Maturity Model of Information Security for Software Developers

M. P. Silva e R. M. Barros

***Abstract*— Currently the software developers have to worry about protecting your information and customer information which it has access. ISO 27001 is currently the largest reference in security procedures Information (SI). This paper presents an information security maturity model based on ISO 27001 for software developers. The model was evaluated by experts in the subject and used to assess the level of maturity of some Brazilian companies. The results of the evaluations showed that the model is a tool that can be used for companies to deploy SI processes.**

***Keywords*— Information Security, Maturity Model, ISO 27001.**

I. INTRODUÇÃO

PROTEGER a informação é uma preocupação para muitas organizações atualmente. Com a dependência cada vez mais do uso da tecnologia, as empresas ficam expostas a um número crescente de ameaças e vulnerabilidades.

Para as empresas que desenvolvem software o desafio é ainda maior pois o conhecimento que produzem é diferencial para sua competitividade. Além disso, o acesso à dados sigilosos de seus clientes, na maioria das vezes, é condicionado à contratos, leis e acordos.

Atualmente no Brasil há um grande movimento por parte destas empresas para melhorarem seus processos de desenvolvimento. Segundo dados disponibilizados na página do SOFTEX[20], já foram realizadas mais de 600 avaliações de empresas de software junto ao modelo MPS.Br.

Isto gerou um crescimento da maturidade no desenvolvimento de software. Atingida essa maturidade, as empresas deste segmento estão buscando modelos de qualidade para outros processos internos como Gestão Estratégica e SI.

Com base no que foi descrito, este artigo apresenta um Modelo de Maturidade de Segurança da Informação baseado na norma ISO 27001. O objetivo deste modelo é auxiliar as empresas de software a avaliarem sua situação com relação à SI.

A Seção 2 apresenta uma fundamentação teórica do trabalho e a caracterização do problema. Na Seção 3 é apresentado o modelo de maturidade e a forma como ele foi avaliado. Os resultados obtidos após a avaliação do modelo junto às empresas está na Seção 4. As conclusões e os trabalhos futuros estão na Seção 7.

M. P. da Silva, Instituto SENAI de Tecnologia (IST), Londrina, Paraná, Brasil, marcelo.pereira@pr.senai.br

R. M. de Barros, Universidade Estadual de Londrina (UEL), Londrina, Paraná, Brasil, rodolfo@uel.br

II. FUNDAMENTAÇÃO TEÓRICA

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 de informações e sistemas que processam é fundamental para o funcionamento de todas as organizações.

Por isso as organizações devem compreender e melhorar o estado atual da sua SI, a fim de garantir a continuidade dos negócios e taxa de retorno sobre os investimentos aumentam[3].

A segurança da informação se caracteriza pela preservação de sua:

- 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 da informação não tem que ser considerada só como uma solução técnica. Deve ser considerado como um sistema integrado que interage com outros sistemas existentes dentro da organização tais como[10]:

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

Hoje em dia, a informação pode ser vista como uma commodities (como a eletricidade), sem a qual muitas empresas e 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 eletricidade, é fácil prever que as ações deste jovem podem parar o sistema de informação de organizações de prestígio[11].

A. Norma ISO 27001

A ISO 27001 é a norma que contém as melhores práticas corporativas de padrões de segurança de TI, abordando os requisitos de gestão, bem como identificando áreas específicas de controle para segurança da informação[4].

A norma estabelece um processo, o qual adapta às necessidades de segurança de qualquer tipo de organização.

Os padrões da ISO 27001 descrevem partes, ou cenários de uso do SGSI (Sistema de Gerenciamento da Segurança da Informação)[5].

A estrutura está estruturada em 11 seções e um anexo. As 4 (quatro) primeiras são introdutórias (um padrão das normas ISO). As outras 7 (sete) definem os procedimentos e registros para o atendimento da norma. O Anexo A é um conjunto de 114 artefatos que podem ser utilizados no SGSI.

