Revista Ciencia & Desarrollo 2015; 20: 91-97 / ISSN 2304-8891

DISEÑO DE SEGURIDAD PARA SALVAGUARDAR ACTIVOS DE INFORMACIÓN EN EL CAMPUS DE LA UNCP *

SAFETY DESIGN TO SAFEGUARD THE ASSETS OF INFORMATION ON CAMPUS UNCP

[1] Henry George Maquera Quispe

RESUMEN

La falta de controles de seguridad en la Universidad Nacional del Centro del Perú ha ocasionado que dispositivos, software y servicios de TI no generen valor a la organización. La norma de calidad – ISO 9001, gestión de servicios de tecnologías de información – ITIL, metodología Magerit v3 y la norma ISO 27002 permitieron iniciar el diseño de seguridad mediante el análisis los procesos de TI, gestión de activos de información, servicios de TI involucrados en la Oficina General de Informática. La metodología Magerit v3 estableció la clasificación, valoración y dependencia de los activos de información. El análisis de amenazas, salvaguardas, impactos y riesgos por categoría de activos fundamentaron las directivas de seguridad que salvaguardaron activos de información. La prueba de U de Mann – Whitney permitió determinar que los niveles de indicadores en las variables de estudio eran diferentes en sus etapas de pre y pos evaluación. Al aplicar la prueba X2 se observó un valor – p o significación asintótica que tiende a $p<0.0001$, lo que indica que existe diferencia significativa entre las muestras de los grupos bajo estudio y se concluye que se rechaza la hipótesis nula y se acepta la hipótesis general.

Palabras clave: activo de información, amenaza, riesgo, servicio, vulnerabilidad.

ABSTRACT

The lack of security controls at the National University of Central Peru has caused devices, software and IT services do not generate value to the organization. The quality standard - ISO 9001, management of information technology services - ITIL v3 methodology Magerit and ISO 27002 allowed start designing security by analyzing IT processes, management of information assets, IT services involved the General Office Computing. The established methodology Magerit v3 classification, valuation and reliance on information assets. Threat analysis, safeguards, impacts and risks for each category of assets substantiated security policies that safeguarded information assets. The test of Mann - Whitney allowed to determine the levels of indicators in the study variables were different in their pre and post evaluation. By applying the value X2 test it was observed – p or asymptotic significance tends $p<0.0001$, indicating that there are significant differences between samples of the groups under study and conclude that the null hypothesis is rejected and the general hypothesis is accepted.

Keywords: information asset, threat, risk, service vulnerability.

INTRODUCCIÓN

La creciente demanda de información exige a las organizaciones soluciones en la administración de servicios de tecnologías de información bajo niveles de calidad, continuidad de servicios y seguridad. Los servicios de tecnologías de información proporcionados por la Oficina General de Informática a través de la red de datos no se encuentran basadas bajo la gestión de servicios de tecnología de información, ello generó el desarrollo de soluciones carentes de planeamiento estratégico que permitan su sostenibilidad, y calidad de servicio a diferentes usuarios de la red de datos. Un análisis previo determinó que existen muchos tipos de incidentes los cuales se muestran en la figura 1. Se aprecia un incidente denominado *Mal uso de Servicios de TI*, este tipo de incidentes se puede subdividir en otros que ayuden a proporcionar un mejor análisis de las amenazas, vulnerabilidades y riesgos que deben ser controlados.

Mediante la clasificación de eventos, la figura 2 muestra sub tipos de eventos relacionados al incidente *Mal uso de*

[1] Magister en Ingeniería de Sistemas: Mención en Ciencias de la Computación e Informática. Docente de la Facultad de Ingeniería de Sistemas. Universidad Nacional del Centro del Perú. Huancayo-Perú.

* Artículo científico de la Tesis Doctoral "Diseño de seguridad de redes para salvaguardar activos de información en el campus de la UNCP mediante la gestión de servicios basada en ITIL.

