The risks analysis like a practice of secure software development. A revision of models and methodologies

José Carrillo Verdún[1], Gloria Gasca Hurtado[1], Edmundo Tovar Caro[1] and Vianca Vega Zepeda[2]

1 Universidad Politécnica de Madrid, Departamento de Lenguajes y Sistemas Informáticos e Ingeniería de Software, Madrid, España, {jcarrillo,etovar}@fi.upm.es; glogasca5@yahoo.com
WWW home page: http://www.upm.fi.es

2 Universidad Católica del Norte, Departamento de Ingeniería de Sistemas y Computación, Antofagasta, Chile, vvega@ucn.cl
WWW home page: http://www.ucn.cl

Abstract. The following document, presents and analyzes the Risks Analysis in the whole software development life cycle, framed like one of the recommended practices for secure software development. It present and compare a set of Risk Analysis methodologies and strategies, considering like criteria some classifications propose by different authors and the objectives that they persecute to orient them towards of evaluation criterion for the secure software development.

1 Introduction

When a new software product is developed, assuring the incorporation of all functionalities required by the users to the new system is not enough, a set of quality characteristics exists which must consider it at software designing and implementing time. On these quality characteristics, exist diverse models and standards developed, under which different quality attributes are considered, they can vary of model in model. Between these attributes, they are possible to be mentioned for example, software mantenibility, reusability, correction, integrity, efficiency and security, among others and vary according to the model.

In relation to the security, the increasing technology incorporation in all organizational processes, has caused that this attribute acquires real relevance, that at present, multiple researches are made, like one carried out in the United States in 2003 [1], where representatives of the industry, academy and the Government, met them for analyze the consequences of the vulnerabilities of the developed software products under the traditional development models, that models do not incorporate

Please use the following format when citing this chapter:

Verdún, J.C., Hurtado, G.G., Caro, E.T., Zepeda, V.V., 2006, in IFIP International Federation for Information Processing, Volume 213, Network Control and Engineering for QoS, Security, and Mobility, V, ed. Gaïti, D., (Boston: Springer), pp. 27–39.

adecuately the security like a necessary characteristic throughout the software development life cycle. This forum, in addition, has made a series of recommendations to follow with the purpose of improving the development processes in the software developer organizations.

At the present time, several works and proposals about software development, indicate the importance of studying and investigating the products security. For example, the process proposed by Software Engineering Institute of the University of Carnegie Mellon, Team Software Process, which has evolved to the TSP-Secure, or the CMM model, developed by the same Institution, that it has served as base for the development of CMM System Security Engineering.

In general, the software security is limited by the work that develops the operators of the implemented systems to protect the vulnerabilities identified in the organization, having a great infrastructure mounted and handled by people who determine and raise the security policies; but software that they protect, has been designed with the security that deserves?, From the beginning of their construction, has been considered the different properties from security and they have been developed throughout its implementation?

This article deals with the Security focused on development process, being centered in a revision of the practice of the Risks Analysis from different aspects. In the first place techniques and approaches are described taking like main reference the McGraw proposal for secure software development (section 2). The McGraw's proposal shown in fig 1, introduces best practices of security and involves a interdisciplinary atmosphere to apply them and to develop them, with the purpose of fighting against the problems which it is exposed software, specifically about connectivity, extensibilidad and complexity [2].

Later (section 3), appear different risks management methodologies. And finally, a comparative of risks analysis tools is made, which raises certain practices like security tests application, threats models use, attacks patterns and risks analysis (section 4).

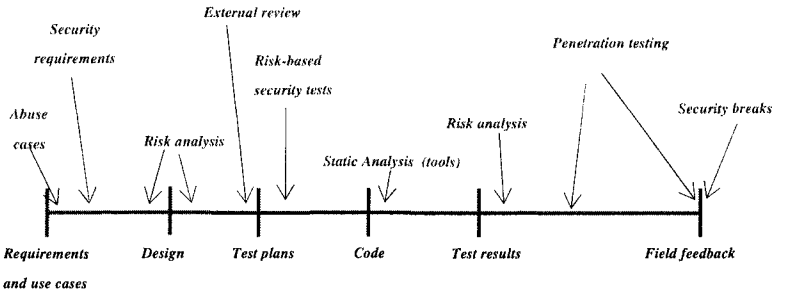

Fig. 1. Software development life cycle - McGraw's proposal

2 Risk Analysis

Throughout this document the concepts software security have been treated from the quality perspective, locating the security like an attribute of the same one.