A ISO 27001 é recomentada pelos principais frameworks de Governança como mostram a Fig. 1 e a Fig. 2:

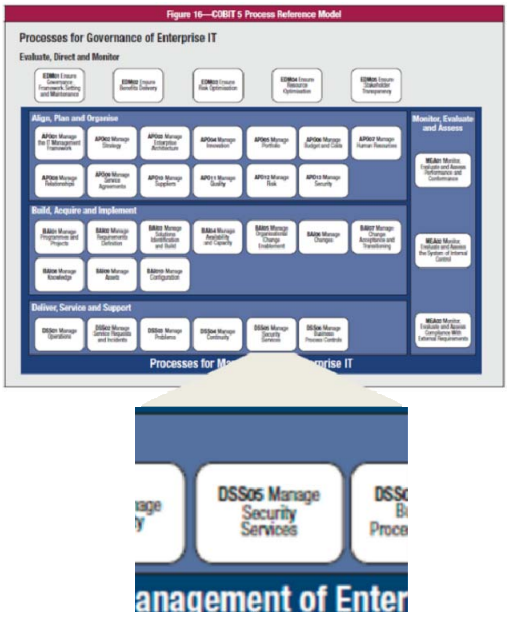


Figura 1. Serviços de Gestão de Segurança do COBIT

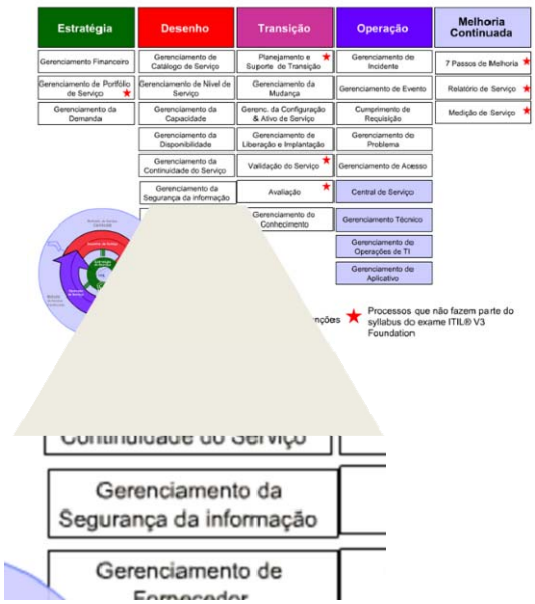


Figura 2. Gerenciamento da Segurança da Informação do ITIL

Conforme apresentado nas figuras, tanto o COBIT quanto o ITIL sugerem o tratamento da segurança da informação. Para tal, sugerem a norma ISO 27001 como opção[13].

A norma foi criada em 2005 e a busca por sua certificação vem crescendo como mostra o gráfico na Fig. 3:

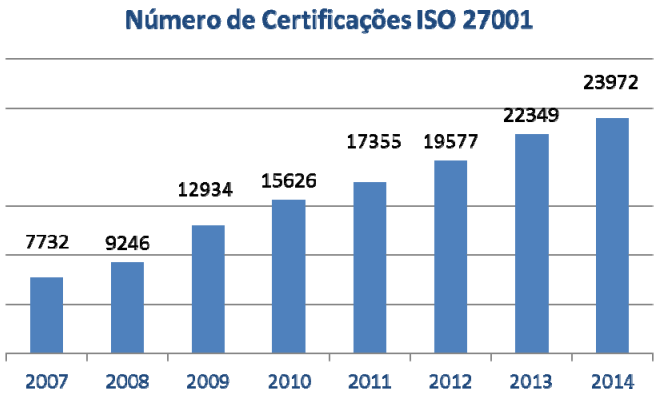


Figura 3. Número de certificações até 2014[23]

Mesmo sendo referência de segurança, em muitos países existe uma dificuldade de implantar a norma. Um exemplo é a Arábia Saudita onde apenas 46 organizações possuem essa certificação[1]. Possíveis razões para essa dificuldade são a falta de conhecimento por parte das empresas.

Outra 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.

Para Beckers, a ISO 27001 não está bem clara para as empresas que o implantam e até propõe uma análise das implantações para entender o motivo[6]. Já Breier afirma que é necessário tornar mais legível a norma e até propõe uma hierarquia dos processos da ISO[7].

Infelizmente para a maior parte das empresas que implantaram a ISO 27001 o modelo fica limitado à sala de informática e ao departamento de gerenciamento de informações. Como as informações existem todas as áreas da empresa podem existir falhar nesta proteção[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].

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].

No Brasil, segundo dados do SEBRAE existem mais de 9000 empresas desenvolvedoras de software e 94% destas empresas são de micro e pequeno porte (MPEs). Neste contexto, um dos problemas a serem tratados é: “Como implementar a ISO 27001 em empresas de pequeno porte?”.