Figura 1. Incidentes de Seguridad Identificados
Fuente: Bitácora de incidentes – Oficina General de Informática

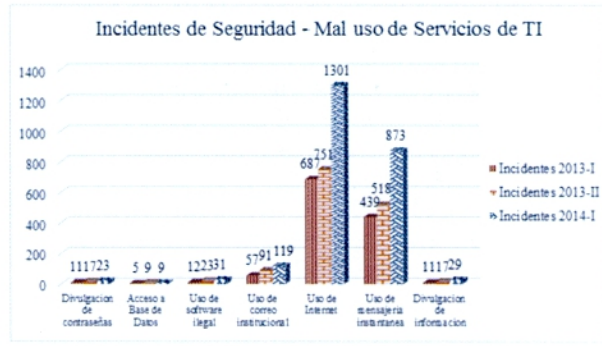

Figura 2. Sub tipos de incidentes al mal uso de Servicios de TI
Fuente: Bitácora de incidentes – Oficina General de Informática

Servicios de TI. Este análisis determino que durante el semestre 2013-I se han suscitado 1222 incidentes, durante el semestre 2013-II se han suscitado 1426 incidentes y durante el semestre 2014-I se han suscitado 2385 incidentes que evidencian que ha existe un incremento en los incidentes de seguridad.

El incremento de incidentes de seguridad mostradas en las figuras 1 y 2 trajeron como consecuencia que la disponibilidad, continuidad e integridad de activos de información se han visto afectados. Al mismo tiempo generó la poca conformidad por parte de los usuarios a los servicios de tecnologías de información proporcionados. Mediante entrevistas al personal de la oficina se identificó que uno de los principales problemas en la administración de recursos de tecnología de información es la carencia de medidas administrativas de seguridad referenciadas en directivas de seguridad que salvaguarden el correcto uso de los recursos de tecnologías de información que tengan directo impacto en actividades académicas y/o administrativas de la Universidad Nacional del Centro del Perú.

La problemática planteada en la investigación es ¿De qué manera el diseño de seguridad de redes influye en la salvaguarda activos de información en el campus de la Universidad Nacional del Centro del Perú?, siendo el objetivo de la investigación determinar el nivel de influencia del diseño de seguridad de redes mediante la formulación de directivas de TI en la salvaguarda de activos de información en el campus de la Universidad Nacional del Centro del Perú" que mediante la aplicación de la metodología Magerit de análisis de riesgos, las buenas prácticas de ITIL 2011 y la norma ISO 27002.

MATERIALES Y MÉTODOS

Gestión de servicio de tecnologías de información

El objetivo principal de Gestión del Servicio es garantizar que los servicios de Tl se alineen con las necesidades del negocio y darles soporte activamente. Es muy importante que los servicios de TI sostengan los procesos de negocio, pero también es cada vez más importante que Tl actúe como un agente para el cambio para facilitar la transformación del negocio.

"Un servicio es un medio de entrego de valor a los clientes facilitando los resultados que los clientes desean lograr sin la responsabilidad sobre los costes y riesgos específicos" (TSO - SD, 2011, p. 13).

"Un proceso es un conjunto de actividades coordinadas que combinan e implementan recursos y capacidades para producir un resultado que, directa o indirectamente, genera valor para un cliente externo o interesa-

