UNIVERSIDAD SIMÓN BOLÍVAR | INSTITUTO DE POSGRADOS

PROPUESTA METODOLÓGICA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL SISTEMA DE INFORMACIÓN FÉNIX DE LA CLÍNICA BONNADONA PREVENIR

Ing. Camilo Andrés Salgado Castro
Ing. Brian Benjamín Caballero Villamil
Ing. Jeison José Llano Álvarez

Trabajo de Investigación o Tesis Doctoral como requisito para optar el título de Especialista en Gestión de Tecnologías de la Información

Tutores
Sandra Patricia Ferreira Pérez

RESUMEN

La mala gestión de riesgos asociados a la seguridad de la información ha propiciado una generación de cambios tanto en herramientas tecnológicas, recursos humanos, y otros agentes que son de gran impacto en la Organización Clínica Bonnadona. Este documento se centra en desarrollar una metodología para la gestión de riesgos de seguridad de la información del software Fénix, basados en la articulación de marcos de trabajo como Cobit 5, las normativas ISO 27001 y la norma técnica ISO/IEC 27005, y el estándar para la seguridad de las aplicaciones Web (OWASP). Teniendo en cuenta lo anterior, se busca proteger en primera instancia el activo más importante que tiene la organización que es la información tanto del cliente interno como el externo.

El desarrollo e implementación de proyectos de software para las entidades del sector salud, debe llevar consigo el complimiento del conjunto de normativas legales que surgen de la necesidad de proteger el activo de información que posee la organización. En 2012 el gobierno nacional mediante la ley 1581, regula el derecho fundamental de *Habeas Data* con la finalidad de proteger los datos personales registrados en cualquier base de datos que permita realizar operaciones como recolección, almacenamiento, uso y tratamiento por parte de las entidades de naturaleza pública y/o privada (COLOMBIA, 2012).

la organización debe fijar reglas de protección, medios de control y una regulación concreta para el manejo y tratamiento de los datos personales tanto del cliente interno como el externo, lo cual se convierte en unos de los principales riesgos a tratar y evaluar de forma constante, por lo tanto, obliga potencialmente a la organización a tener un modelo consistente de identificación, gestión, evaluación y tratamiento de los riesgos asociados al software Fénix.

Por lo anterior, se propone una metodología articulada para cubrir aquellos puntos críticos que el marco de trabajo, normativas y estándar seleccionados no abarcan, con el fin de tener una metodología consistente que permita una buena gestión de riesgos de seguridad de la información.

La metodología se planteó en dos etapas principales, la primera correspondería a las buenas prácticas propuestas por Cobit para la implementación de un gobierno de TI para el área de desarrollo de software, y una segunda etapa que correspondería en su forma base al proceso de gestión de riesgos de seguridad de la información propuestos en la ISO 27001 y la NTC ISO/EC 27005 que se articularía con las mejores prácticas de Cobit y OWASP, para crear una metodología consistente que permita identificar, gestionar, evaluar y tratar los riesgos de seguridad de la información en el software Fénix.

La segunda etapa de la metodología, esta subdividida en 5 actividades o fases como lo son: establecimiento del contexto (articulada con Cobit 5), identificación del riesgo y estimación del riego (articulada con ISO 27001, NTC ISO/IEC 27005), evaluación del riego (articulada con OWASP), tratamiento del riesgo (articulada con Cobit) y por último la aceptación del riesgo (articulada con ISO 27001, NTC ISO/IEC 27005). Lo anterior complementado por las actividades transversales de comunicación del riesgo y monitoreo del riesgo.

Antecedentes:

La Organización Clínica Bonnadona Prevenir, cuenta con un departamento de calidad encargado de asegurar el cumplimiento del conjunto de políticas definidas, así mismo, con la identificación, gestión, evaluación y tratamiento de los riesgos en los diferentes departamentos que conforman esta unidad. La verificación constante de la evolución de los objetivos dentro de

los plazos previstos y de los recursos que fueron asignados para dichos objetivos, hace de este departamento muy importante, sin embargo, no profundiza cuando se trata de tecnologías de la información y proyectos de software. En base a lo anterior, los riesgos identificados en la matriz creada por el departamento de calidad, no se alinean a los específicos del área de desarrollo de software.

Objetivos:

Desarrollar basados en la articulación de Cobit 5, las normas ISO 27001, NTC ISO/IEC 27005 y el estándar OWASP una propuesta metodológica para la gestión de riesgos de seguridad de la información del software Fénix.