III. *MODELO DE MATURIDADE PARA SI*

Uma sugestão para responder a questão da Seção anterior foi criado um modelo de maturidade de SI baseado nos procedimentos da ISO 27001. Esses procedimentos são classificados em níveis de maturidade para que as pequenas empresas implantem um SGSI de forma gradativa.

A elaboração deste modelo seguiu o fluxo de trabalho mostrado na Fig. 4:

Figura 4. Fluxo para Criação do Modelo de Maturidade.

Cada uma das fases mostrada na Fig. 4 está detalhada nas subseções seguintes.

A. *Análise da ISO 27001*

A análise foi feita na ISO/IEC 27001:2013[22] e em suas duas notas de correção (ISO/IEC 27001:2013/Cor1:2014 e ISO/IEC 27001:2013/Cor 2:2015). Foram analisadas seções 4 a 11 (obrigatórias) e todos os artefatos do Anexo A.

O conteúdo da norma foi classificado nas seguintes abordagens:

- Infraestrutura – Hardware e Software necessários para SI;
- Pessoas – Papéis e responsabilidades necessários para SI;
- Riscos – Gestão de Riscos ligados à SI;
- Processos – Políticas e procedimentos para nortear a gestão da SI;
- Tratamento da Informações – métodos e controles adotados para o tratamento das informações na empresa.

B. *Definição dos Níveis de Maturidade*

Para definir o nível de maturidade foi utilizado o nivelamento sugerido pela ISO 15504 (atualmente ISO 33000[23]). Os níveis definidos para este modelo são apresentados na Fig. 5:

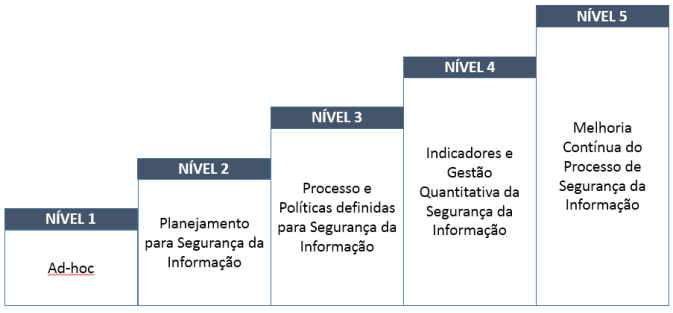


Figura 5. Níveis de Maturidade de Segurança da Informação

No nível 1 a empresa realiza ações informais para garantir SI. Já no nível 2, as ações para garantir segurança são planejadas. A partir do nível 3, são definidos processos para a realização das atividades. Esses processos passam a ser gerenciados através de indicadores no nível 4. Por fim, a empresa se encontra no nível 5 quanto possui ações que buscar melhorar continuamente as atividades voltadas para a SI.

C. *Definição dos Itens de cada Nível*

Nesta etapa a norma foi decomposta em 35 resultados esperados. A Tabela I mostra a lista destes resultados:

TABELA I
RESULTADOS ESPERADOS DO MODELO

1 – Inventário de Ativos
2 – Uso de Ativos
3 – Atualização de Equipamentos de Usuários
4 – Prevenção contra Sobrecarga no Sistema
5 – Controle de Acesso das Pessoas
6 – Tratamento da Interrupção de Energia Elétrica
7 – Gestão da Rede de Computadores
8 – Atualização dos Servidores
9 – Utilização de Firewall
10 – Proteção Contra Programas Maliciosos
11 – Controle do Acesso Remoto da Rede da Empresa
12 – Gestão dos Usuários da Rede
13 – Responsabilidades por Segurança da Informação na Empresa
14 – Treinamentos sobre Segurança da Informação na Empresa
15 – Gestão dos Riscos Relacionados à Segurança das Informações
16 – Tratamento das Ameaças e Vulnerabilidades
17 – Gestão dos Incidentes de Segurança da Informação
18 – Classificação das Informações Empresa
19 – Controle das Informações com Acesso Restrito
20 – Backup das Informações da Empresa
21 – Tratamento das Senhas da Empresa
22 – Segurança da Informação no Desenvolvimento dos Produtos
23 – Política de Segurança da Informação
24 – Existência de SGSI
25 – Gestão dos Controles do SGSI
26 – Armazenamento dos Backups
27 – Eliminação Segura da Informação
28 – Mecanismos para Criptografia da Informação
29 – Direitos de Propriedade Intelectual
30 – Conhecimento da Legislação sobre Segurança da Informação
31 – Confidencialidade entre Clientes e entre Fornecedores
32 – Confidencialidade dos Funcionários
33 – Avaliação de Segurança Durante as Mudanças
34 – Gestão de Ambientes de Desenvolvimento, Teste e Produção
35 – Segurança na Gestão de Configuração