Between the diverse concepts that exist of quality, it has been taken like reference that is mentioned in [3]. That one reference to that the quality is given by the client requirements, it is to say that "the quality exists in a product when it is apt for the use that the clients that buy it give him." Considering this definition of quality, it is important to focus the Risks Analysis like a support element to identify those problems that affect a software development project.

In the software development processes models Spiral, considered like a realistic approach for great scale systems, the Risks Analysis is also proposed throughout the software development life cycle [4]. This Paradigm uses an evolutionary approach, allowing to the developer and the client to understand and to react to the risks in each level. It uses the creation of prototypes like a risk reduction gear[1]. The Spiral Model recommends the iterative Risks Analysis within the phases of the software development life cycle, defining explicitly the stages in which it must be made, which agree with the McGraw's model [2]; where it recommends the accomplishment of the Risks Analysis of high level in the early phases and its iterative application throughout the service software development life cycle, specially in the Testing stage [5].

McGraw in [6], raises the security is due to incorporate throughout the software development cycle whole, with the purpose of include characteristic emergent like: to specify what must be protected, who must to be in charge and by how long must become that protection.

The security is always related to the information and the services that must be protected, therefore it has relation with the intruders skill, who attack the system. The risk analysis, specially in the design level, allows to identify the main security problems and their impact [7], once identified and classified allows to establish the guide of software security tests.

The attack models are a very useful tool for the identification of the risks that can affect a new software product. The classification and identification of the attacks models that Whittaker proposes [8] and the risks taxonomy propose by Wang and Wang in [9] gives facilities to do the risks identification task by means of possible attacks to the system.

Some studies made[2] sustain the importance that it has to specially do an risks analysis in early stages of the software development. In addition, Microsoft informs that more than 50% of the software security problems they are in design defects, nevertheless, the work for measure the software security and the risks are important throughout the software development life cycle [6].

As it is observed in fig 1, and like it has considered in the preceding paragraphs, it recommended to do the Risk Analysis in the Requirements, Design and Tests stages. In the following sections, some approaches for each one of these stages are described.

[1] http://www.itlp.edu.mx/publica/tutoriales/analisis/index.html
[2] www.cio.com/archive/021502/security.html

2.1 Risk Análisis in Requirement level

Next three strategies considered in [5] are enunciated , they describe the risks analysis process in the Requirements phase:

1. **SecureUML**: It is a methodology for access control policies modeled and for the handling of the integration model in the software development. SecureUML is located in the access control and the security requirements models for applications in predictable atmospheres.
2. **UMLsec**: It is an extension of UML that allows the security characteristics modeled related to confidentiality and access control[3].
3. **Abuse Cases Model**: Proposed by Sindre and Opdahl as a way to understand the form in which it would be possible to be responded to the applications threats in less controlable surroundings; they describe the functions that the system does not have to admit.

2.2 Risk Análysis in Design level

In the Design level, the risk analysis must fulfill characteristics like the indicated in [6]: a consequent system vision, the high level of system knowledge and the consideration of the typical vision of analysts and developer when they belive in the sufficiency to describe and to discover the design problems in the code level. In adition, it is also necessary to consider the business risk analysis and the architectonic risk analysis:

1. **Business Risk Analysis**: The companies wants answers as opposed to the investment and to the cost. Therefore, to appraise the impact is a primary target at the moment for do the risk analysis, considering that a good strategy considers questions of cost of the project, so that the direction of the organization can decide the investment in software in relation to the direct cost (responsibility, wasted productivity and reelaboration) as indirect cost (reputation and damage of mark) [10].
2. **Architectonic Risk Analysis**: Similar to the previous one, this analysis measures the technical security exposition in the proposed design of an application and it connects them with the impact of the company. Beginning with a representation of high level of the design, the analysis team considers each one of the modules, interface, interaction, etc. against the well-known attack methodologies and their success probability. In order to provide a general visualization of the security state of a software system, the analysts apply the analysis against the individual design subcomponents [10].

