EVALUACIÓN TÉCNICA DE LA SEGURIDAD INFORMÁTICA DEL DATACENTER DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO

Patricio Moscoso Montalvo[1], *Ricardo Guagalango Vega*[2], *Walter Fuertes D*[3].,*Romel Aldás*[4]

1 Escuela Politécnica del Ejército, Ecuador, patricio.moscoso@hotmail.com

2 Escuela Politécnica del Ejército, Ecuador, ricardoguagalango@hotmail.com

3 Escuela Politécnica del Ejército, Ecuador, wfuertesd@espe.edu.ec

4 Escuela Politécnica del Ejército, Ecuador, romel.aldas@gmail.com

RESUMEN

Con el desarrollo exponencial del Internet, hoy en día existen amenazas y vulnerabilidades que atentan contra la seguridad informática de las universidades. El presente artículo se enfoca en el uso de los controles de la Norma ISO 27000, dedicada a especificar requerimientos necesarios para: establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información. En este contexto se ha aplicado la Metodología formal de Análisis y Gestión de Riesgos denominada MAGERIT, que permite recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos. Para automatizar su gestión y tratamiento se ha utilizado PILAR, software que permite el análisis de riesgos en Seguridad Informática, cubriendo los retos de la seguridad como: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información. El tratamiento de los riesgos se lo realiza con salvaguardas, normas y procedimientos de seguridad para obtener el riesgo residual. Los resultados obtenidos muestran una mejora a nivel de seguridad informática, y se reduce el riesgo de la situación actual. Como producto final, se propone obtener un informe ejecutivo, y los lineamientos para el Plan de Seguridad Informático, cara a certificarse en la Norma ISO 27001.

Palabras Clave: Normas ISO: Organización Internacional de Normalización, MAGERIT: Metodología De Análisis y Gestión de Riesgos de los Sistemas de Información, PILAR: Software que utiliza la Metodología MAGERIT y proviene de los pilares de seguridad.

ABSTRACT

With the exponential development of Internet, today there are threats and vulnerabilities that attempt against the technology security of universities. The present article focuses on the use of controls of the Norma ISO 27000, which specifies the necessary requirements to: establish, implant, maintain and improve a Security Management System of Information. In this context the Risk Management and analysis Formal Methodology denominated MAGERIT has been applied, which enables the recommendation of appropriate measures that should be adopted to control these risks. In order too automate its management and treatment the software PILAR has been used, which enables the analysis of risks in technology Informatics Security, covering the security challenges such as: confidentiality, integrity, availability, authenticity and information tracing. The risk treatment is carried out with security safeguards, norms and procedures to obtain the residual risk. The obtained results show an improvement at an informatics level, and the risk of the current situation is reduced. As a final product, there's the proposal of obtaining an executive report, and the lineaments for the Informatics Security Plan, to be certified in the Norma ISO 27001.

KeyWords: ISO Standards: International Standarization Organization, MAGERIT: Risk Analysis and Management Methodology for Information Systems, PILAR: Software that used the methodology MAGERIT.

1. INTRODUCCIÓN

Las universidades reciben cada año a miles de estudiantes que ingresan a las diferentes carreras, y para mantener políticas y controles de acceso a la información, es de interés el establecer las condiciones adecuadas en Seguridad Informática. Por tanto se realizó una Evaluación Técnica de la Seguridad Informática, tomando como caso de estudio la Unidad de Tecnologías de Información UTIC'S de la Escuela Politécnica del Ejército (ESPE) que no está libre de riesgos y amenazas.

Para concienciar a los responsables de los Sistemas de Información de la existencia de riesgos y de la necesidad de minimizarlos, fue necesario aplicar los controles de la ISO 27002 [3], e ISO 27004 para conocer la situación actual del Data Center, ya que estas Normas son parte del estándar aceptado mundialmente, y que puede ser aplicado en cualquier organización.

Además fue necesario un método sistemático para analizar los riesgos [1], que ayudaron a descubrir y planificar las acciones adecuadas; MAGERIT 2, es la metodología formal para el análisis y gestión de riesgos que soportan los sistemas de información, elaborada por el Consejo Superior de Administración Electrónica de España [2].