Cada resultado esperado que aparece na Tabela I foi classificado conforme as abordagens definidas na etapa de análise da ISO 27001. A forma como o resultado esperado está implementado determina seu nível de maturidade conforme a Fig. 5.

D. *Questionário para a Avaliação*

O questionário criado para avaliar o nível de maturidade das empresas é composto de 35 questões, uma para cada um dos resultados esperados. Para cada questão, foram criadas 5 respostas, uma para cada nível de maturidade.

A soma dos pontos determina o nível de maturidade. Para definir a pontuação de cada nível foi utilizado como referência o modelo de avaliação de processo do MPS.Br (85% de aderência ao nível) conforme apresentado na Tabela II:

TABELA II
PONTUAÇÃO DOS NÍVEIS

Nível de Maturidade	**Pontuação**
1 – Ad Hoc	Menos de 60 pontos
2 – Gerenciado	Entre 60 e 88 pontos
3 – Definido	Entre 89 e 118 pontos
4 – Gerenciado Quantitativamente	Entre 119 e 147 pontos
5 – Otimizado	Mais de 147 pontos

E. Avaliação por Especialistas

O modelo foi apresentado para 5 (cinco) profissionais com experiência em SI para que avaliassem sua estrutura e indicassem melhorias e ajustes. A Tabela III mostra o perfil destes profissionais, cujos nomes não serão identificados:

TABELA III
PERFIL DOS ESPECIALISTAS

Especialista	Perfil
Especialista 1	Analista Responsável pela Segurança de Dados de uma Federação de Indústrias
Especialista 2	Consultor de TI, especialista em Segurança e Gestão de Incidentes
Especialista 3	Doutor e professor em Segurança de Redes
Especialista 4	Mestre e Consultor de Governança de TIC
Especialista 5	Doutorando e Consultor de Governança de TIC

Estes especialistas avaliaram o modelo proposto pelos itens abaixo:

- Elaboração das questões baseada na ISO 27001;
- Nivelamento do modelo com 5 níveis;
- Pontuação das respostas;
- Método de compilação dos pontos usando BI;
- Apresentação dos resultados (gráficos).

Cada item foi respondido utilizando a Escala de Likert, estabelecida abaixo:

1. Discordo totalmente
2. Discordo parcialmente
3. Indiferente
4. Concordo parcialmente
5. Concordo totalmente

O grau de rigorosidade definido para esta avaliação foi 4 pontos no mínimo. Os resultados desta avaliação aparecem na Tabela IV:

TABELA IV
AVALIAÇÃO DOS ESPECIALISTAS

Questão	Especialista	Avaliação
Questões para a avaliação baseada na ISO 27001	Especialista 1	5,0
	Especialista 2	5,0
	Especialista 3	3,0
	Especialista 4	2,0
	Especialista 5	3,0
Nivelamento do modelo com 5 níveis	Especialista 1	4,0
	Especialista 2	4,0
	Especialista 3	5,0
	Especialista 4	5,0
	Especialista 5	5,0
Pontuação das respostas	Especialista 1	4,0
	Especialista 2	5,0
	Especialista 3	4,0
	Especialista 4	4,0
	Especialista 5	4,0
Método de compilação dos pontos (usando BI)	Especialista 1	5,0
	Especialista 2	5,0
	Especialista 3	4,0
	Especialista 4	5,0
	Especialista 5	5,0
Apresentação dos resultados (gráficos)	Especialista 1	5,0
	Especialista 2	5,0
	Especialista 3	5,0
	Especialista 4	5,0
	Especialista 5	5,0
Média Final		**4,4**

F. Avaliação das Empresas

Foi criado um formulário eletrônico contendo as 35 questões e enviado para 50 empresas brasileiras localizadas no Estado do Paraná e 9 (nove) responderam o questionário, o que equivale a 18% das empresas consultadas.

