não tem que ser considerada só como uma solução técnica. Deve ser considerada como um sistema integrado que interage com outros sistemas existentes dentro da organização tais como:

- Regulações – Padrões e Diretivas Legais;
- Estrutura organizacional – Papéis e responsabilidades;
- Metodologia – Políticas e estratégias;
- Controles – Processos, procedimentos e ferramentas.

Hoje em dia, as informações são vistas como commodities, sem as quais muitas organizações não funcionam. Contudo, no mundo interligado em que vivemos, a informação é muito mais vulnerável do que outra mercadoria.

Embora seja altamente improvável que as ações de um adolescente descontente em outro continente afetem uma empresa de fornecimento de eletricidade, é fácil prever que as ações deste jovem podem parar o sistema de informação de organizações de prestígio [11].

Atualmente, a norma ISO/IEC 27000 é uma das mais utilizadas práticas corporativas de padrões de segurança de TI, abordando os requisitos de gestão e identificando áreas específicas de controle para segurança da informação [4].

Seu processo se adapta às necessidades de segurança de qualquer tipo de organização e seus padrões descrevem cenários de uso do SGSI (Sistema de Gerenciamento da Segurança da Informação).

Mesmo sendo referência de segurança (a norma já passou das 19 mil certificações registradas), em muitos países existe uma dificuldade de implantá-la. Possíveis razões para essa dificuldade são a falta de competências e a indisponibilidade de recursos por parte das empresas.

Uma questão que tem sido amplamente ignorada é que as normas internacionais são derivadas da experiência coletiva e conhecimento dos especialistas internacionais em vários comitês de normalização [1].

Para Beckers [5], a norma não está bem clara para as empresas que o implantam e até propõe uma análise das implantações para entender o motivo. Já Breier [7] afirma que é necessário tornar mais legível a norma e até propõe uma hierarquia dos processos da ISO.

Na maioria das empresas que implantaram a ISO/IEC 27000 o modelo fica limitado à sala de informática e ao departamento de gestãodasinformações. Comoas informações existem em todos os departamentos da empresa, a norma pode ter deficiência de proteção destas informações [9].

Para muitas organizações alcançar uma certificação é necessário para a continuidade dos negócios e a garantia da boa reputação. Especialistas apontam que as escolhas das normas de segurança devem ser orientadas pelas necessidades da organização [8].

Sendo assim, avaliar a SI nas empresas é uma atividade da gestão estratégica [2], ou seja, "é necessário que líderes e gestores entendam suas responsabilidades e apoiem a gestão de segurança da informação para melhorar a proteção dos ativos da organização" [7].

A.O Modelo ITMark

O ITMark é um modelo de qualidade criado pelo ESI (European Software Institute) para atender as MPEs. O modelo combina vários modelos de melhoria simplificados em um único regime. Sua avaliação permite que as empresas [12]:

- Avaliem os processos técnicos e de gestão através de modelos e normas reconhecidos na indústria de TI;
- Iniciem uma iniciativa de melhoria;
- Obtenham reconhecimento e visibilidade de compromisso com a qualidade.

O modelo do ITMark avalia as empresas sob a ótica de três processos:

- Gestão de Negócios: avaliado com base no Ten Squared (102), EFQM e ISO/IEC 9001;
- Gestão de desenvolvimento de software: avaliado com base no CMMI-DEV nos níveis de maturidade 2 e 3;
- Gestão de segurança da informação avaliado com base nas normas ISO/IEC 27002:2005 (Práticas para a gestão da segurança da informação) e ISO/IEC 27001:2005 (Gestão de Sistemas de Informação de Segurança – Requisitos).

Para garantir que o modelo seja avaliado nas empresas independente do seu tamanho e da sua maturidade, os resultados esperados pelo ITMark foram agrupados em três níveis:

- Nível Basic: verifica se a empresa está consciente dos temas relacionados com a gestão técnica, de segurança e de negócios e tem criado ações para controlá-los.
- Nível Premium: verifica se a empresa já atingiu um bom nível de capacidade destes processos de acordo com modelos reconhecidos mundialmente.
- Nível Elite: verifica se a empresa chegou a um alto nível de definição e institucionalização dos processos de negócios, segurança e desenvolvimento de software, assim como a qualidade de seus produtos é boa por causa do seu processo de melhoria contínua.