Materiales y Métodos:

Para desarrollar este documento, utilizamos artículos de la base de datos de investigación académica IEEE, además se revisaron estudios en la web donde ya se había aplicado cobit 5 para la gestión de riesgos en software, así mismo, donde se implementó una metodología de gestión de riesgos utilizando el estándar OWASP. También, se indago sobre la ley colombiana para el tratamiento de *Habeas Data*, y las normas ISO 27001 y la NTC ISO/IEC 27005.

Durante la creación de esta propuesta, se utilizaron métodos de recolección de datos como talleres, lluvia de ideas, además, se tomaron en cuenta los reportes o incidencias hechos en el mismo software.

Resultados:

Se logró crear una metodología para la gestión de riesgos de la seguridad de la información aplicable inicialmente al software Fénix, que esta alineada a las políticas de la

organización y a su vez a los lineamientos establecidos en el área de desarrollo de software. Luego de implementar la metodología donde se tomaron como ejemplo un grupo de tres riesgos, se evidencio que existen fallas en cuanto a seguridad de la información en el aplicativo que serán tratados con su respectivo plan de acción.

Conclusiones:

La articulación de Cobit 5 con las normativas ISO 27001, la norma técnica ISO/IEC 27005, y el estándar para la seguridad de las aplicaciones Web (OWASP), permitió crear una metodología consistente para la buena gestión de riesgos referentes a la seguridad de la información. Esta gestión de riesgos impactará de forma radical la finalización del proyecto y se podrá implementar en proyectos de software futuros. Así mismo, permitirá establecer un gobierno para el área de desarrollo de software basado en las buenas prácticas propuestas del marco de trabajo de Cobit 5.

Palabras clave:

Cobit, Metodología, ISO 27001, NTC ISO/IEC 27005, Owasp, Bonnadona, Organización, Riesgos, Gestión de Riesgos, Gestión, Paciente, Software Fénix, Software, instrumento, análisis, análisis de riesgos

ABSTRACT

The mismanagement of risks associated with information security has led to a generation of changes both in technological tools, human resources, and other agents that have a great impact on the Bonnadona Clinical Organization. This document focuses on developing a methodology for the management of information security risks of the "Fénix" software, based on the joint of frameworks such as Cobit 5, the ISO 27001 regulations and the ISO / IEC 27005 technical standard, and the standard for Web Application Security (OWASP). Considering the above, it seeks to protect in the first instance the most important asset that the organization has, which is the information of both the internal and external clients.

The development and implementation of software projects for entities in the health sector must carry with it compliance with the set of legal regulations that arise from the need to protect the information asset owned by the organization. In 2012 the national government through law 1581, regulated the fundamental right of Habeas Data in order to protect personal data registered in any database that allows operations such as collection, storage, use and treatment by entities of nature public and / or private (COLOMBIA, 2012).

The organization must establish protection rules, means of control and a specific regulation for the handling and processing of personal data of both the internal and external clients, which becomes one of the main risks to be dealt with and constantly evaluated, therefore, it potentially forces the organization to have a consistent model for the identification, management, evaluation, and treatment of the risks associated with the "Fénix" software.

Therefore, an articulated methodology is proposed to cover those critical points that the selected framework, regulations and standards do not cover, in order to have a consistent methodology that allows a good management of information security risks.

The methodology was proposed in two main stages, the first would correspond to the good practices proposed by Cobit for the implementation of an IT governance for the software development area, and a second stage that would correspond in its basic form to the management process of Information security risks proposed in ISO 27001 and NTC ISO / EC 27005 that would be articulated with the activities of this process, to create a consistent methodology that allows identifying, managing, evaluating and treating information security risks in the “Fénix” software.

Background:

The Bonnadona Prevenir Clinical Organization has a quality department in charge of ensuring compliance with the set of defined policies, likewise, with the identification, management, evaluation, and treatment of risks in the different departments that make up this unit. The constant verification of the evolution of the objectives within the foreseen deadlines and of the resources that were assigned for said objectives, makes this department very important, however, it does not go in depth when it comes to information technology and software projects. Based on the above, the risks identified in the matrix created by the quality department are not aligned with those specific to the software development area.

Objective:

To develop based on the articulation of Cobit 5, the ISO 27001, NTC ISO / IEC 27005 standards and the OWASP standard a methodological proposal for the management of information security risks of the “Fénix” software.