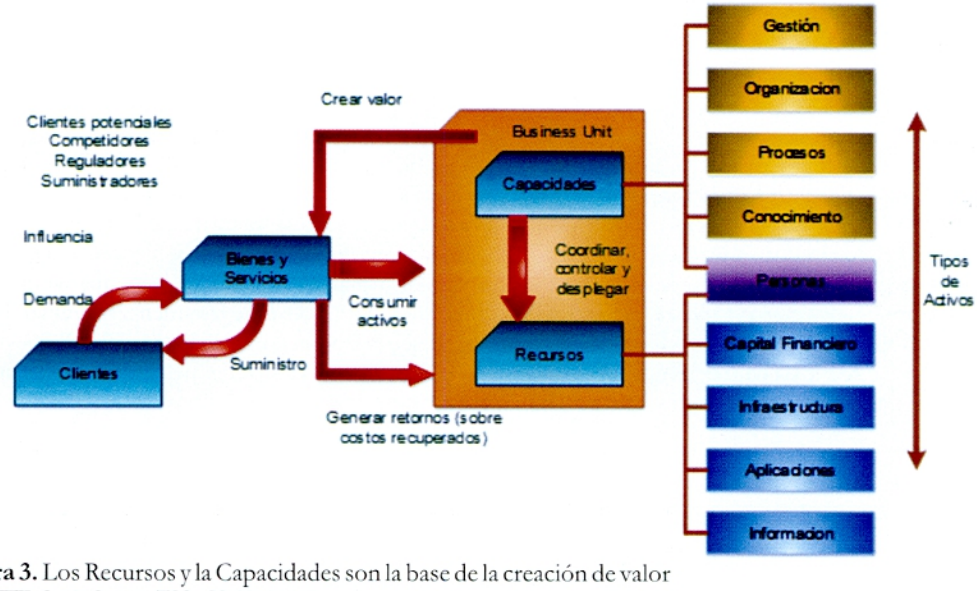

Figura 3. Los Recursos y la Capacidades son la base de la creación de valor
Fuente: ITIL Service Strategy (TSO - SS, 2011, p 40)

do" (TSO - SS, 2011, p.19).

Sistema de gestión de seguridad de la información

Los recursos y capacidades son tipos de activos. Las organizaciones los utilizan para crear valor en forma de bienes y servicios. Los recursos son entradas directas para la producción. La gestión, la organización, las personas y el conocimiento sirven para transformar los recursos. Las capacidades representan la aptitud de una organización para coordinar, controlar y desplegar los recursos para generar valor.

Los objetivos de seguridad: Disponibilidad, Integridad, Confidencialidad, y la terminología utilizada en la industria de la seguridad: Vulnerabilidades, Amenazas, Riesgos, Control son componentes fundamentales que deben ser entendidos si la seguridad se va a tener lugar de una manera organizada.

Evaluación de riesgos y análisis

"Una evaluación de riesgos es una herramienta para la gestión de riesgos, es un método de identificación de vulnerabilidades y amenazas y la evaluación de los posibles impactos para determinar dónde aplicar los controles de seguridad" (Harris, 2013, p. 74).

Política de seguridad

"Una política de seguridad es una declaración general de conjunto producida por la alta dirección (o un tablero de la política seleccionada o comité) que dicta el rol que juega la seguridad dentro de la organización" (Harris, 2013, p. 102).

Población y muestra

La población para desarrollo de la tesis está conformada 541 usuarios constituidos entre usuarios (docentes y estudiantes) de la Facultad de Ingeniería de Sistemas de la Universidad Nacional del Centro del Perú. La muestra en el trabajo de investigación es una muestra estratificada debido a las categorías identificadas en la población de estudio donde cada elemento pertenece a un único estrato.

Tabla 1. Muestra por estratos

Categoría	Estrato Ni	Proporción %	Muestra por
Docentes	23	4,250	13
Estudiantes	340	62,847	188
Personal	170	31,423	94
Personal	8	1,479	4

Método de investigación

El método de investigación utilizado es el comparativo que permitió descubrir la correlación entre la información obtenida de las pre-prueba y pos-prueba desarrollada en la investigación mediante la contratación. Se utilizará el método específico de inferencia mediante la inducción – deducción que permite adquirir conocimientos generales a partir de hechos particulares y obtener conocimientos particulares a partir de características generales. Se utilizó el procesamiento estadístico en la información obtenida en las encuestas. Se utilizó la prueba estadística X^2 que permitió la evaluación de hipótesis acerca de la relación entre dos variables de forma que se determine la relación entre las variables independientes: Seguridad de redes (Gestión de servicios, análisis de riesgos) y la variable dependiente salvaguarda de activos de información.

Tabla 2. Relación de activos con los procesos de la Oficina General de Informática.

Activos de Información	Procesos						
	Gestión Estratégica Operativa	Planeamiento de Tecnologías de Información	Gestión de Redes de Datos y Telefonía	Gestión de Aplicaciones e Intranet	Gestión de Soporte Tecnológico	Gestión de Atención a Eventos Académicos, Científicos y Culturales	Gestión de Proyectos y Administración de aplicaciones
[IBD] Información de Base de Datos				X	X		
[SW] Aplicaciones (Software)			X	X	X		
[SC] Servicios de Comunicación			X	X		X	
[HW] Equipos Informáticos – Hardware			X	X	X		
[COM] Redes de Comunicaciones			X				
[AUX] Equipamiento Auxiliar			X				
[L] Instalaciones	X	X	X		X	X	
[P] Personal	X	X	X	X	X	X	X