A avaliação do ITMark, feita com a presença de um consultor credenciado do ESI é composta de entrevistas, análise de documentos e artefatos relacionados às três áreas avaliadas e observação do espaço físico da empresa.

Os resultados avaliados na empresa são compilados através de uma metodologia de avaliação que utiliza a norma ISO/IEC 15504 como base e também um conjunto de critérios que estão apresentados na Tabela 1.

TABELA 1 CRITÉRIOS DE NÍVEIS DE MATURIDADE

Nível	Negócio	Segurança	Desenvolvimento
Elite	75% atingido	Nível 3	Nenhum processo não implementado e mais de 10 largamente ou totalmente implementados
Premium	60% atingido	Nível 2	Nenhum processo não implementado e mais de 2 largamente ou totalmente implementados
Basic	50% atingido	Nível 1	Até 2 processos não implementados, exceto os processos de Gestão de Projetos (PP, PMC)

Para Segurança, o nível 1 verifica se a empresa faz ações básicas para garantir a SI. No nível 2, o objetivo verificar se os processos documentados para o tratamento da SI. Por fim, no nível 3, o objetivo é verificar o grau de institucionalização dos processos de SI na empresa.

A avaliação da área de Desenvolvimento considera que um processo está Totalmente Implementado quando atende os resultados especificados pelo modelo sem pontos fracos e Largamente Implementado quando atende os resultados especificados, porém com pontos fracos (requer melhorias).

B.Avaliação de Segurança da Informação

Avaliação de SI não é tarefa fácil, pois exige conhecimento em diferentes áreas como comunicação, segurança lógica, segurança física, leis, organização e análise de risco. A avaliação do ITMark verifica todas essas áreas, através de perguntas, obtendo assim, um panorama da SI na empresa.

Seguindo o padrão de nivelamento por maturidade do ITMark, a SI da empresa é avaliada através de perguntas sobre segurança cujas respostas devem ser 'Sim' ou 'Não'. A Tabela 2 mostra os requisitos desta avaliação:

TABELA 2 REQUISITOS DETALHADOS DA AVALIAÇÃO DA SEGURANÇA

Nível	Questões	% Respostas 'SIM'	Questões Obrigatórias
1	28	66%	7
2	16	80% (nível 1)	7 (nível 1) + 4 (nível 2)
3	17	70% (nível 2)	7 (nível 1) + 4 (nível 2)

A quantidade de respostas iguais a 'Sim' exigidas para cada nível é mostrada na terceira coluna da tabela enquanto que a quarta coluna mostra quantas questões obrigatoriamente a resposta de ser igual a 'Sim' no nível exigido.

A avaliação de nível 1 verifica se a empresa tem feito ações para garantir a segurança das informações. Na avaliação de nível 2 o objetivo verificar se a empresa possui processos documentados para o tratamento da segurança das informações.

Por fim, na avaliação de nível 3, o objetivo é verificar o grau de institucionalização dos processos de segurança das informações na empresa. Avalia-se também o quanto a empresa está preocupada com a melhoria destes processos.

As perguntas são acumulativas nos níveis, ou seja, na avaliação nível 2 devem ser aplicadas as perguntas dos níveis 1 e 2 enquanto que no nível 3 todas as perguntas devem ser aplicadas considerando as regras de Questões Obrigatórias (o nível 3 não possui Questões Obrigatórias).

III.3 APLICAÇÃO DO ITMARK

A análise apresentada neste artigo refere-se a quatro empresas brasileiras avaliadas no modelo ITMark nível Basic. São MPEs, localizadas na região de Londrina e desenvolvedoras de software para automação comercial, metrologia, segurança de ambientes e telecomunicações.