Das empresas que responderam ao questionário, 80% existem a mais de 10 anos, 4 possuem mais de 30 funcionários e 2, menos de 10 funcionários. A maioria (60%) atuam nas áreas de Gestão de Empresas.

As respostas foram exportadas para um software de BI (Business Intelligence) para serem a analistas. A Fig. 6 mostra a avaliação de uma das empresas:

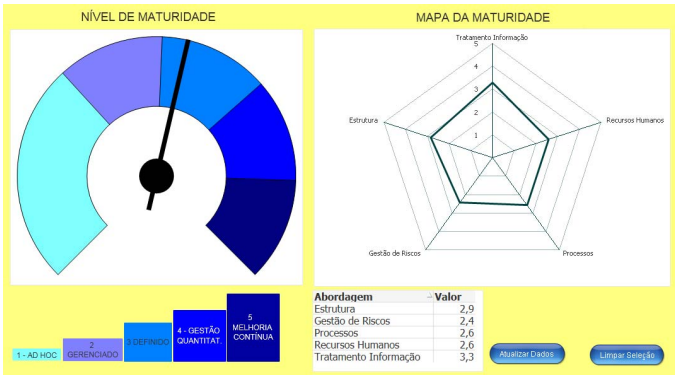


Figura 6. Resultado da Avaliação de uma das empresas pesquisadas

A grande vantagem do BI é a análise multidimensional, que permite examinar a informação sob diferentes perspectivas, identificando padrões, relacionamentos e modelos que estão ocultos entre os dados armazenados.

G. Apresentação dos Resultados

Conforme visto na Fig. 6, as respostas são pontuadas e transformadas em valores que representam a avaliação da empresa com relação à SI.

O primeiro gráfico representa o nível de maturidade da empresa, de acordo com os critérios definidos na Tabela II. A Fig. 7 mostra o nível de maturidade da empresa selecionada:

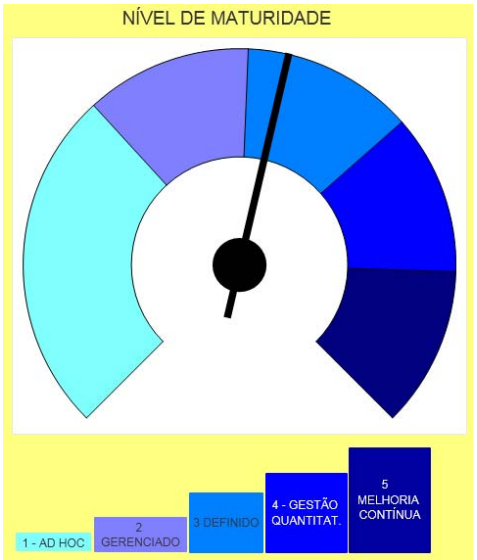
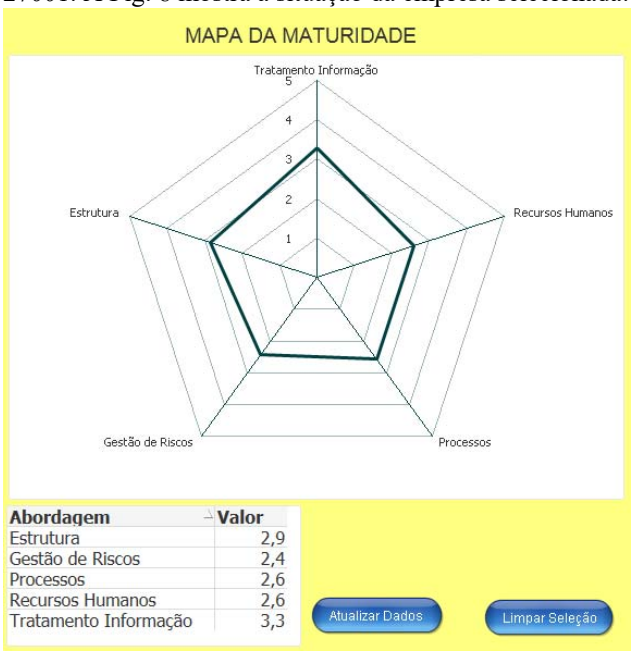


Figura 7. Nível de Maturidade

O segundo gráfico mostra a média de pontos distribuídos entre as abordagens definidas na etapa de análise da ISO 27001. A Fig. 8 mostra a situação da empresa selecionada:



Abordagem	Valor
Estrutura	2,9
Gestão de Riscos	2,4
Processos	2,6
Recursos Humanos	2,6
Tratamento Informação	3,3

Figura 8. Pontuação de Acordo com as Abordagens de SI

De acordo com a Fig. 7 e a Fig. 8, a empresa selecionada está no nível 3 do modelo de maturidade. Entretanto, há pontos de melhoria identificados no gráfico de Abordagens como Gestão de Riscos, Processos e Recursos Humanos.