Frente a este escenario, la comunidad investigadora ha mostrado un creciente interés en mejorar el Sistema de Gestión de la Seguridad de la Información a a nivel institucional, a través de las Norma ISO 27000. Así por ejemplo el trabajo propuesto por Alberto Rusbel y Duchi Bastidas en [11.], realizaron un estudio apoyandose en la Norma para definir politicas y realizar un plan de contingencias. Fanny Paulina Flores Estévez y Diana Carolina Jiménez Núñez en [12.], diseñaron un Sitema de Gestión de Seguridad de Información (SGSI), tomando como referencia la Norma ISO 27001:2005.

En el mismo contexto el trabajo propuesto por Alarcón Chávez y Rómulo Vladimir, en [13.], establece la aplicación de la Norma ISO 27001:2005 para definir políticas de seguridad, un plan y procedimientos para solucionar los problemas. Otros Investigadores de España, David Rodríguez Sánchez en [16.], aplicando la Norma ISO 27002, realizaron un control y auditoría para el servicio de correo electrónico.

Como principal contribución, se presenta en este artículo técnicas de evaluación para revisar controles y procedimientos Informáticos, determinar falencias actuales y sugerir soluciones amparadas en los estándares ISO 27000, en el área de Seguridad Informática, se utilizó el software PILAR, que aplica la Metodología MAGERIT; y se complementa con los Controles de la Norma ISO 27002.

Con el Análisis y Gestión de Riesgos realizado y los controles especificados en los dominios de Seguridad de la Norma ISO 27002, se obtuvo recomendaciones que servirán a la Institución para una futura elaboración del Plan de Seguridad Informático y considerar la posibilidad de certificarse con la Norma ISO 27001.

El resto del artículo ha sido organizado como sigue: La sección 2 muestra las técnicas de evaluación utilizadas para obtener el diagnostico previo de la seguridad informática de la institución. La sección 3 detalla la metodología para el análisis y gestión de riesgos. En la sección 4 se detalla la utilización del software empleado para realizar el análisis mencionado en la sección 3. En la Sección 5 se muestran los resultados obtenidos. En la sección 6, se analizan algunos trabajos relacionados. Finalmente en la sección 7, se presentan las conclusiones y líneas de trabajo futuro sobre la base de los resultados obtenidos.

2. TÉCNICAS DE EVALUACIÓN EN SEGURIDAD INFORMATICA PARA DIAGNÓSTICO DEL DATA CENTER

El concepto central sobre el que se construye la Norma ISO 27001 es el SGSI Sistema de Gestión de Seguridad de la Información, este sistema debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Para establecer y gestionar el SGSI en base a ISO 27001, se utiliza el ciclo continuo PDCA (ver Fig.1), Plan (planificar); en este ciclo se define el alcance del SGSI, la organización, su localización, activos y tecnologías, Do (hacer); este ciclo implanta el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control

identificados, incluyendo la asignación de recursos, responsabilidades y prioridades, posteriormente el ciclo Check (verificar); detecta a tiempo los errores en los resultados generados por el procesamiento de la información e identifica brechas e incidentes de seguridad, y para culminar con el ciclo Act (actuar); este realiza las acciones preventivas, correctivas y comunica las mejoras realizadas.

2.1 Normas ISO

El objetivo que tiene los estándares ISO es mostrar eficiencia en cuanto a calidad y también el mejoramiento de procesos, además son utilizados en la gestión de seguridad Informática por parte de la Familia ISO 27000 [5], y permiten la unificación de estándares aceptados a nivel mundial.