2.3. Risk Analysis in the Testing level.

The risks evaluation in the Testing phase, it allows to evaluate the system against the different risks that affect the product quality. The Risk Analysis in this stage

[3] www4.in.tum.de/~umlsec/

allows the project team to arrange and to compare the quality risks with the other categories risks. Categories as like they are defined in [3]:

a) **Financial risks**: It affects the project budget.
b) **Schedule Risks**: They affect the time assigned to project
c) **Feature Risks**: They affect the product characteristics, generally their development obtained a mistaken result.
d) **Quality Risks**: They affect the relation client - satisfaction.

This analysis assures the evaluation of product quality risks and the failures identification in different attributes from quality, not only in the software functionality. The Risk Analysis also will have to be do having in account other characteristics, like the Rex Black's recommendation in [3]. The same author proposes the accomplishment of Risk Analysis under three techniques:

1. **Informal technique**: It works well without considering the development process maturity. The author proposes the use of a table with three columns where the Risks, the error mode associated to the risk will be enunciated and finally a column of Priority, determining evaluation ranks. For the risks idenficación, the errors and specially the priority; the author raises a meeting with a team of project key people.
2. **Standard ISO 9126 Approach**: This standard proposes that the software system quality can be measured throughout six very important characteristics:
   Functionality: System Capacity requeridad
   Reliability: The system works when it is needed and how it is needed.
   Usability: The System can be to use like instinctive, comprehensible and useful for the users.
   Efficiency: Resources use.
   Mantenibility: System update facility.
   Performance: System answer capacity.
   Like in the Informal Technique, the Risk Analysis process, is developed defining quality sub-characteristics also identified in the standard - within which is the security – and the priority levels related to the test of each area are determined for the project stakeholders.
3. **Failure Mode and Effect Analysis (FMEA)**: It is a tool that reviews the potential product or the process failures, it values the risk priorities[4]. This tool appears in spreadsheet format and it admits a easy analysis evaluation. The use of this method is advisable specially on development projects very structured, with the purpose of formalizing the of quality risk analysis process. An example of application of this tool is described in [3].

The key of an Risk analysis that supports the software development process in iterative form, from early stages like design, to final stages like Testing; it is the accomplishment of a good analysis, using tools and methodologies able to bring to light software problems that with the tests or a delayed Risk analysis would not be identified or would be correct easily and consequently it obtain a unsecure software development.

[4] http://web2.concordia.ca/Quality/tools/11failuremodeanalisys.pdf

3 Risks Management Methodologies

In order to be able to develop a secure software product, able to proactively resitir the attacks which is exposed, it is essential to consider the risks throughout the development cycle. With this objective, different strategies and frameworks have been proposed, they harnesses the risks identification, allowing managing them, that is to say, to plan, to implement and to control the measures against the risks and vulnerabilities founded.

3.1. Risks Management Proposals

Next, some strategies propose appear to develop the risks management. They have been selected by the endorsement and recognition that have the organizations who have developed them.

Risk Management Framework (RMF): This proposal has been elaborated by Cigital, where the business goals determine the risks, the risks lead the methods, the methods measure the yield, the measures handle the decisions support and the decisions support handles the reajuste/reelaboration and the aplicationn quality [6]. The RMF intention is to assume a capable, consequent and repetible approach for the risks prevention. The Cigital's proposal describes in [11] like a iterative process, it trim in five basic activity stages, concentrated in following the trajectory, visualizing and to understand the process with respect to the software risk. This structure has been applied in the software field during almost 10 years [11] and the design that presents allows to discover the company risks, including those of software. RMF consists of five fundamental stages:

1. **Understand the Business Context:** The business objectives and risks are identified. The analyst will have to extract and to describe the objectives of the company, the priorities and circumstances to understand the software risks perfectly [11].
2. **Identify and link the Business and Technical Risks:** It must identify business risks. Aid to define and to direct the use of technical methods to extract, to measure and to mitigate the software risk. On the other hand, the technical risks, involve impacts like unexpected system faults, failures in the software controls, data modification. This stage is understood like one of the best practices of Fig 1.
3. **Synthesize and Rank the Risks:** Within the two previous stages, it will find many evident risks, nevertheless the sintetización and priorización of these will have to serve to give value to the analysis process that is tried to make.
4. **Define the Risks Mitigation Strategy:** This strategy will be defined under the business context. It must identify the validation techniques that are going to be used to mitigate appropriately the risks.
5. **Carry out Fixes and Validate:** When a strategy is defined (step 4) it must be executed. When identifying a problem it must be rectified, following the defined strategy. This process must be measured in relation to the risk mitigación strategy.

Finally the Cigital's proposal raises an additional activity but not less important, to inform and to report.

Framework for Managing Information Security Risk: Software Engineering Institute (SEI) of the University of Carnegie Melon, has developed the evaluation strategy OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation), whose objective is to measure the organizacional risk and it focuses in strategic and practical aspects. Aid to an organization to take decisions on the basis of the risks from confidentiality, integrity and availability of the critical assets associated to the information that has its [12]. In this context, the SEI also proposes a Risks Managing Framework [13] it is a risks identification process and its address. Next, they briefly describe each one of the stages that conforms the cyclical process:

1. **Identify:** The objective of this stage is to anticipate the risks, before problems appear. As result it obtains a set of documented risks, including critical assets, threats and vulnerabilities.
2. **Analyze:** This point is the of specific risk analysis. The obtained result is the impact and probability of occurrence of each identified risk and a mitigación approach of such risks.
3. **Plan:** The actions are determined to develop to improve the organization security and the critical assets protection. As result is obtained: protection strategy; risks mitigation plan; action plans, budget, success criteria, indicators for to monitor the fulfillment of the action plans and the allocations of responsibility for the implementation of these plans.
4. **Implement:** Its objective is to execute the defined action plans.
5. **Monitor:** It is the track process of the action plans to determine its fulfillment. Some results of this stage are: Completed actions, progress reports, indicators risk.
6. **Control:** In this stage it determines if the personnel adjusts to the defined action plans, and if the organizacionales changes have caused new risks. As result new decisions can be obtained on changes in the plans or due to the new risks identification.

Magerit: Information Systems Risks Analysis and Management Methodology. The reason of being of Magerit is directly related to the generalization of the use of the electronic, computer science and telematics means, it supposes evident benefits; but also it gives rise to certain risks that must be diminished with security measures which they generate confidence. Magerit allows to know the risk that the work elements are put under, being considered an essential procedure[5]. This methodology proposes a methodical approach that allows to make decisions with foundation and to rationally explain the taken decisions. The risk determination is made by means of six steps defined methodically in [14], they are:

1. To determine the eminent assets for the organization.
2. To value such assets based on the cost that would suppose for the organization to recover it of a failure of availability, integrity, confidentiality or authenticity.
3. To determine to what threats are exposed those assets.
4. To value the vulnerability of the assets to the potential threats.

[5] http://www.csi.map.es/csi/pg5m20.htm

5. To consider the impact, defined as the damage on the assets derived from the materialization of the threat.
6. To consider the risk, defined as the impact weighed with the rate of occurrence of the threat.

Integrated approach for risks mitigation: The Institute of Technology of Californian Jet Laboratory Propulsion along with the University of Californian At Davis, has developed an integrated approach for security risks mitigation [15], it form of the following components:

a) **Vulnerability Matrix (Vmatrix)**: It is a data base that contains catalogued vulnerabilities taxonomy and that can be acceded like library.
b) **Security Assessment Tools (SAT)**: It is a tools list available, where the intention of each one is included.
c) **Properties-based Testing**: It tries to cover the existing emptiness between the formal verification and the ad-hoc verification.
d) **Model-Based Security Specification and Verification**: It is used to verify if they are fulfilled the wished security properties.