IV. RESULTADOS

A avaliação do modelo junto aos especialistas atingiu o valor de rigorosidade definido como aceitável. A Fig. 9 mostra o resumo da avaliação:

Questão	Avaliação
Questões para a avaliação baseada na ISO 27001	3,6
Nivelamento do modelo com 5 níveis	4,6
Pontuação das respostas	4,2
Método de compilação dos pontos (usando BI)	4,8
Apresentação dos resultados (gráficos)	5,0
Total	**4,4**

Figura 9. Avaliação dos Especialistas

Conforme apresentado na Fig. 9, somente a elaboração das questões com base na ISO27001 não atingiu o valor de rigorosidade. Apesar disso, o valor final foi 4,4.

Alguns especialistas sugeriram melhorias no modelo. Estas melhorias estão citadas abaixo:

- Reavaliar os níveis de maturidade para abranger casos em que este não exista, ou seja, não há nem ações informais com relação ao desenvolvimento seguro das aplicações;
- Avaliar a possibilidade de tornar o modelo híbrido, baseado não só na ISO 27001, trazendo outras visões a exemplo do MPS.Br, ITMARK[12][19] e MOPROSOFT;
- Discordância com o nome Ad Hoc para o nível 1. E um termo que precisa ser explicado, e uma expressão. Poderia ser um nome em português mais intuitivo.
- Revisão na faixa inicial da pontuação pois ficou ampla.

Os resultados apresentados pelas empresas mostram que algumas tem uma preocupação maior com a segurança, enquanto outras não se planejam ou não tem estrutura para garantir a SI. A Fig. 10 mostra o nível de maturidade de cada empresa:

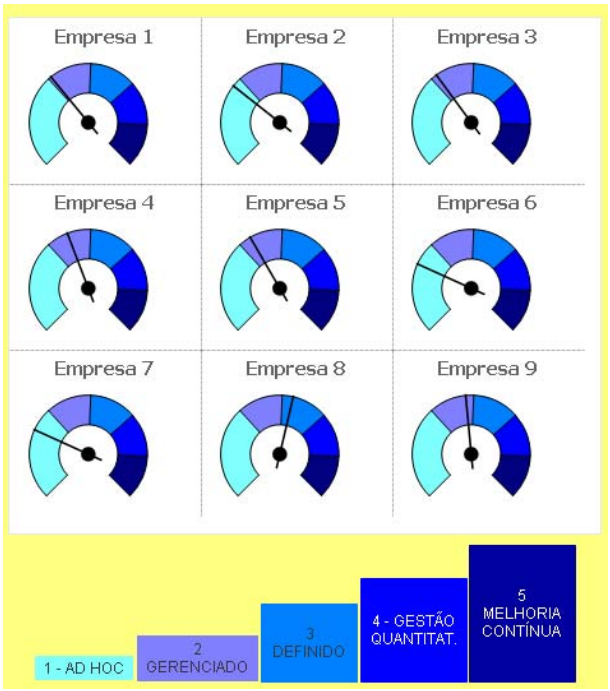


Figura 10. Gráfico de Maturidade das empresas pesquisas

Por fim, a Fig. 11 mostra o mapa de maturidade das empresas pesquisas:

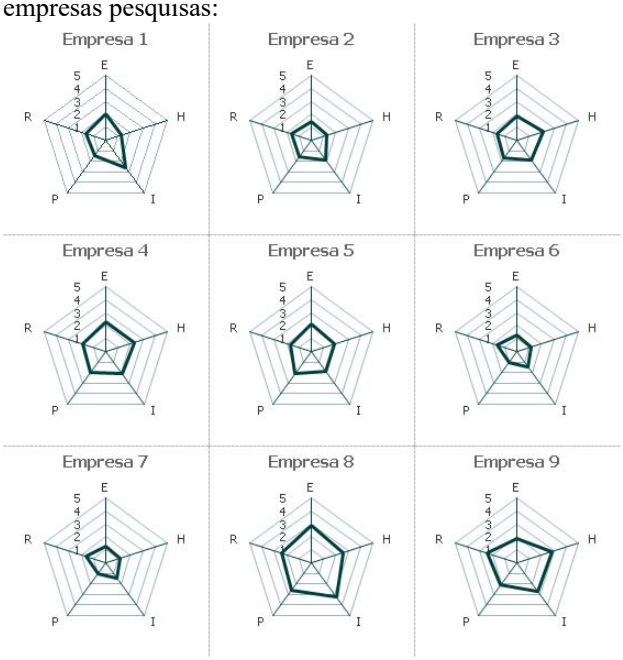


Figura 11. Mapa de Maturidade das empresas pesquisas

Conforme aparece na Fig. 11, a distribuição por Abordagens mostra as deficiências das empresas na busca pela melhoria em SI. A Empresa 1, por exemplo, apresenta

infraestrutura de nível 3 mas como as demais Abordagens são deficitárias, o nível de maturidade da empresa é 2.

V. CONCLUSÃO

As MPEs que desenvolvem software possuem limitação de recursos e estão mais expostas a invasões e perda de informações. Assim, se tornam uma grande fonte de oportunidades de desenvolvimento de projetos ligados à área de Segurança da Informação no Brasil.

O modelo de maturidade apresentado neste artigo foi avaliado por especialistas em SI e mostrou ser uma ferramenta que pode contribuir para o diagnóstico de projetos para melhorar a SI das MPEs.

Com base nos resultados da avaliação das empresas, é possível afirmar que a avaliação de SI, considerando seu nivelamento é uma proposta viável para as empresas. Isto pode mudar o paradigma das empresas que se preocupam apenas com a segurança da sua rede.

Vale lembrar que a avaliação foi feita em apenas 9 (nove) empresas brasileiras, o que não valida totalmente sua viabilidade. Sendo assim, novas avaliações precisam ser realizadas em empresas do Brasil com diferentes características.

Como futuros trabalhos, recomenda-se uma análise mais detalhada do modelo e uma avaliação de um número maior de empresas, com diferentes perfis. Também é recomendado desenvolver um software que contemple o questionário e a elaboração dos gráficos para permitir um autodiagnostico das empresas.

REFERÊNCIAS

[1] K. I. Alshitri, I. Khalid e A. N. Abanumy, "Exploring the Reasons behind the Low ISO 27001 Adoption in Public Organizations in Saudi Arabia", International Conference on Information Science & Applications - ICISA, p.1-4, 2014.

[2] J. Anttila, K. Jussila, J. Kajava e I. Kamaja, "Integrating ISO/IEC 27001 and other Managerial Discipline Standards with Processes of Management in Organizations", Seventh International Conference on Availability, Reliability and Security - ARES, p. 425-436, 2012.

[3] A. Asosheh, P. Hajinazari e H. Khodkari, "A practical implementation of ISMS", Seventh International Conference on e-Commerce in Developing Countries: with focus on e-Security - ECDC, p. 1-17, 2013.

[4] M. P. Azuwa, R. Ahmad, S. Sahib e S. Shamsuddin, "A propose technical security metrics model for SCADA systems", International Conference on Cyber Security, Cyber Warfare and Digital Forensic - CYBERSEC, p. 70-75, 2012.

[5] K. Beckers, S. Fassbender, M. Heisel e H. Schmidt, "Using Security Requirements Engineering Approaches to Support ISO 27001 Information Security Management Systems Development and Documentation", Seventh International Conference on Availability, Reliability and Security - ARES, p. 242-248, 2012.

[6] K. Beckers, M. Heisel, I. Côté, L. Goeke e S. Güler, "Structured Pattern-Based Security Requirements Elicitation for Clouds", International Conference on Availability, Reliability and Security - ARES, p. 465-474, 2013.

[7] J. Breier e L. Hudec, "New approach in information system security evaluation", First European Conference on Satellite Telecommunications - ESTEL, p. 1-6, 2012.

[8] T. Caldwell, "Setting the gold standard", Computer Fraud & Security, n. 12, p. 15-19, 2013.