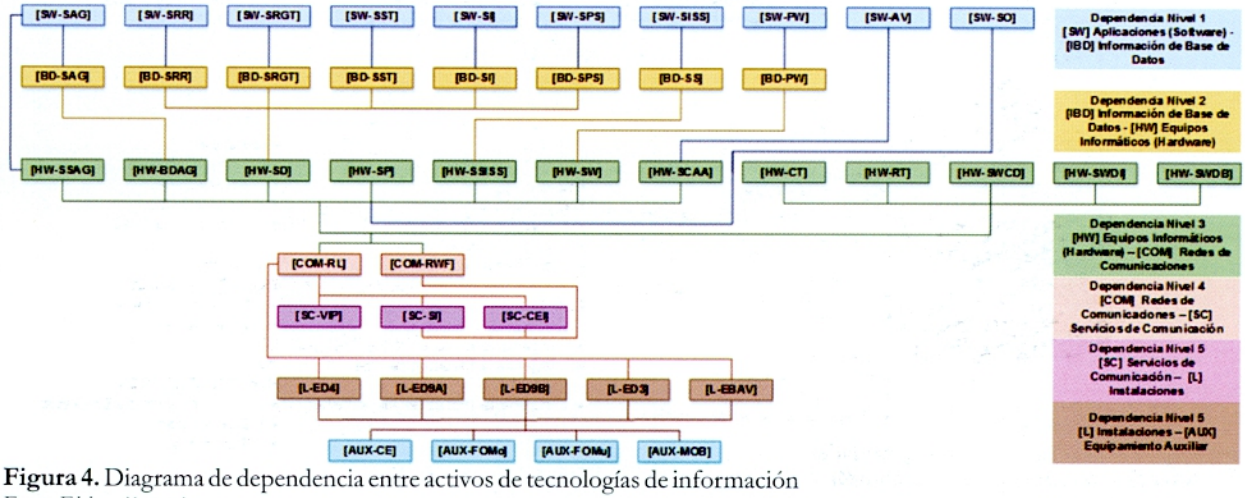

Figura 4. Diagrama de dependencia entre activos de tecnologías de información
Fuente: Elaboración propia

RESULTADOS

La tabla 2 permite observar la relación entre los tipos de activos de información identificados y los procesos establecidos mediante el análisis de las actividades en producción por la Oficina General de Informática. Esta relación permite establecer controles que facilitan la salvaguarda de los tipos de activos identificados.

El análisis de dependencia entre activos mostrada en la figura 4 presenta un modelo que expresa la relación funcional entre los activos de información, esta dependencia es importante a fin de determinar el nivel de valoración de cada activo. Un activo sumamente importante es [P] Personal que interactúa con todos los activos identificados.

Los activos de información son accedidos por usuarios mediante la red de datos de la UNCP por lo que se for-

Tabla 3. Relación de tipos de activos de información, riesgos, impacto y directiva de seguridad para salvaguarda de activos de información.

Activos	Estimación de Impacto	Riesgo	Directiva de Seguridad de TI
[IBD] Información de Base de Datos	MA	MA	Directiva: Normas de seguridad de la información almacenada en los equipos de la UNCP.
[SW] Aplicaciones (Software)	MA	MA	Directiva: Normas que regulan el uso de las tecnologías de información y comunicaciones en el Campus de la UNCP Directiva: Normas que regulan la publicación de información en la página web de la UNCP.
[SC] Servicios de Comunicación	MA	MA	Directiva: Normas para el uso del servicio de internet en la UNCP.
[HW] Equipos Informáticos – Hardware	MA	MA	Directiva: Normas Técnicas para la protección física de los equipos informáticos en el campus de la UNCP.
[COM] Redes de Comunicaciones	MA	MA	Directiva: Normas de seguridad de la información almacenada en los equipos de la UNCP.
[AUX] Equipamiento Auxiliar	A	A	Directiva: Normas de seguridad física para Oficina General de Informática.
[L] Instalaciones	MA	MA	Directiva: Normas de seguridad física para Oficina General de Informática.
[P] Personal	A	A	Directiva: Normas generales de seguridad para situaciones críticas en los ambientes de la Oficina General de Informática.