The authors indicate that although, each component can be applied in independent form, when applying them altogether, it obtain benefits like the developing system trustworthiness is increase.

3.2. Proposals Analysis

The strategies presented in the previous section, they are coincident in several points. Perhaps one of most important is the implicit recognition that it is impossible that the 100% of the detected risks they are eliminated, thus is necessary and imprecindible the risks priorización based on the damage that can cause, of such way to invest greater resources in those than can cause greater losses to the organization. Others of the agreement points are given by the iterative approach of the proposals, reaffirming of this form the fact that the risks and threats can be varying through the time, thus, it due to do constants revisions and adjustments to the new organizations reality. The three first proposals are oriented to give processes to follow to manage the risks, however, the last integrated approach proposal, is but well a tools set that facilitates this work.

4 Risk Analysis Tools

Next, it briefly describe a tools set for the risk analysis development, which in the following section will be put under a classification and comparison on the basis of the criteria explained down. The tools selection has been do having in account the prestige and experience of the organizations who have developed them or who suggest them as successful tools for the risk analysis.

Microsoft's STRIDE: *Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege*[6], it is a commercial tool, developed to support the threats identification in the software development. Keith Brown, in their book "The .NET Developer's Guide to Windows Security"[7], enunciates the importance of the threats modeled when software is development and designs and he raises as guideline for his modeled the use of this tool. As well, Kenneth van Wyk[8] raises the accomplishment of risks analysis to prevent threats in the software development and he relates the utility of this tool like support to the work, effort and time that a good risks analysis requires.

Sun's ACSM/SAR: It was created to evaluate of formal way the software development and to determine its security level. Mark G. Graff and Kenneth R. van Wyk[9] study the code maintenance within software development because they consider it vital for the security and they propose methodologies and practices for the security software development from the point of view of evaluations for this analysis. For that reason its proposal enunciates tool ACSM/SAR and ASSET like good elements for the developer.

ASSET: Automated Security Self-Evaluation Tool is the automated version of questionnaire "Security Self-Assessment Guide for Information Technology Systems", created by National Institute of Standards and Technology (NIST). This questionnaire looks for to help in the systems security evaluation that has an organization. ASSET is forms of two tools: ASSET-System, this one is the interface that allows to respond the questionnaire; and ASSET-Manager which orders and summarizes the questionnaire application results.

Siemerns CRAMM: Risks Valuation Tool. It includes in addition, other tools that approach tasks like: to identify the impact of the risk valuation in the company, to measure the threats and the vulnerabilities, to identify risks and justifying the required controls, based in the risk valuation. Within the advantages of this tool, the developers argue[10] that it has an excellent capacity to determine requirements for specific controls like: Authentication Level, Encriptation and Hardware Protection, to identify security functional requirements required by the new application, to develop security requirements, evaluation of a security atmosphere, among others.

Cigital's SQM Solutions: Cigital Software Quality Management, was created under the motto "To identify and to eliminate software security defects during the software development and it test" the product Cigital SQM tries to offer a new series of solutions and services for software quality developed around innovating products. In addition, this tool combines the risks prevention, software measurement and software process improvement to help the companies to lead the cost of the quality software development.[11]

SecureUML: It is done on the UML base (Unified Modeling Language). This tool considers the advantages to integrate security engineering in the software

[6] http://books.slashdot.org/article.pl?sid=05/11/21/1442228

[7] http://pluralsight.com/wiki/default.aspx/Keith.GuideBook/What%20Is%20A%20Security%20Principal.html

[8] http://www.esecurityplanet.com/views/article.php/3417561

[9] http://www.cedarlug.org/article.php?story=2004040617250150

[10] http://www.insight.co.uk/files/datasheets/CRAMM%20(Datasheet).pdf

[11] http://www.cigital.com/news/index.php?pg=art&artid=110

development life cycle, with the purpose of facilitating the mature security development beyond avoiding the infraction of the security policies.[12]

UMLSec: Its objective is to raise an approach based on UML (Unified Modeling Language) it allows to express the information related to the security by means of diagrams in the system specification. Therefore UMLsec is defined under the UML profile, in particular when associating the security restrictions of a software design, references to a formal semantics of a simplified UML fragment[13].