[9] S. Chang, J. Su e H. Li, "Risk Assessment Mechanism for Personal Information Operations - Case Study by Hospital", 16th International Conference on Computational Science and Engineering, p. 786-793, 2013.

[10] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for Information Security Management", Journal of Information Security, vol. 4, n. 2, p. 92-100, 2013.

[11] H. Elachgar e B. Regragui, "Information Security, new approach", Second International Conference on Innovative Computing Technology - INTECH, p. 51-56, 2012.

[12] Itmark. Disponível em: <http:// http://it-mark.eu/>. Bilbao, Biscaia, Espanha. Acessado em: 16 de Junho de 2016.

[13] S. M. C. Lopes, V. G. André e J. M. S. Neves, "Governança de TI – um estudo sobre ITIL e COBIT", Simpósio de Excelência em Gestão e Tecnologia - SEGeT, 2010.

[14] 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, n. 1, p. 95-100 2014.

[15] S. Nazir, S. Shahzad, M. Nazir e H. U. Rehman, "Evaluating Security of Software Components Using Analytic Network Process", 11th International Conference on Frontiers of Information Technology - FIT, p. 183-188, 2013.

[16] C. Pardo, F. J. Pino, F. García, M. Piattini e M. T. Baldassarre, "An ontology for the harmonization of multiple standards and models", Computer Standards & Interfaces, n. 34, p. 48-59, 2012.

[17] E. A. Rigon e C. M. Westphall, "Modelo de Avaliação da Maturidade da Segurança da Informação", Revista Eletrônica de Sistemas de Informação, n. 12, p. 1-19, 2011.

[18] S. Ristov, M. Gusev e M. Kostoska, "A New Methodology for Security Evaluation in Cloud Computing", 35th International Convention on Information and Communication Technology, Electronics and Microelectronics - MIPRO, p. 1484-1489, 2012.

[19] M. P. da Silva, J. D. Brancher, "Avaliação de Segurança da Informação Usando o Modelo ITMark", Journal on Advances in Theoretical and Applied Informatics, p. 7-11, v. 2, n.1, 2016.

[20] SOFTEX, Associação para Promoção da Excelência do Software Brasileiro. Disponível em: <http:// www.softex.br/mpsbr/mps/mps-br-em-numeros>. Campinas, São Paulo, Brasil. Acessado em: 16 de Junho de 2016.

[21] M. A. Talib, A. Khelifi e T. Ugurlu, "Using ISO 27001 in teaching information security", 38th Annual Conference on IEEE Industrial Electronics Society - IECON, p. 3149-3153, 2012.

[22] ISO27001, ISO/IEC Std. ISO 27001:2005, Information Technology - Security Techniques - Requeriments. ISO, 2005.

[23] ISO33000, ISO/IEC Std. ISO 33000:2014, Information Technology - Process Assessment Standard. ISO, 2014.

[24] 27001 Academy, "O que é ISO 27001?". Disponível em: <http://advisera.com/27001academy/pt-br/o-que-e-a-iso-27001>. Acessado em: 16 de junho de 2016.

M. P. Silva Graduou-se em Processamento de Dados na Faculdade de Tecnologia de São Paulo (FATEC), Especialista em Gestão de Projetos na Universidade Internacional de Curitiba (UNINTER), Mestre em Ciência da Computação pela Universidade Estadual de Londrina (UEL) e profissional certificado PMP (Project Management Professional). Trabalha no IST – Instituto SENAI de Tecnologia do SENAI (Serviço Nacional de Aprendizagem Industrial), Londrina, Paraná, onde é consultor de negócios e professor no curso de MBA em Gestão de Projetos desde 2012. Seus interesses estão relacionados com gestão de projetos, melhoria de processos de software e projetos de inovação.

R. M. Barros Graduou-se em Ciência da Computação pela Universidade Federal de São Carlos (UFSCar) e em Administração de Empresas pela Universidade Estadual de Londrina (UEL), Mestre em Ciência da Computação pela Universidade Federal do Rio Grande do Sul (UFRGS) e Doutor em Engenharia Elétrica pela Universidade Estadual de Campinas (UNICAMP). Desde 1995 é Professor do Departamento de Computação da Universidade Estadual de Londrina, ministrando aulas no curso de Ciência da Computação, tanto na graduação, como no mestrado. Seus interesses estão relacionados com Engenharia de Software.