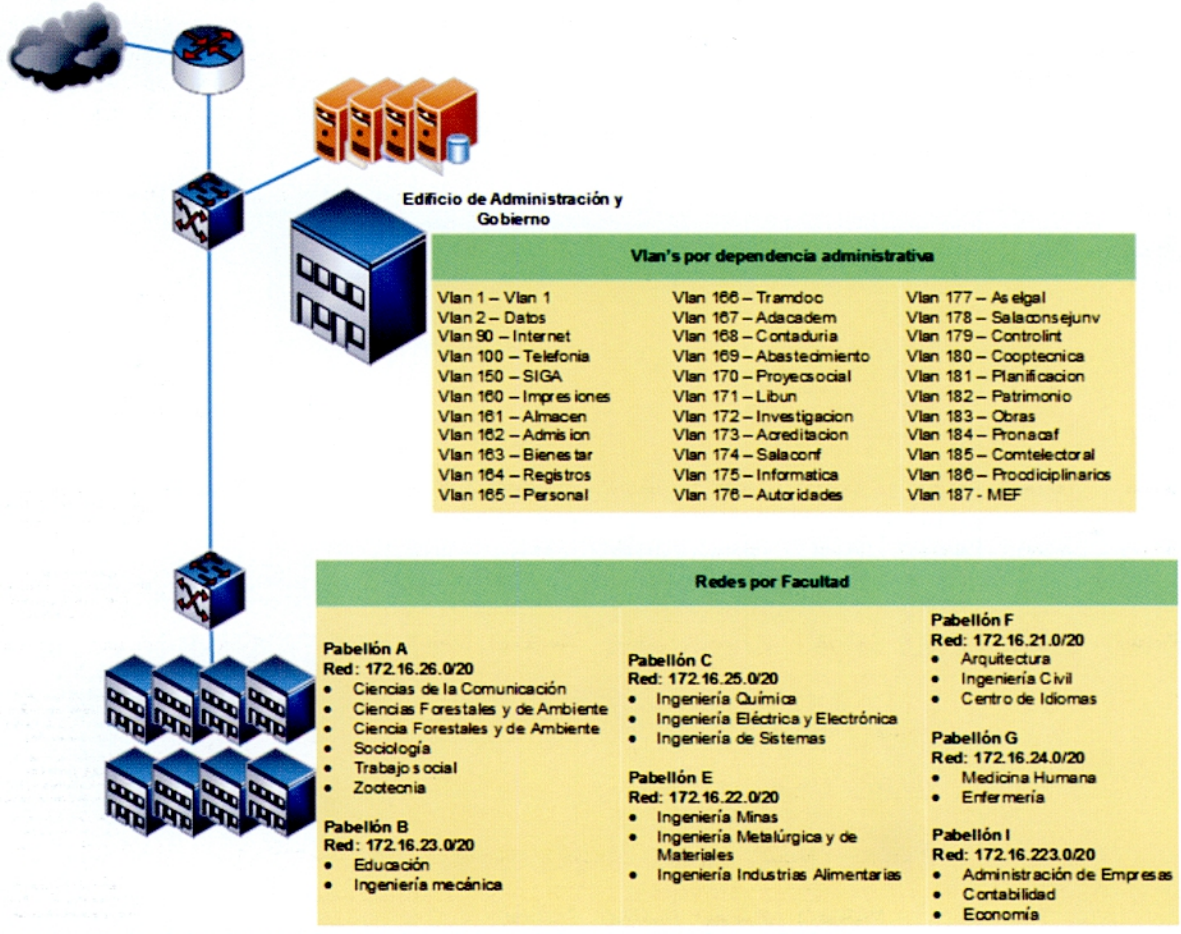

Figura 5. Vlan's y Subredes en el Campus de la Universidad Nacional del Centro del Perú
Fuente: Elaboración Propia

muló la estrategia de segmentación mediante estructuras de Vlan's expresada en la figura 5. Esta estrategia de administración de redes ha permitido tener un orden en la asignación de direcciones lógicas en los diversos dispositivos de red.

La integración de activos, impactos y riesgo permitió formular directivas que permitan la continuidad de los servicios de tecnologías de información proporcionados a través de la red de datos de la UNCP. La tabla 3 resume la relación entre los tipos de activos información y la directiva de seguridad que permite su adecuada salvaguarda.