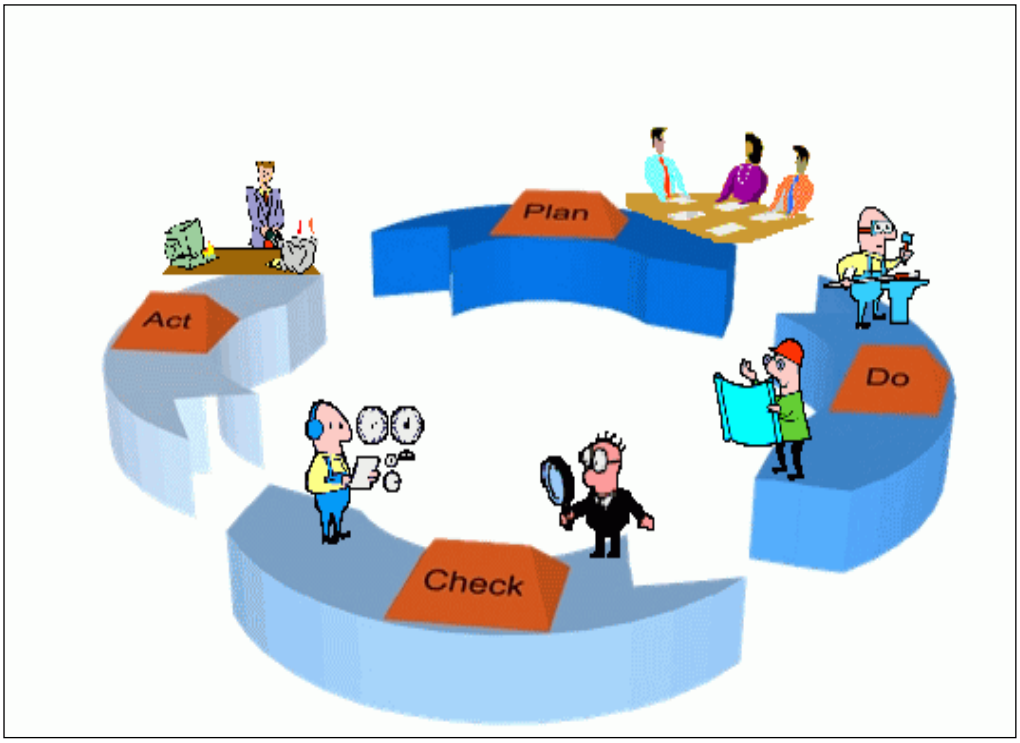

Figura1: Ciclo continúo PDCA para establecer y gestionar un SGSI [4.]

Normas Utilizadas de la ISO 27000

Las normas utilizadas en este proyecto que permitieron evaluar el nivel de seguridad del Data Center de la ESPE y guiaron para el tratamiento del mismo fueron la Norma ISO 27001, que en resumen contiene los requisitos del sistema de gestión de seguridad de la información [6], además la Norma ISO 27002, que es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información [7], apoyándose de los de los controles de la Norma ISO 27004, y para tener un enfoque de gestión de riesgos en la seguridad de la información de UTIC'S la Norma ISO 27005, apoyada de una metodología formal [9].

3. CONFIGURACIÓN DEL EXPERIMENTO

3.1 Diseño de la Topología de Prueba

Para realizar pruebas buscando vulnerabilidades de Testeo se utilizó desde un computador el software Helix, especializado en análisis forense y recuperaciones de emergencia, dentro de la red LAN (Red de área local) como fuera de ella (ver Fig. 2).