Failure Mode and Effect Analysis (FMEA): It is a methodology to analyze and to discover all the potential system error ways, its effects and how to correct or to mitigate these failures. It is the analysis procedure more used in the initial stages of the systems development like Conceptual Design stage[14], nevertheless there are authors like Rex Black that considers the possibility and utility of this tool to eliminate all the potential system failures, therefore they focus it in the Testing stage. It is a specific methodology to value the system, the design, the process, or the service in the different possible ways in that the failures (problems, errors, risks, consequences) can happen [16].

Pilar: The risks analysis and management methodology Magerit (section 3) in its second version[15], is accompanied by the risks analysis and management tool PILAR, elaborated by the National Cryptoanalytic Center and the Spain Public Administrations Ministry; it allows to define the assets and threats of an information and communications system, with object to determine its safeguard that allow to reduce the risk to which is put under the system[16]. PILAR constitutes a tools set that supports to the information system risks analysis and management, following the Magerit 1.0 methodology and that at the present time offers:

a) Pilar-1: qualitative analysis, before entering a detailed quantitative analysis.
b) Pilar-2: detailed quantitative analysis, with the purpose of obtaining results of the investment recovery in its safeguard, in terms of declining risk[17].

5. Risk Analysis Tools Comparative

The following table shows a classification and comparison of the described tools. This classification uses some criteria proposed by McGraw (Column Type) and others defined by the authors of this article (Column Security).

The criterion "Type" indicates the classification given by McGraw in [5]. In the comparative that appears it indicates the objective that looked for to reach at the time of its development:

- Commercial: Those methodologies done with an aim to commercialize it like support to certain task within the software development.

[12] http://www.foundstone.com/resources/whitepapers/wp_secureuml.pdf
[13] http://www4.in.tum.de/~juerjens/papers/uml02.pdf
[14] http://www.nepss.org/presentations/dfr9.pdf
[15] http://www.revistasic.com/revista64/propuestas_64.htm
[16] http://www.boe.es/boe/dias/2004/11/23/pdfs/A38750-38750.pdf
[17] http://www.ccn.cni.es/medidas_tecnicas/herramientas.htm

- Standards: They are tools, standards or methodologies done by official institutions and proposals like standards of risk analysis.
- Security: It has been catalogued because they have been thought under the criteria of software security or secure software, is to say that the security aspects are the main objective to support within the development of the risk analysis.

The criterion "Security", determined by the authors of this investigation, looks for to categorizar the methodologies and tools considering the support levels that can offer these methodologies in the security requirements analysis for the software development, from a low level at a high level, of the following form:

**: Low Level
***: Mean level
****: High Level
*****: Very High Level

Table 1. Risks Analysis Methodologies and Tools Classification.

Tool or Metodology	Type	Security
Microsoft's STRIDE	Comercial	****
Sun's ACSM/SAR	Comercial	***
ASSET	Comercial - Standard	***
Siemerns CRAMM	Comercial	***
Cigital's SQM Solutions	Comercial-Security	*****
SecureUML	Comercial- Security	****
UMLSec	Comercial- Security	****
Pilar	Standard	**
Failure Mode and Effect Analysis (FMEA)	Security	****

Of this form, the Low Level indicates that the mentioned methodology or tool allows to make an risk analysis, but that its philosophy has not been thought directly in analysis of software security aspects, whereas the Very High Level, it will occur to a tool that has been constructed or raised under the philosophy of the software security aspects, considering the difference between security software and safe software (critical).

When the table is analyzing, it can be observed that most of the risks analysis tools were not developed for its exclusive application in the software security development, but well, they are of general use. The approaches and strategies of security and risks evaluation in the organizations, have been focused like a necessity by the increasing incorporation of the information technology, although it is certain, the software products are part of this technology, at the time of making the risks analysis, would be due to incorporate particular considerations, as threats and typical attacks that frequently happen, and also the vulnerabilities generated by errors or negligences in the design and implementation of these products.