DISCUSIÓN

La figura 6 muestra los niveles de impacto potencial en relación a la cantidad de amenazas identificadas entre los tipos de activos de información. Se aprecia que el tipo de activo *[SW] Aplicaciones – Software* cuenta con un impacto *Muy Alto* en todos sus activos en caso de enfrentarse a una amenaza, esto indica que es importante diseñar e implementar mecanismos de control a fin de minimizar el riesgo de TI existente.

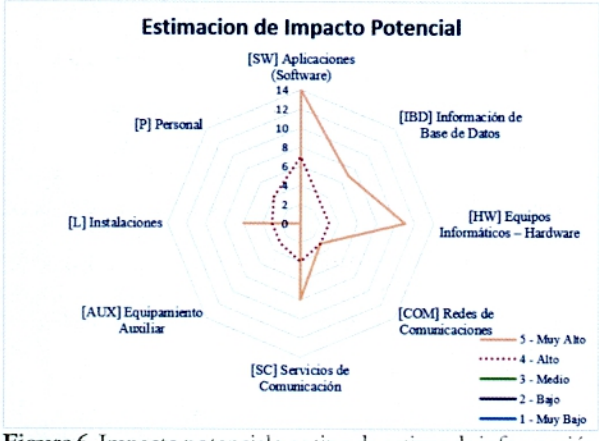

Figura 6. Impacto potencial por tipo de activos de información

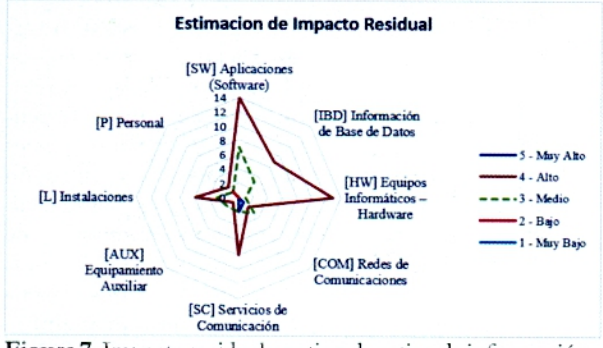

Figura 7. Impacto residual por tipo de activo de información

Los niveles de impacto en las ante las posibles amenazas de TI mostradas en la figura 7 expresa una disminución ante la información mostrada en la figura 6. Este cambio expresa que los impactos se han reducido producto de la ejecución de las directivas de seguridad de TI. Un nivel *Alto* de impacto se comprende como de una naturaleza de riesgo capaz de detener los servicios de TI por lo que se amerita iniciar procesos de implementación de medidas de control en la administración de activos de información.

Los nuevos niveles de riesgo de TI evaluados ante la participación de directivas de seguridad se muestran en la figura 8 y expresan un nivel de riesgos de TI residual. Este cambio expresa que los riegos de TI se han reducido producto de la ejecución de las directivas de seguridad de TI. Un nivel *Alto* de Riesgo de TI se comprende como de naturaleza capaz de detener los servicios de TI por lo que se amerita iniciar procesos de implementación de medidas de control en la administración de activos de información.

Se aplicó la prueba de U de Mann – Whitney a fin de comparar el comportamiento de las muestras entradas. De la prueba se determinó que el valor – p o significación asintótica tiende a $p < 0{,}0001$. Dado que el valor de significancia asintótica no excede el valor de significancia de 0,05 se concluye que el grado de aceptación del nivel de servicio de TI es diferente entre las pre y pos pruebas realizadas.

Se aplicó la prueba estadística X^2 cuadrada para muestras independientes. Se tomó como la primera categoría la muestra encontrada en la Pre prueba y como segunda categoría la muestra encontrada en la Pos prueba a fin de determinar si existe relación entre la gestión de servicios categori-

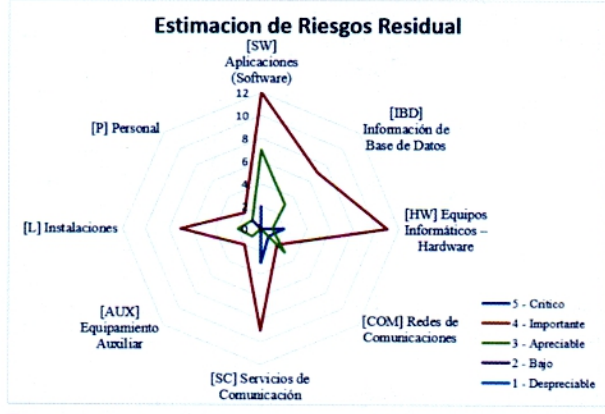

Figura 8. Riesgo residual de TI por tipo de activo de información

Estadísticos de prueba[a]