As empresas fazem parte de um APL (Arranjo Produtivo Local) e estão envolvidas com projetos de qualidade e melhoria de software por mais de 5 anos. Todas possuem as certificações MR-MPS-SW nível F e MoProSoft nível 2.

A avaliação das empresas foi feita presencialmente, por um consultor da Colômbia representante do ESI Center. O consultor não conhecia as empresas e antes da avaliação foi feito somente um treinamento para apresentar o modelo. A Tabela 3 mostra o roteiro das avaliações:

TABELA 3 ROTEIRO DA AVALIAÇÃO ITMARK – NÍVEL BASIC

Etapa	Duração	Participantes
Seminário ITMark Overview	4 horas	4 pessoas por empresa: responsável pela Qualidade e um representante de cada uma das áreas avaliadas.
Avaliação da gestão empresarial	4 horas	Responsável pela Qualidade, presidente ou representante legal da empresa e sua equipe de gestão (gerentes, diretores e coordenadores de área).
Avaliação da segurança da informação	4 horas	Garantia da Qualidade e o Responsável pela Segurança da Informação (Infraestrutura ou Suporte)
Avaliação de processos técnicos	6 horas	Responsável pela Qualidade, Gestor de projetos e o responsável pela área que está sendo avaliada.
Consolidação	1 hora	Avaliador
Apresentação dos resultados finais	1 hora	Todos que a empresa desejar.

A Tabela 3 mostra a sequência das atividades da avaliação. No treinamento o consultor do ESI apresentou o modelo e a metodologia para a avaliação. Na sequência o consultor visitou a sede de cada uma das empresas onde foram avaliados os processos e apresentado o resultado da avaliação.

A metodologia da avaliação das três áreas consiste na verificação dos documentos organizacionais e de projetos além da entrevista com as pessoas que executam os processos documentados e também a observação da execução das atividades.

Nas avaliações dos processos de Gestão de Negócios e Desenvolvimento de Software as empresas não tiveram dificuldades, pois já possuíam certificações destes processos. A Figura 1 e a Figura 2 mostram resultados destas avaliações:

NEGÓCIO		
Categoria	Realização actual vs ideal	Realização Objectivo vs ideal
MERCADO	76.62 %	79.22 %
GESTÃO	44.26 %	68.07 %
PRODUTOS E SERVIÇOS	42.31 %	68.68 %
MARKETING, VENDAS E DISTRIBUIÇÃO	13.49 %	65.87 %
PLANO ESTRATÉGICO E BOARD	90.48 %	74.15 %
ANÁLISE FINANCEIRA	78.06 %	50.51 %
PERFIL DO CLIENTE E ANÁLISE	71.62 %	85.43 %
FACTORES DE INVESTIMENTO	39.56 %	43.96 %
DESENVOLVIMENTO E PRODUÇÃO	67.23 %	66.39 %
RECURSOS HUMANOS E SOCIEDADE	60.08 %	68.91 %
Realização total vs ideal	58.92 %	66.61 %

❑ A organização atingiu os requisitos mínimos para ter conformidade com os critérios estabelecidos em ITMark (>50% do ideal).

Figura 1: Exemplo de Apresentação do Resultado da Avaliação de Negócios

De acordo com a Figura 1, os itens avaliados na Gestão de Negócios foram definidos com base nos nove critérios de qualidade do modelo EFQM (European Foundation for Quality Management). O percentual apresentado na avaliação equivale à aderência da empresa aos itens verificados em cada critério.