The objective to describe the security aspects of the methodologies mentioned, is to focus future research works directed to support the Risk analysis like a good practice within the life cycle, framed in the proposal of figure 1.

6 Conclusions

The importance of Risk Analysis in the early stages of the software development life cycle, like it has been showed previously; it extends from the product quality to the security and evolve to such an extent that wakes up the interest of the business in aspects like costs and investment return.

In the security scope, if the requirements and necessities of an organization are not considered from the early stages of the software development life cycle and these are not evaluated in the other development stages, hardly it will be obtained a system robust, able to repulse the attacks so common in the present time.

Every day the organizations take more serious the security problems, and this is demonstrated with the different initiatives taken to do that the software developers become aware from the importance of improving their processes, incorporating practical that they look for to reach the security product implementation, proactive to the attacks. The necessity to incorporate the study and application of the security software life cycle under the standards parameters and associated quality models to good practices, with the purpose of having developments able to respond and to face the attacks and the systems attackers, it is complemented with the preoccupation of the industry, the academy and the commerce giving as result variety of efforts in the search to raise solutions to this problem.

The study and the Risk Analysis Tools comparative made present the beginning of the investigation that are developing the authors of the present article, leaving laid the way to investigate thorough the methodologies, tools, standards and principles to establish development models with practices and evaluations at the right moment to guarantee the quality, evaluating in first instance the security in the software development. Mainly the study to the practices raised by McGraw, shown in fig 1, for the security software development is left open.

References

1. N. Davis, W. Humphrey, S. Redwine, G. Zibulski, and G. McGraw, "Processes for producing secure software," *Security & Privacy Magazine IEEE*, vol. 2, pp. 18 - 25 2004.
2. G. McGraw, "Software Security," *IEEE Security & Privacity*, pp. 80-83, 2004.
3. B. R., "The Risks to System Quality Investing in Software Testing Series, Part 3."
4. I. Sommerville, "Ingeniería de Software," P. Education, Ed., 6 ed. México, 2002.
5. D. M. Verdon, G., "Risk analysis in software design," *IEEESecurity & Privacy Magazine*, vol. 2, pp. 79-84, 2004.
6. G. McGraw, "From the ground up: the DIMACS software security workshop," *IEEE Security & Privacy Magazine*, vol. 1, pp. 59-66, 2003.

7. B. M. Potter, G., "Software security testing," *IEEESecurity & Privacy Magazine*, vol. 2, pp. 81-85, 2004.
8. J. A. Whittaker, "Software's invisible users," *IEEE Software*, vol. 19, pp. 84-88, 2001.
9. H. W. a. C. Wang, "Taxonomy of security considerations and software quality," *Communications of the ACM*, vol. 46, pp. 75 - 78, 2003.
10. K. R. M. Van Wyk, G., "Bridging the gap between software development and information security," *Security & Privacy Magazine IEEE*, vol. 3, pp. 75 - 79, 2005.
11. G. E. McGraw, "Risk Management Framework (RMF)," *Cigital, Inc.*, 2005.
12. C. Alberts, Dorofee, A., Stevens, J., Woody, C., "Introduction to the OCTAVE Approach," vol. Software Engineering Institute, 2003.
13. C. Alberts and A. Dorofee, *Managing Information Security Risk. The OCTAVE Approach*: Addison Wesley, 2005.
14. J. Mañas, "Pilar. Herramientas para el Análisis y la Gestión de Riesgos," 2004.
15. D. P. P. Gilliam, J.D.; Kelly, J.C.; Bishop, M.;, "Reducing software security risk through an integrated approach," *Software Engineering Workshop, 2001. Proceedings. 26th Annual NASA Goddard*, pp. 36 - 42 2001.
16. H., *Failure Mode and Effect Analysis. FMEA from Theory to Execution*, Second Edition ed.