	Aceptación - Niveles de servicio de TI	Aceptación - Continuidad de servicios de TI	Aceptación - Disponibilidad de activos de TI	Aceptación - Integridad de los activos de TI	Aceptación - Confidencialidad de activos de TI
U de Mann-Whitney	15722,500	12847,000	15260,000	13597,500	16159,500
W de Wilcoxon	60572,500	57697,000	60110,000	58447,500	61009,500
Z	-14,616	-15,967	-14,886	-15,706	-14,447
Sig. asintótica (bilateral)	,000	,000	,000	,000	,000

a. Variable de agrupación: Prueba Desarrollada

Figura 9. Prueba de U de Mann – Whitney
Fuente: Software SPSS

Tabla cruzada

			Aceptación - Niveles de servicio de TI					
			Muy Bajo	Bajo	Medio	Alto	Muy Alto	Total
Prueba Desarrollada	Pre Prueba	Recuento	203	86	10	0	0	299
		Recuento esperado	123.0	108.0	39.0	17.0	12.0	299.0
	Pos Prueba	Recuento	43	130	68	34	24	299
		Recuento esperado	123.0	108.0	39.0	17.0	12.0	299.0
Total		Recuento	246	216	78	34	24	598
		Recuento esperado	246.0	216.0	78.0	34.0	24.0	598.0

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	214.156[a]	4	.000
Razón de verosimilitud	250.850	4	.000
Asociación lineal por lineal	189.642	1	.000
N de casos válidos	598		

a. 0 casillas (0.0%) han esperado un recuento menor que 5. El recuento mínimo esperado es 12.00.

Figura 10. Prueba X^2 cuadrada
Fuente: Software SPSS

zado y el diseño de seguridad de redes para salvaguardar los activos de información a través del indicadores de esta variable.En la evaluación se observa que valor – p o significación asintótica tiende a p<0.0001, lo que indica que existe diferencia significativa entre las muestras de los grupos bajo estudio y se concluye se rechaza la hipótesis nula y se acepta la hipótesis:

El diseño de seguridad de redes mediante la formulación de directivas de seguridad de TI basada en el análisis de riesgos y gestión de servicios de tecnología de información permitirá salvaguardar de manera positiva y significativa los activos de información en el campus de la Universidad Nacional del Centro del Perú.

La gestión de servicios de TI permite establecer y compartir procesos de gestión en TI en la organización. Esta apreciación se comparte con la tesis *Improving IT Service Management using an Ontology-based and Model-driven approach* publicada por la Dra. María Valiente mediante la cual se aplica modelos formales establecidos por ITIL con el fin de construir modelos de gestión de servicios mediante la administración de activos de tecnologías de información. Sin embargo la tesis publicada por la Dra. María Valiente no ha incorporado una etapa de análisis de procesos de TI y un análisis de riesgos de TI que le permitan desarrollar una solución integrada sostenible basada en la demanda de servicios.

Los controles formulados a través de las directivas de seguridad de TI establecidos en la sección *Políticas de seguridad* brindan una alternativa de control en relación del análisis de riesgos de TI de los activos de información establecidos por la metodología Magerit. La tesis *Nueva propuesta evolutiva para el agrupamiento de documentos en sistemas de recuperación de información* publicada por el Dr. Jose Luis Castillo Sequera propone un estudio de sistemas de recuperación basado en un sistema evolutivo basado en el círculo de mejora continua sustentado en forma indirecta en la norma ISO 9001. Dr. Jose Luis Castillo Sequera aplica técnicas evolutivas similares a las aplicadas en la presente investigación que garantizan un sistema de información sostenible y de rápida adaptación ante los cambios en la demanda de servicios en los usuarios del campus de la Universidad Nacional del Centro del Perú.

