CONCLUSIONES

Las tecnologías identificadas para la Arquitectura de Software, que permiten el desarrollo de Web Adaptativa, para el Secuenciamiento de Objetos de Aprendizaje del primer curso de programación de computadoras a nivel Universitario son: el Ontology Web Language OWL, el IMS Learning Design, la tecnología Java para la Web, el lenguaje Script de Interacción Action Script 3.0 y el formato de distribución SWF, aplicándose a nivel estructural, los patrones de diseño de software: Composición, Observador y el Modelo Vista Controlador.

La estrategia didáctica propuesta para el primer curso de programación de computadoras soportada por la Web Hipermedia Secuenciadora de Objetos de Aprendizaje está basada en un enfoque cognitivista y teorías de aprendizaje propias del constructivismo.

Los resultados de la evaluación de la Arquitectura de Software propuesta, en comparación con las características de calidad mínima requerida para un proyecto de este tipo nos muestran una diferencia de 70 puntos en el atributo de calidad denominado "Confidencialidad", y 43 puntos en el atributo de calidad "Seguridad Externa", en contra de la Arquitectura de Software Propuesta, pero 35 puntos en el atributo de calidad "Configurabilidad", 19 puntos en el atributo de calidad "Escalabilidad", 17 puntos en el atributo de calidad "Portabilidad", 14 puntos en el atributo de calidad "Interoperabilidad", 12 puntos en el atributo de calidad "Confiabilidad" y 11 puntos en el atributo de calidad denominado "Desempeño" en favor de la Arquitectura de Software propuesta.

Del total de atributos de calidad analizados en la Arquitectura de Software, el 59% de atributos de calidad, son favorables para la Arquitectura de Software propuesta y, el 41% de los atributos de calidad analizados son desfavorables, haciendo adecuada la aplicación de la Arquitectura de Software propuesta, para asegurar el desarrollo de calidad de una Web Hipermedia Secuenciadora de Objetos de Aprendizaje en el primer curso de programación de computadoras a nivel universitario.

BIBLIOGRAFÍA

LA WEB SEMÁNTICA, LA SIGUIENTE GENERACIÓN DE WEBS. (2007). Recuperado el 15 de 12 de 2008, de http://sociedad de la informacion.telefonica.es/jsp/articulos/impresion.jsp?elem=4299

ADL. (2003). Sharable Courseware Object Reference Model (SCORM) Version 1.3, Application pro. Advanced Distributed Learning.

ALVARADO, R. D. (2010). Metodología para el desarrollo de Ontologías.

ARTEAGA, C., FABREGAT, R. (2002). Integración del aprendizaje individual y del colaborativo en un sistema hipermedia adaptativo. Universitat de Girona.

BERNERS-LEE, T., HENDLER, J. A., Y LASSILA, O. (2001). The Semantic Web. Scientific American.

BILLY REYNOSO, C. (2004). Introducción a la arquitectura de software. Buenos Aires: Universidad de Buenos Aires.

GARRETT, J. J. (2005). Ajax: a new approach to web application. Recuperado el 13 de 08 de 2011, de http://www.adaptivepath.com/publications/essays/archives/000385.php

HERRAR MORENO, R. (2010). Simulación de Circuitos Basados en Web. Universidad de Costa Rica.

SALAMANCA, J. (2007). Propuesta didáctica para el rediseño del curso de programación básica. Technology, Engineering And Calculus HewlettPackard MobileEnvironment.

SÁNCHEZ ALONSO, S. (2005). Diseño y uso de objetos didácticos basado en contratos. Madrid: Universidad de Politécnica de Madrid.

SOTO CARRIÓN, J. (2008). Mécanismos semánticos orientados a la flexibilidad de repositorios para objetos de aprendizaje. España: Universidad de Alcalá.

WITBROCK, M., MATUSZEK, C., BRUSSEAU, A., KAHLERT, R. C., FRASER, C. B., Y LENAT, D. B. (2005). Knowledge begets knowledge: steps towards assisted knowledge acquisition in cyc. USA: In Papers of AAAI Spring Symposium on Knowledge .