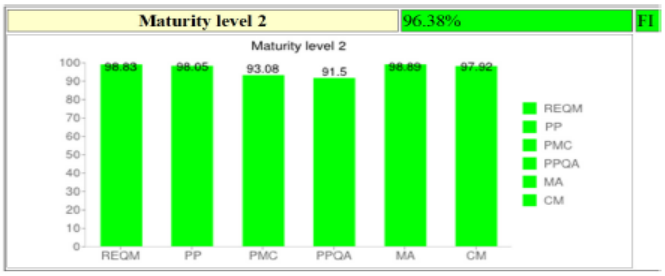

Figura 2: Exemplo de Apresentação do Resultado da Avaliação de Desenvolvimento

Conforme mostra a Figura 2, a empresa possui os processos equivalentes ao CMMI nível 2 implantados na área de Desenvolvimento onde os processos de Requisitos (REQM), Gestão de Projetos (PP e PMC), Qualidade (PPQA), Medições (MA) e Configuração (CM) têm aderência superior a 90%

Na avaliação de SI, participaram os responsáveis pela Qualidade pela Segurança da Informação nas empresas. O avaliador fez as 28 perguntas de segurança do nível Basic. Dessas questões, 19 teriam que ser respondidas com 'Sim' para que a empresa fosse aprovada. A Tabela 4 mostra as questões:

TABELA 4 REQUISITOS DETALHADOS DA AVALIAÇÃO DA SEGURANÇA

Questão	Pergunta
A1	**Existe um inventário básico de ativos (hardware e software)?**
A2	Cada ativo tem seu proprietário identificado?
A3	Há uma política de classificação da informação?
A4	Existem procedimentos de classificação da informação?
A5	Existem papéis e responsabilidades definidas para a gestão da segurança?
A6	Os responsáveis de segurança receberam treinamento especializado?
A7	Existe um perímetro físico de segurança definido?
A8	Existem equipamentos para alimentação ininterrupta?
A9	Existem mecanismos para a eliminação segura da informação?
A10	**Cada usuário tem um identificador exclusivo?**
A11	São definidas permissões em função dos papéis e responsabilidades?
A13	**Os equipamentos dos usuários são atualizados periodicamente?**
A14	**Os servidores são atualizados periodicamente?**
A15	**Existem mecanismos de proteção contra malwares?**
A16	Existem procedimentos de backup e recuperação de dados?
A17	**Um plano de backups é definido e executado?**
A18	As cópias de segurança são etiquetadas e armazenadas em lugares seguros (fora da organização se for necessário)?
A19	Os backups são testados periodicamente para verificar sua correta geração e recuperação?
A20	**Controles da rede são configurados e implementados?**
A21	Foi identificado na empresa um responsável pela gestão da segurança?
A22	Os funcionários assinam acordos de confidencialidade?
A23	São assinados acordos de confidencialidade com clientes e fornecedores?
A24	A empresa conhece a legislação que se aplica na sua região e nas regiões das empresas parceiras, clientes, fornecedores, etc?
A25	A empresa verifica os direitos de propriedade intelectual (uso de cópias ilegais, etc.)?
A26	A organização cumpre com os requisitos da LOPD (Lei de Proteção de Dados Pessoais)?
A27	A organização cumpre os requisitos da LSSICE (Lei de Serviços da Sociedade da Informação e Comércio Eletrônico)?
A28	Controles de segurança dos sistemas de informação são verificados periodicamente na empresa para garantir o cumprimento das normas vigentes?

As questões destacadas em negrito na Tabela 4 são as perguntas obrigatórias (também chamadas de 'killers questions'). Para obter a certificação Nível Basic, nenhuma destas questões deve ser respondida com 'Não'.

O avaliador também percorreu as dependências das empresas, passando por recepção, setores do desenvolvimento e perímetro dos servidores. Analisou a forma como é feito o backup e o treinamento dos responsáveis pela segurança.

Em uma das empresas, foi constatado que mudariam de endereço nos próximos dias. Sendo assim, o consultor solicitou uma visita na nova sede da empresa para validar as questões de segurança relacionadas com local físico.

Ao final da avaliação, o avaliador utilizou um software pata compilar as informações coletadas e gerar os resultados da avaliação da empresa que foram apresentados conforme o exemplo da Figura 3:

Figura 3: Exemplo de Apresentação do Resultado Final da Avaliação

Antes de mostrar os números apresentados na Figura 3, o avaliador apresentou as inconsistências encontradas na empresa e as oportunidades de melhoria nas empresas, principalmente na área de segurança, uma vez que esta nunca tinha sido avaliada nas empresas.