Materials and Methods:

To develop this document, we used articles from the IEEE academic research database, in addition, studies on the web were reviewed where cobit 5 had already been applied for risk management in software, likewise, where a methodology for managing risks was implemented. risks using the OWASP standard. Also, the Colombian law for the treatment of Habeas Data, and the ISO 27001 and NTC ISO / IEC 27005 standards, was investigated.

During the creation of this proposal, data collection methods such as workshops, brainstorming were used, in addition, reports or incidents made in the same software were considered.

Results:

It was possible to create a methodology for information security risk management applicable initially to Fénix software, which is aligned with the organization's policies and in turn with the guidelines established in the software development area. After implementing the methodology where a group of three risks were taken as an example, it was evident that there are flaws in terms of information security in the application that will be dealt with their respective action plan.

Conclusions:

The Cobit 5 joint with the ISO 27001 regulations, the ISO / IEC 27005 technical standard, and the standard for the Web applications Security Risks (OWASP), allowed to create a consistent methodology for the good management of risks related to the security of the information. This risk management will radically impact project completion and can be implemented in future software projects. Likewise, it will allow the establishment of a government for the software development area based on the good practices proposed in the Cobit 5 framework.

KeyWords:

Cobit, Methodology, ISO 27001, NTC ISO / IEC 27005, Owasp, Bonnadona, Organization, Risks, Risk Management, Management, Patient, Fénix Software, Software, Instrument, Analysis, Risk Analysis.

REFERENCIAS

Arévalo, M. C. (13 de Octubre de 2020). *Opirani*. Obtenido de https://www.piranirisk.com/es/blog/cuantos-controles-tiene-la-norma-iso-27001

Avdoshin, S. M., & Pesotskaya, E. Y. (2011). Software risk management . *2011 7th Central and Eastern European Software Engineering Conference (CEE-SECR)*(10.1109/CEE-SECR.2011.6188471), 1-6.

COLOMBIA, E. C. (17 de Octubre de 2012). LEY ESTATUTARIA 1581 DE 2012. Bogotá. Obtenido de https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf

Foundation, T. O. (2013). *OWASP top 10 - 2013 Los diez riesgos mas criticos en aplicaciones web.* Maryland: Creative Commons Attribution ShareAlike.

H. (06 de 2015). *Bonnadona Prevenir | Misión - Visión.* Obtenido de Organización Clínica Bonnadona Prevenir: https://www.organizacioncbp.org/mision.php

Isaca. (2012). *blplegal.* Obtenido de http://blplegal.net/zoneSite/RestFulApiZoneSite/uploads/1539031830-Cobit%205%20-%20Procesos%20Catalizadores.pdf

Isaca. (2012). COBIT 5.0. Enabling Processes. *Isaca (2012)*. Estados Unidos.

Isaca. (2012). COBIT 5.0. Un marco de negocio para el gobierno y la gestión de TI de la empresa. *Isaca (2012)*. Estados Unidos.

Isaca. (2012). *ucipfg.* Obtenido de https://www.ucipfg.com/Repositorio/MATI/MATI-01/Unidad4/lecturas/51855611-Risk-IT-Framework-Espanol.pdf

Marlene Lucila Guerrero Julio, C. U. (25 de Septiembre de 2019). Evaluación del contexto organizacional en la gestión del riesgo de tecnología de información con un enfoque basado en COBIT. *RITI Journal*, 4. doi:https://doi.org/10.36825/RITI.07.14.004

RAFAEL ENRIQUE RODRÍGUEZ RODRÍGUEZ, A. F. (2018). DESARROLLO DE UN MODELO PARA CALCULAR EL NIVEL DE SEGURIDAD EN SITIOS WEB, BASADO EN EL TOP 10 DE VULNERABILIDADES MÁS EXPLOTADAS EN 2017 SEGÚN EL MARCO DE REFERENCIA OWASP. *DESARROLLO DE UN MODELO PARA CALCULAR EL NIVEL DE SEGURIDAD EN SITIOS WEB, BASADO EN EL TOP*

10 DE VULNERABILIDADES MÁS EXPLOTADAS EN 2017 SEGÚN EL MARCO DE REFERENCIA OWASP, 48-51. Bogotá, Colombia.

Tao, Y. (12 de 08 de 2008). A STUDY OF SOFTWARE DEVELOPMENT PROJECT RISK MANAGEMENT. *2008 International Seminar on Future Information Technology and Management Engineering*, (pág. 1). Leicestershire. doi:10.1109/FITME.2008.125