METODOLOGÍA PARA LA IMPLEMENTACIÓN DE SEGURIDAD ORGANIZACIONAL Y CONTROL DE ACTIVOS SEGÚN NTP-ISO/IEC 17799

METHODOLOGY FOR THE IMPLEMENTATION OF ORGANIZATIONAL SECURITY AND CONTROL OF ASSETS ACCORDING TO NTP-ISO/IEC 17799

ÁREA
Seguridad de la Información

AUTORES
Jahaira Zuleika Campos Pérez[1]
Francisco Richard Herrera Piscoya[2]

RESUMEN

Introducción: En una organización existe información que es muy valiosa y que muchas veces no se sabe de la importancia que esta representa; por tal motivo se pierde eficiencia y eficacia en la gestión de esta. Pero para poder lograr mejorar este escenario es primordial buscar una correcta seguridad organizacional y un efectivo control de activos; ya que ambos son los pilares en la solución que se busca alcanzar.

Objetivo: Proveer una Metodología que permita implementar políticas de seguridad organizacional y control de activos según la Norma Técnica Peruana NTP-ISO/IEC 17799 en la U.N.P.R.G.

Supuesto: Una Metodología para la formulación de políticas de seguridad organizacional y control de activos contribuirá a una efectiva y eficaz gestión de la información.

Material y métodos: Análisis de literatura, estándares y normas de seguridad de la información. Estudio de los principales procesos que manejan la información en la Universidad Nacional Pedro Ruiz Gallo. Se elaboró un marco de trabajo teniendo como base la seguridad organizacional y el control de activos; además de una metodología que sustente el marco propuesto.

Resultados: Se desarrolló un esquema de trabajo, conformado por seis pasos, que permitió poner énfasis en el análisis gap, control interno y gestión de riesgos.

Conclusiones: La correcta implementación de políticas de seguridad organizacional y control de activos repercute directamente en una efectiva gestión de la información. El resultado de este trabajo nos permite cumplir con los estándares que han sido impuestos por la Oficina Nacional de Gobierno Electrónico e Informático (ONGEI).

Palabras clave: Seguridad organizacional, control de activos, políticas de seguridad.

[1] Ingeniera de Sistemas, estudiante de Posgrado en Gerencia en Tecnologías de Información y Comunicaciones de la UPAO.

[2] Ingeniero de Sistemas, estudiante de Posgrado en Gerencia en Tecnologías de Información y Comunicaciones de la UPAO.

ABSTRACT

Introduction: In an organization there is information that is valuable and often it is not known how important this is, for this reason you lose efficiency and effectiveness in managing this. But in order to achieve better search this scenario is correct primary organizational security and effective control of assets, as both are the pillars on the solution being sought.

Objective: Provide a methodology to implement organizational security policies and control of assets as the Peruvian Technical Standard NTP-ISO/IEC 17799 in UNPRG.

Material and methods: Analysis of literature, standards and information security. Study of the main processes that handle data at the Universidad Nacional Pedro Ruiz Gallo. Developed a framework on the basis of organizational security and control of assets, and a methodology that supports the proposed framework.

Results: To test the methodology was developed scheme of work consists of six steps, which allowed us to emphasize the gap analysis, internal control and risk management.

Conclusions: Successful implementation of organizational security policies and control of assets has a direct impact on effective information management. The result of this work allows us to meet the standards that have been imposed by the National Office of Electronic Government and Information Technology.

Key words: Organizational security, asset control, security policies.

INTRODUCCIÓN

La estructura organizacional del área informática y el control de activos de tecnología de información, son parte fundamental es dentro del correcto desenvolvimiento de una organización, pero llevarla a cabo es un procedimiento relativamente nuevo en nuestro país. La Oficina Nacional de Gobierno Electrónico e Informática - ONGEI, ha considerado necesario tomar las medidas pertinentes para administrar apropiadamente las áreas de tecnología de información dentro de las entidades estatales.

En la Universidad Nacional Pedro Ruiz Gallo (U.N.P.R.G.), la dirección y gestión de tecnologías de información no se realizan, teniendo en cuenta un código de buenas prácticas que le permitan asegurar los principios fundamentales y básicos de la información, y por ende no cuenta con una metodología que le permita la implementación del sistema de administración y gestión de la seguridad de la información (plasmado en el Plan de Seguridad de la Información) como lo establece la Norma Técnica Peruana NTP-ISO/IEC 17799 en sus buenas prácticas, careciendo de esta manera con políticas de seguridad organizacional y control de sus activos.

Por ello, el presente artículo ayudará a mostrar la formulación de los lineamientos generales para una adecuada estructura organizacional y un efectivo tratamiento de los riesgos inmersos en un activo de tecnología de información, identificando sus posibles amenazas y vulnerabilidades.