IV.RESULTADOS E DISCUSSÕES

De uma forma geral, as empresas foram bem avaliadas e apresentaram poucos problemas e sugestões de melhorias na SI. Os resultados das avaliações de segurança das quatro empresas são apresentados na Tabela 5:

TABELA 5 RESULTADO DAS AVALIAÇÕES NAS EMPRESAS

	Total das Respostas			
Empresa	Sim	Não	Não Avaliado	Grau de Aderência
Empresa 1	25	1	2	96%
Empresa 2	20	5	3	80%
Empresa 3	22	4	2	84%
Empresa 4	20	6	2	77%

Mesmo não tendo ocorridos trabalhos nas empresas para prepará-las para a avaliação, as empresas atingiram resultados satisfatórios para o nível Basic do ITMark, embora somente uma delas atingiu mais de 90% de aderência.

A avaliação expôs problemas que as empresas possuíam mesmo tendo certificações de qualidade na área de desenvolvimento, mostrando que tais modelos não tem a preocupação direta com SI.

Ficou evidente que os responsáveis pela segurança das informações nas empresas devem ser identificados e receber formação/treinamento sobre os aspectos de segurança da infor-

mação necessários para desempenhar as suas funções como.

Na ausência de um papel específico para segurança, a responsabilidade cabe ao técnico de infra-estrutura da empresa, o que não é suficiente pois a responsabilidade da segurança das informações recai sobre os usuários.

Problemas com geração e armazenamento de backup e até mesmo a eliminação segura da informação foram identificados durante as avaliações onde ficou constatada que somente uma das empresas tem real preocupação com estes processos.

A empresa que melhor efetua o backup possui um sistema que gera backups dos servidores e dos terminais com agendamento, criptografia e armazenamento em nuvem sem a intervenção humana.

Outro ponto que deve ser levado em conta é o perímetro dos servidores. As empresas não estão preocupadas com a segurança física e o acesso restrito de seus servidores e precisam tornar esse ambiente mais protegido com barreiras de segurança e controles de entrada apropriados.

Os demais problemas encontrados e suas recomendações de melhoria são:

- Inventário desatualizado. Em algumas empresas, não foi identificado nenhum documento dos ativos de hardware e software e seu controle de entrada e saída na empresa.
- Política de segurança ineficaz ou inexistente. Nenhuma das empresas possuía uma política de segurança clara e que contempla todos os itens considerado importantes pelo modelo ITMark.
- Os colaboradores não possuem um acordo formal sobre o comportamento permitido na rede. Com exceção de uma empresa, as demais não possuíam documentos que evidenciam o comprometimento das pessoas com a segurança das informações.

V. CONCLUSÃO

As MPEs, que estão em destaque no mercado de software atual, possuem limitação de recursos e estão mais expostas a invasões e perda de informações, são, na verdade uma grande fonte de oportunidades de desenvolvimento de projetos ligados à área de Segurança da Informação no Brasil.

Além das oportunidades de melhoria identificadas nas avaliações, é importante destacar que as empresas precisam documentar os processos e procedimentos relacionados à segurança bem como as regras e controles para as pessoas que trabalham na organização.

Uma análise nos resultados apresentados nas avaliações permite recomendar a criação de um modelo de implantação dos resultados exigidos pelos processos de segurança do ITMark.

O pré-requisito para a implantação seriam as empresas que já possuem certificações nos modelos de qualidade existentes, uma vez que tornaria mais fácil a aderência aos demais processos do ITMark.

A avaliação de segurança do modelo ITMark não só consolida o trabalho que as empresas fazem para produzir com qualidade como também gera oportunidades para melhoria da segurança no trabalho das informações da empresa e de seus clientes e funcionários.

Com base nos resultados atingidos, é possível afirmar que a avaliação de SI, considerando seu nivelamento é uma proposta viável para as empresas uma vez que a implantação da norma ISO/IEC 27000 não leva em conta a maturidade das empresas e não possui nivelamento.