CONCLUSIONES

1. La gestión de servicios de tecnologías de información se integra en la gestión por procesos mediante el análisis del modelo de procesos de la Oficina General de Informática que mediante el desarrollo de un modelo de procesos logró establecer una propuesta organizada y estructurada de las actividades asignadas a esta dependencia basada en los reglamentos actualmente vigentes que han servido como punto inicial en la identificación de servicios de TI con el objetivo de controlar los activos de información. Por lo tanto la identificación de servicios de TI tiene un nivel significativo y alto en la salvaguarda de activos de información probada con una prueba estadística X^2 cuadrada con un valor – p<0,0001.
2. El análisis de riesgo basada en la metodología Magerit permite valorar activos y riesgos de mediante escalas estándares que orientan el criterio del investigador en las actividades desarrolladas con la asistencia del personal de la Oficina General de informática en el objetivo de formular estrategias de solución. Por lo tanto el análisis de riesgos de TI tienen un nivel significativo y alto en la salvaguarda de activos de información probada con una prueba estadística X^2 cuadrada con un valor – p < 0,0001.
3. Las directivas de seguridad de TI formuladas para su ejecución en el control de activos son una importante

actividad que regula la implementación de estrategias técnicas. Las estrategias de seguridad son percibidas por el usuario mediante niveles de servicio, niveles seguridad y percepción de incidentes que permite determinar el grado de impacto del diseño de seguridad en la salvaguarda de activos de información. Por lo tanto la evaluación de las estrategias de seguridad basada en la gestión de servicios de tecnologías de información – ITIL, la metodología Magerit y la norma ISO 27002 deben tener como relación directa a los servicios proporcionados a los usuarios de la Universidad Nacional del Centro del Perú a través de la red de datos.

REFERENCIAS BIBLIOGRÁFICAS

Beltrán, J., Carmona, M. A., Carrasco, R., Rivas, M. A.; Tejedor, F. (2002). *Guía para una Gestión basada en procesos.* Instituto Andaluz de Tecnología. España.

Bon, J. V. (2008). *Fundamentos de la Gestión de Servicios de TI basada en ITIL.* Editorial Van Haren Publishing. Inglaterra

Castellanos. (2008). *Retos y nuevos enfoques en la gestión de la tecnología y del conocimiento.* Universidad Nacional de Colombia. Colombia.

Castillo, J. L. (2010). Nueva propuesta evolutiva para el agrupamiento de documentos en sistemas de recuperación de información. (Tesis Doctoral). Universidad de Alcalá. España.

Fernandez, M. B. (2013). Evaluation Methodologies for Security Testing of Biometric Systems beyond Technological Evaluation. (Tesis Doctoral). Universidad Carlos III de Madrid. España.

Harris, S. (2013). CISSP. Editorial Mc Graw Hill. (Sexta Edición). Estados Unidos.

ISO. (2005). Norma Internacional ISO 9000 – Sistemas de gestión de la calidad – Fundamentos y vocabulario. ISO Copyright. Suiza.

ISO. (2005). Norma Internacional ISO 20000 – Information Technology – Service Management. ISO Copyright. Suiza.

ISO. (2008). Norma Internacional ISO 9001 – Sistemas de gestión de la calidad – Requisitos. ISO Copyright. Suiza.

ISO. (2005). Norma Internacional ISO 27001 – Tecnologías de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos. ISO Copyright. Suiza.

ISO. (2013). Norma Internacional ISO 27002 – Tecnologías de la Información – Técnicas de seguridad – Código de prácticas para controles de seguridad de información. ISO Copyright. Suiza.

TSO - SS. (2011). ITIL Service Strategy. Editorial TSO. Inglaterra.

TSO - SD. (2011). ITIL Service Design. Editorial TSO. Inglaterra.

TSO - ST. (2011). ITIL Service Transition. Editorial TSO. Inglaterra.

TSO - SO. (2011). ITIL Service Operation. Editorial TSO. Inglaterra.

TSO - CSI. (2011). ITIL Continual Service Improvement. Editorial TSO. Inglaterra.

UNCP – MOF. (2010). Manual de Organización y Funciones (MOF). Universidad Nacional del Centro del Perú. Perú.

UNCP – ROF. (2010). Reglamento de Organización y Funciones (ROF). Universidad Nacional del Centro del Perú. Perú.

Valiente, M. C. (2011). Improving IT Service Management using an Ontology-based and Model-driven approach. (Tesis Doctoral) Universidad de Alcala. España.

Correspondencia:
Henry George Maquera Quispe: henry.maquera@gmail.com

Fecha de Recepción: 05/09/2015
Fecha de Aceptación: 20/11/2015