MATERIAL Y MÉTODOS

Se realizó un estudio, dividido en 3 fases; cada una estuvo relacionado puntos específicos desarrollados:

- **Análisis:** se realizó el estudio de la literatura relacionada directamente con la U.N.P.R.G. como es: Plan Estratégico, Plan de seguridad, Plan de Tecnologías de Información, manuales de procedimientos, entre otros. Además se analizaron las diferentes normas y estándares: NTP ISO/IEC 17799 - 2007, COSO, COBIT, NTP ISO/IEC 12207, CMMI (Figura 1).
- **Procedimental:** Para complementar la fase anterior, se realizaron: encuestas y entrevistas al personal relacionado directamente con la seguridad de la información dentro de la U.N.P.R.G. Además, se realizó un trabajo de observación directa para poder corroborar la forma de cómo se llevaban a cabo los diferentes procesos de seguridad de la información.
- **Experimental:** Esta fase se caracterizó por la aplicación de estándares que fueron estudiados en la fase de análisis; también se realizó

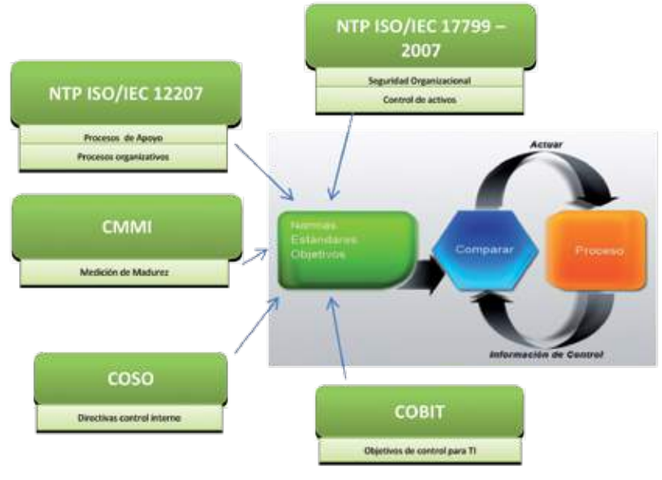

Figura 1. Normas y estándares tomados en cuenta en la investigación

la selección de las mejores prácticas de seguridad relacionadas directamente con la seguridad organizacional y el control de activos. Se logró el establecimiento de la metodología en base a la selección de las mejores prácticas.

RESULTADOS

Para la presente investigación se propone una metodología de implementación; llamada MISOYCA; que permite la eficiente gestión de la información tomando como referencia la seguridad organizacional y el control de activos; esta metodología se planteó teniendo en cuenta los siguientes pasos:

1. ENTENDIMIENTO DE LOS REQUERIMIENTOS.

Taller estratégico con la gerencia para analizar requerimientos de la NTP ISO/IEC 17799 - 2007.

2. DETERMINACIÓN DE LA BRECHA.

- Efectuar análisis GAP.
- Determinar la brecha y estimar el presupuesto y cronograma.

3. ANÁLISIS Y EVALUACIÓN.

- Efectuar un análisis y evaluación de riesgos.
- Definir la política de seguridad.
- Definir el plan de continuidad del negocio.
- Seleccionar controles y Objetivos de control a implantar.
- Elaborar un anunciado de aplicabilidad.

4. DESARROLLO DE COMPETENCIAS ORGANIZACIONALES.

- Entrenamiento en documentación de procedimientos, instrucciones de trabajo.

5. REDACCIÓN DEL MANUAL DE SEGURIDAD DE LA INFORMACIÓN.

- Elaboración del manual de seguridad de información.

6. AUDITARSE INTERNAMENTE.

- Efectuar auditoria interna.Se puede observar en la figura 2 los pasos de la metodología MISOYCA.