A avaliação foi feita em apenas cinco empresas brasileiras, o que não valida totalmente sua viabilidade. Assim, novas avaliações precisam ser realizadas no Brasil em diferentes organizações. Também é necessário preparar e capacitar consultores brasileiros para diminuir os custos da avaliação.

REFERÊNCIAS

[1] K. I. Alshitri e A. N. Abanumy, “Exploring the Reasons behind the Low ISO 27001 Adoption in Public Organizations in Saudi Arabia” in Proc. ICISA, 2014, pp. 1–4.

[2] K. I. Anttila *et al.*, “Integrating ISO/IEC 27001 and other Managerial Discipline Standards with Processes of Management in Organizations” in Proc. ARES, 2012, pp. 425–436.

[3] A. Asosheh e P. Hajinazari and H. Khodkari, “A practical implementation of ISMS” in Proc. ECDC, 2013, pp. 1–17.

[4] M. P. Azuma *et al.*, “A propose technical security metrics model for SCADA systems” in Proc. CyberSec, 2012, pp. 70–75.

[5] K. Beckers *et al.*, “Using Security Requirements Engineering Approaches to Support ISO 27001 Information Security Management Systems Development and Documentation” in Proc. ARES, 2012, pp. 242–248.

[6] K. Bechers *et al.*, “Structured Pattern-Based Security Requirements Elicitation for Clouds” in Proc. ARES, 2013, pp. 465–474.

[7] J. Breier e L. Hudec, “New approach in information system security evaluation” in Proc. ESTEL, 2012, pp. 1–6.

[8] T. Caldwell, “Setting the gold standard”, Computer Fraud & Security Elsevier, vol. 2013, no. 12, pp. 15–19, Dez. 2013.

[9] S. Chang *et al.*, “Risk Assessment Mechanism for Personal Information Operations - Case Study by Hospital” in Proc. CSE, 2013, pp. 786–793.

[10] G. Disterer, “ISO/IEC 27000, 27001 and 27002 for Information Security Management”, Journal of Information Security, vol. 4, no. 2, pp. 92–100, Abr. 2013.

[11] H. Elanchar e B. Regragui, “Information Security, new approach” in Proc. INTECH, 2012, pp. 51–56.

[12] ITMark, “ITMARK”, 2014. Disponível em: www.it-mark.eu. Acesso em: 15 fev. 2015.

[13] S. Mubashir Ali e T. R. Soomro, “Integration of Information Security Essential Controls into Information Technology Infrastructure Library – A Proposed Framework”, International Journal of Applied Science and Technology, vol. 4, no. 1, pp. 95–100, Jan. 2014.

[14] S. Nazir *et al.*, “Evaluating Security of Software Components Using Analytic Network Process”, in Proc. FIT, 2013, pp. 183–188.

[15] C. Pardo *et al.*, “An ontology for the harmonization of multiple standards and models”, Computer Standards & Interfaces Elsevier, vol. 34, no. 1, pp. 48–59, Jan. 2013.

[16] E. A. Rigon e C. M. Westphall, “Modelo de Avaliação da Maturidade da Segurança da Informação”, in Proc. SBSI, 2013, pp. 93–104.

[17] S. Ristov *et al.*, “A New Methodology for Security Evaluation in Cloud Computing”, in Proc. MIPRO, 2012, pp. 1484–1489.

[18] SOFTEX, “Comunicado Softex 22/2012”, 2012. Disponível em: www.softex.br/comunicado-softex-222012. Acesso em: 15 fev. 2015.

[19] SOFTEX, “MPS.BR em números”. 2015. Disponível em: www.softex.br/mpsbr/mps/mps-br-em-numeros. Acesso em: 15 fev. 2015.

[20] M. A. Talib *et al.*, “Using ISO 27001 in teaching information security”, in Proc. IECON, 2012, pp. 3149–3153.

[21] R. I. Tecnalia, “ITmark: Stand OUT from the crowd”, 2012. Disponível em: www.tecnalia.com.es/en/health/case-studies/it-mark.htm. Acesso em: 15 fev. 2015