DESARROLLO DE UN MODELO DE SEGURIDAD INFORMÁTICA

DEVELOPMENT OF A MODEL OF COMPUTER SECURITY

Nilo Fernández A., Henry Maquera Q. y Richard Mercado R.
Facultad de Ingeniería de Sistemas, Universidad Nacional del Centro del Perú, Perú.

RESUMEN

Actualmente las amenazas y ataques se han vuelto más comunes y de mayor complejidad, la inexistencia de los esquemas de seguridad informática en las organizaciones, la falta de cultura informática y otros factores son las causas de que se deben tomar en cuenta para contar con un modelo de seguridad informática. La seguridad informática busca dar apoyo a los objetivos y misión de las organizaciones, a través de la protección de sus principales recursos y activos que son: la información, la tecnología que la soporta (software y hardware) y las personas que la utilizan o conocen a través de la selección y aplicación de protecciones adecuadas, manteniendo así el debido cuidado de sus recursos físicos, financieros, reputación y otros activos tangibles e intangibles. El trabajo de investigación permite el DESARROLLO DE UN MODELO DE SEGURIDAD INFORMÁTICA. La UNCP como organización posee una serie de elementos a nivel de informática que apoyan a la Gestión Académica así como a sus procesos, los cuáles requieren de seguridad en varios niveles y según sus características para ello se hace una evaluación de los activos con los que se cuentan con sus respectivos riesgos, amenazas y vulnerabilidades y estableciendo la seguridad para cada uno de ellos, teniendo como base las necesidades y actualidad existentes en seguridad. Se implementa un modelo de seguridad que consta de medidas de seguridad implementados con software basados en GNU/LINUX haciendo de está manera la implementación del modelo basada en software libre y mejorando la seguridad de la información.

Palabras clave: Seguridad informática, activos, riesgos, amenazas, vulnerabilidades, medidas de seguridad

ABSTRACT

Today, the threats and attacks have become more common and more complex, the lack of computer security schemes in organizations, lack of computer literacy and other factors causes to be taken into account to have a model computer security. Computer security seeks to support the goals and mission of the organizations, through the protection of resources and its main assets are the information technology that supports it (software and hardware) and people who use or know through the selection and application of appropriate safeguards, thus maintaining proper care of their physical, financial, reputational and other tangible and intangible assets. The research enables the development of a security model COMPUTERS. The UNCP as an organization has a number of computer-level elements that support the Academic Management and its processes, which require security at various levels according to their characteristics and for this it is an assessment of the assets that have their respective risks, threats and vulnerabilities and establishing security for each, based on currently existing needs and safety. It implements a security model that consists of security measures implemented with software based on GNU / LINUX thus making the implementation of the model based on free software and improving information security.

Key words: Computer science security, assets, risks, threats, vulnerabilities, safety measures

INTRODUCCIÓN

Una característica importante en las organizaciones actuales es mejorar el nivel de seguridad de la información que manejan por lo tanto toda organización hace uso de elementos como hardware, software y personas que son los activos

de la información. Una característica deseable es contar con un modelo de seguridad informática para lograr la seguridad de la información. Por lo que planteamos la siguiente hipótesis:

Los elementos que ayudan a diseñar un modelo de seguridad de la información en la gestión académica de la Universidad Nacional del Centro del Perú son el análisis de riesgos y los controles de seguridad.

El análisis de riesgos nos permitirá detectar las amenazas a los que están sometidos los activos de la gestión académica de la UNCP.

La implementación de controles nos permitirá mejorar el nivel de seguridad de la información de la gestión académica en la UNCP.

Por lo tanto los objetivos que buscamos en el presente trabajo son:

Implementar un modelo de seguridad informática para proteger la información de la gestión académica en la Universidad Nacional del Centro del Perú.

Detectar las amenazas a los que son sometidos los activos de la gestión académica de la UNCP.

Adoptar controles que mejoren el nivel de seguridad informática en la gestión académica de la UNCP.

MATERIAL Y MÉTODOS

El lugar donde se desarrollo el trabajo fue la Universidad Nacional del Centro del Perú, específicamente el área de la gestión académica y su manejo informático.

Se realizo un análisis de los activos a través de visitas de identificación y su respectivo análisis de riesgos para cada activo encontrado, para poder determinar el nivel de seguridad en términos cuantitativos se estableció los niveles de seguridad de A hasta D asignándose un valor numérico para cada requerimiento haciendo uso de un listado de activos.

El nivel de investigación es aplicado y se uso un método comparativo. Debido a que se estableció las medidas de seguridad para cada requerimiento de seguridad encontrado y su implementación basada en diferentes aplicaciones software utilizadas todas en licencia libre y haciendo uso de equipos de computo.

De está manera se volvió a hacer el análisis de nivel de seguridad considerando ya las medidas implementadas y su nuevo valor resultante en el requerimiento de seguridad, para poder demostrar la hipótesis.