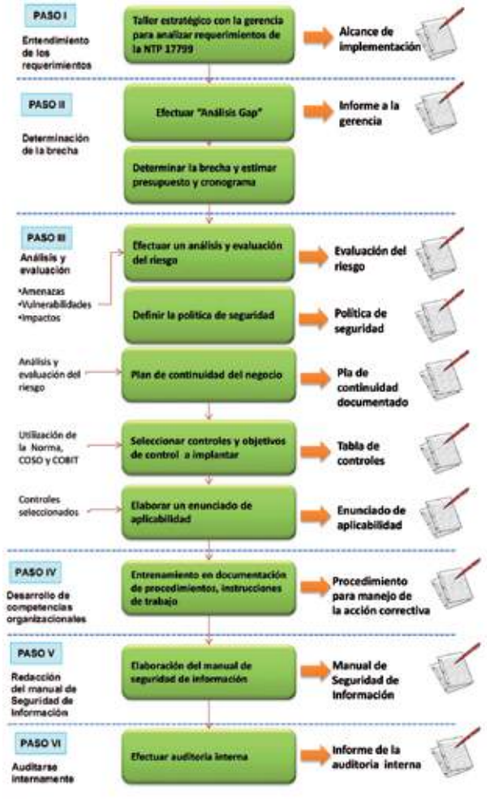

Figura 2. Pasos de la Metodología MISOYCA

DISCUSIÓN

La presente investigación nos permitió estudiar elementos y pilares muy importantes dentro de la Universidad Nacional Pedro Ruiz Gallo; dentro de los cuales podemos mencionar: Planeación Estratégica, Funciones de la Actividad Informática, Dirección, Estructura Organizacional, Administración de Factor Humano, Administración del Recurso Informático, Controles Informáticos, Estándares de Sistemas y Documentación de Sistemas; se logró detectar que existe una **DEFICIENCIA TOTAL y la INEXISTENCIA DE MANUALES** que aseguren la correcta implantación de la seguridad dentro de la universidad; por ende la información que se maneja en el interior de la universidad no se encuentra protegida y mucho menos podemos afirmar que esta se gestione de manera eficaz; lo que se pudo lograr en la presente investigación es cumplir con la elaboración de una metodología que permita implantar una correcta seguridad organizacional y un correcto control de activos; pilares fundamentales según las normativas y estándares para asegurar una efectiva gestión de la información; además permite cumplir con las directivas emitidas por la ONGEI en lo que respecta a la implantación de seguridad de la información dentro de las entidades estatales.

CONCLUSIONES

La presente investigación nos permitió obtener, a través de los requerimientos, la determinación de la brecha y el análisis y evaluación, un diagnostico general de la situación real de la organización y de esta manera poder elaborar procedimientos adecuados de solución.

La metodología MISOYCA fue elaborada tomando como base un conjunto de normas y estándares aceptados internacionalmente.

La correcta implementación de políticas de seguridad organizacional y control de activos, en base a estándares y normas nacionales e internacionales, repercute directamente en una Efectiva gestión de la información.

El resultado de este trabajo nos permitió elaborar documentos que nos facilitan el cumplimiento con los estándares que han sido impuestos por la ONGEI.

BIBLIOGRAFÍA

12207, C. N. (2008). Norma Técnica Peruana – ISO/IEC 12207. Lima: Ediciones ONGEI.

17799, C. N. (2008). Norma Técnica Peruana – ISO/IEC 17799. Lima: Ediciones ONGEI.

BROOKING, A. (2008). El capital intelectual: el principal activo de las empresas del tercer milenio. Barcelona: Paidos empresa.

CASTILLO MAZA, J. (2009). ISO 17799: Gestión de Seguridad de los sistemas de información. Lima: MP ediciones.

CISA. (2007). Preparación al Examen CISA. Madrid: Ediciones CISA.

CMMI. (2008). Guide lines for process integration and product improvement. New York: M.B. Chrissis.

COBIT. (2008). Manual del Estándar COBIT. Ginebra: Ediciones COBIT.

COSO. (2008). Internal Control Integrated Framework. New York: Ediciones COSO.

FREMONT, E. K., & ROSENZWEIG, J. E. (2009). Administración en las organizaciones. Enfoque de Sistemas y de contingencias. México: Mc Graw Hill.

HUERTA, A. V. (2008). Gestión de la seguridad de la información: UNE 71502, ISO 17799. España: Valencia.

INEI. (27 de Noviembre de 2007). INEI. Recuperado el 1 de Febrero de 2011, de INEI: www.inei.gob.pe/web/metodologias/attach/lib614/cap03.htm

M.B.CHRISSIS, M. S. (2008). CMMI, Guidelines for Process Integration and Product Improvement. New York: Ediciones CMMI.

PIATTINI, M. G. (2009). Auditoria Informática – Un Enfoque Practico. Mexico: Mc Graw Hill.

PINILLA, J. D. (2008). Auditoria Informática – Aplicaciones en Producción. Argentina: Ediciones Alfa & Omega.

SEDISI. (2009). Guía de Seguridad Informática. Madrid: SEDISI.