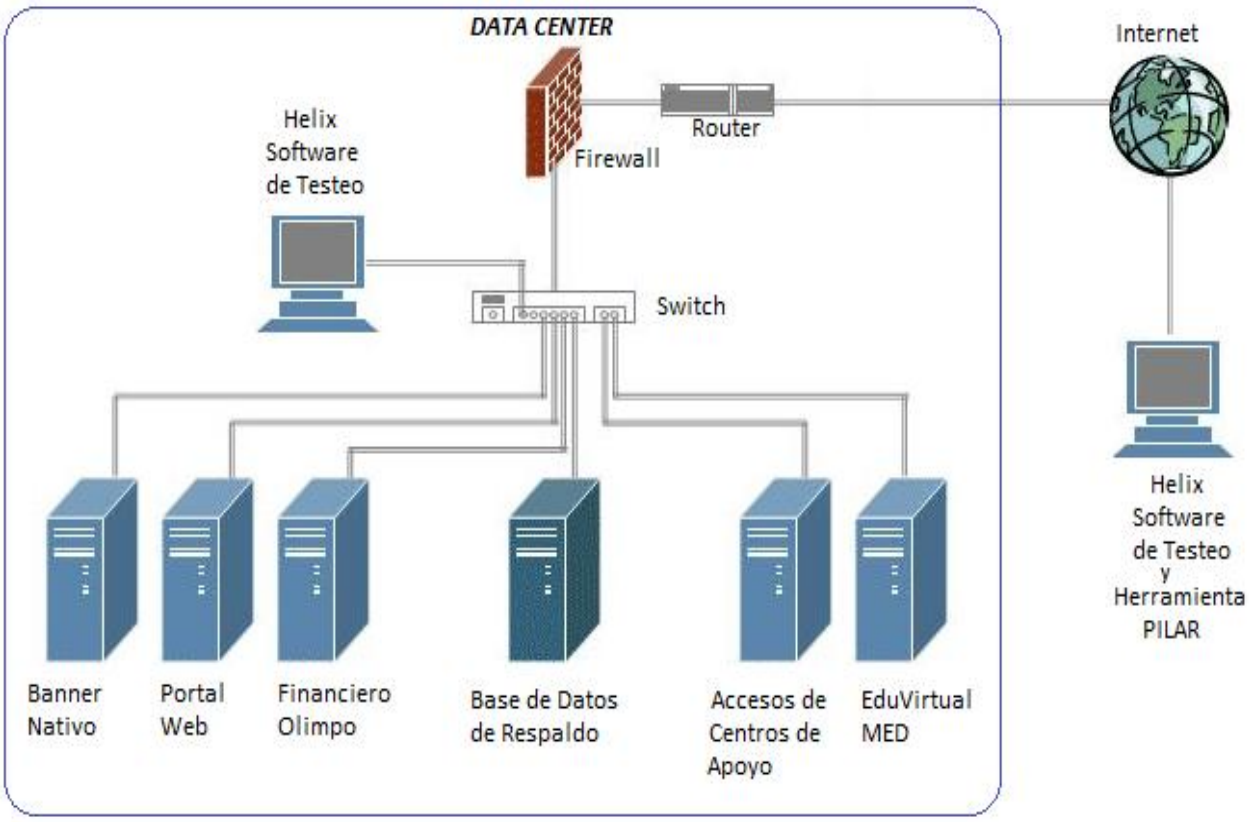

Figura2: Diseño de la Topología de Prueba

3.2 APLICACIÓN DE MAGERIT

3.2.1 Objetivo al aplicar la Metodología

Para establecer las directrices para la gestión del riesgo en la seguridad de la información del Data Center de la ESPE, fue necesario analizar la seguridad informática con el fin de evaluar la situación actual como un diagnóstico y mediante una planificación proponer soluciones eventuales.

3.2.2 Desarrollo aplicando la Metodología

Para aplicar la metodología MAGERIT, se tiene que llevar a cabo el proceso (ver Fig. 3).Estas actividades tendrán un lineamiento para llegar a los resultados propuestos que será explicado a continuación:

i. Identificación de Activos: Son los activos que posee la Organización clasificados de acuerdo a su función;
ii. Valoración de Activos: Es la valoración asignada al activo de acuerdo a la criticidad;
iii. Identificación de Amenazas: Son eventos que degradarían el valor de los activos;
iv. Frecuencia: Se refiere a los eventos que suceden en un tiempo determinado;
v. Degradación: Es cuán perjudicado resultaría el activo al materializarse las amenazas;
vi. Impacto: Es un indicador de qué puede suceder cuando ocurren las amenazas;
vii. Riesgo: Es la probabilidad de materialización de amenazas sobre el activo. Identificación y Valoración de Salvaguardas: Son las medidas precisas a tomar para reducir el riesgo;
viii. Riesgo Residual: Es el riesgo remanente después de aplicar las salvaguardas.