RESULTADOS

Teniendo en cuenta el modelo de seguridad y las medidas implementadas en cada etapa del modelo se muestra a continuación el resumen de los requerimientos y las medidas adoptadas para cada uno.

REQUERIMIENTOS DE SEGURIDAD	Controles adoptados
Establecer políticas para la contratación y funciones del personal.	Asignación de responsabilidades y funciones considerando la seguridad, Selección y política de personal
Restringir el acceso a los datos	gestión de usuarios y privilegios
Asignar al personal un sistema de identificación único para ser validado	gestión de usuarios y contraseñas
Controlar el acceso a datos	Eliminación de usuarios predeterminados en la BD, validación de datos
Controlar el acceso a nivel Intranet e Internet.	Control a través de IP, Firewall, Sistema de detección de Intrusos, control de sesiones y Certificados Digitales
Encriptación de datos	Encriptación de contraseñas y Transmisión segura con TLS
Encriptar datos a nivel de redes	Encriptación para conexión a nivel de intranet e internet de usuarios, certificados digitales para identificación y transmisión.
Proteger datos y sistemas de software malicioso	Copias de respaldo, Instalación de Antivirus y monitoreo del sistema
Mantener al día los parches de software	Instalación y configuración del servidor, Actualizaciones automáticas, tener información actualizada de vulnerabilidades
Mantener niveles de privilegios de usuarios.	Registro y gestión de privilegios,
Restringir el acceso físico a los equipos.	Perímetro de seguridad, protección contra amenazas externas, mantenimiento de equipos y retiro de propiedad

Finalmente tenemos la comparación de los niveles de seguridad por requerimiento establecido y su respectivo valor inicial y final.

DISCUSIÓN

Teniendo en cuenta las medidas adoptadas e implementadas de seguridad y el resultado obtenido con un valor cuantitativo del resultado del nivel de seguridad, y que dentro de las hipótesis planteadas se considera que el análisis de riesgos nos permitirá detectar las amenazas a los que están sometidos los activos de la gestión académica de la UNCP, el cual hemos podido resumir, los activos y los criterios para aceptar un riesgo y tomar la medida de acción posterior, además se plantea los controles a implementar y las recomendaciones de control para los riesgos habiendo cumplido con ello se aprecia que realmente esta hipótesis es válida.

Teniendo en cuenta la hipótesis acerca de que la implementación de controles nos permitirán mejorar el nivel de seguridad de la información de la gestión académica en la UNCP, está se muestra cómo un listado de los Requerimientos y sus medidas de acción y también los requerimientos y su nuevo valor asignado alcanzado después de haber implementado las acciones correspondientes en la que se muestra que el nivel de seguridad es de 49 frente a 25 que se tenía inicialmente por lo que se aclara que la hipótesis es válida.

CONCLUSIONES

1. Para el diseño del modelo de seguridad informática se realizó el análisis de riesgos que nos ha permitido detectar las amenazas a los que son sometidos los activos de la información y los requerimientos de seguridad que se presentaron, han permitido delimitar el ámbito del modelo y su estructura en áreas, exclusivamente en la gestión académica de la UNCP.
2. El modelo de seguridad propuesto consta de varias áreas en las que se han logrado implementar controles de seguridad para cada uno. De está manera se logro la implementación y mejora del nivel de seguridad que es medido a través de la asignación de valores, obteniéndose un valor inicial de 25 y final de 45.
3. Para el desarrollo del modelo de seguridad informática se tuvo en cuenta la Norma Técnica Peruana y las recomendaciones de la ISO 17799 además, se realizó la evaluación económica del mismo el cuál ha sido tomado como referencia para considerar que el proyecto de seguridad es económicamente factible.
4. Las áreas involucradas en el modelo de seguridad han requerido la implementación de controles de seguridad que requieren monitoreo, revisión y mantenimiento de los mismos, convirtiéndose de está manera la seguridad en un proceso más de la gestión académica de la UNCP.

AGRADECIMIENTOS

A todos las personas que colaboraron con el presente trabajo involucrándose en los diversos aspectos de seguridad.

REFERENCIA BIBLIOGRÁFICA

1. **Barrios Joel.** Implementación de servidores con GNU/Linux. Alcance Libre. Mexico, 2007
2. **Borghello, Cristian.** Seguridad Informática. Universidad Tecnológica Nacional. Argentina, 2002.
3. **Borghello, Cristian.** Seguridad de la Información.10-09-2008 URL: http://www.segu-info.com.ar/ .
4. **Instituto Nacional de Estadística e Informática.** Guía práctica para el desarrollo de planes de contingencia de Sistemas de Información Edit.: Taller grafico del INEI. Perú, 2001.
5. **Instituto Nacional de Estadística e Informática.** Delitos Informáticos Edit.: Taller grafico del INEI. Perú. 2001
6. **Microsoft Technet.** Academia Latinoamericana de Seguridad Informática. Módulos Electrónicos. 2006.