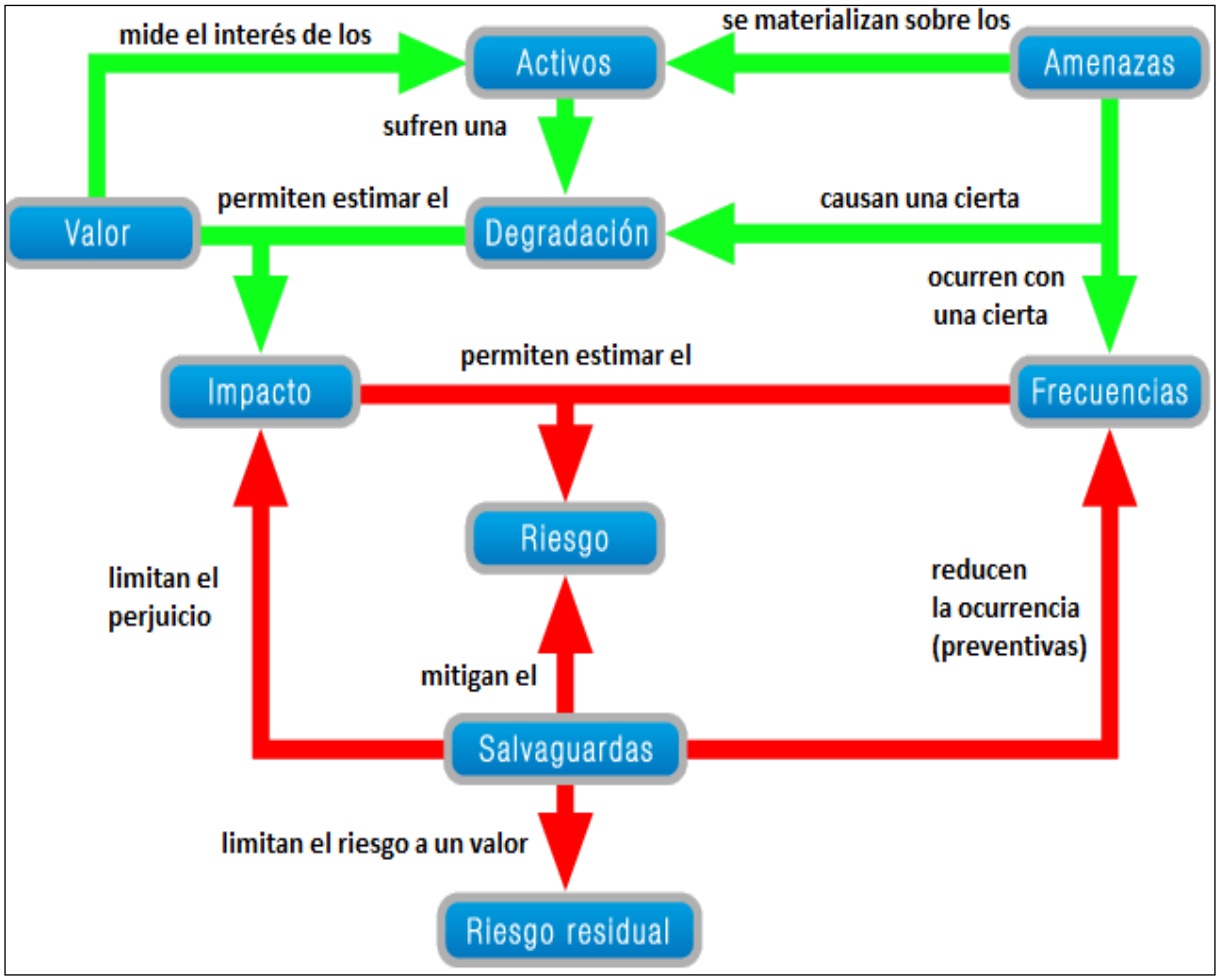

Figura3: Proceso de Metodología MAGERIT [10.]

3.3 APLICACIÓN DE LA HERRAMIENTA PILAR

Para complementar el análisis y gestión de riesgos fue necesario usar Pilar, un software que utiliza la metodología MAGERIT, y posee una biblioteca estándar de propósito general que permite evaluar con puntaje a la seguridad informática.

3.3.1 Utilización de Herramienta Pilar

Pilar puede ser instalado actualmente en Plataformas Windows y Linux, y su descarga desde la web respectiva. Este software tiene un costo comercial para empresas pero se puede obtener una licencia de evaluación por parte de sus creadores.

Pilar requiere para su funcionamiento previa a su instalación el motor Java o máquina Java virtual.

La versión de Pilar 4.4.2 se ejecuta a nivel de Windows XP, y desde la versión 4.4.5 en más plataformas incluyendo Windows 7.

Pilar permite en su interface desarrollar los siguientes pasos para obtener el Análisis de Riesgos (ver Fig. 4).

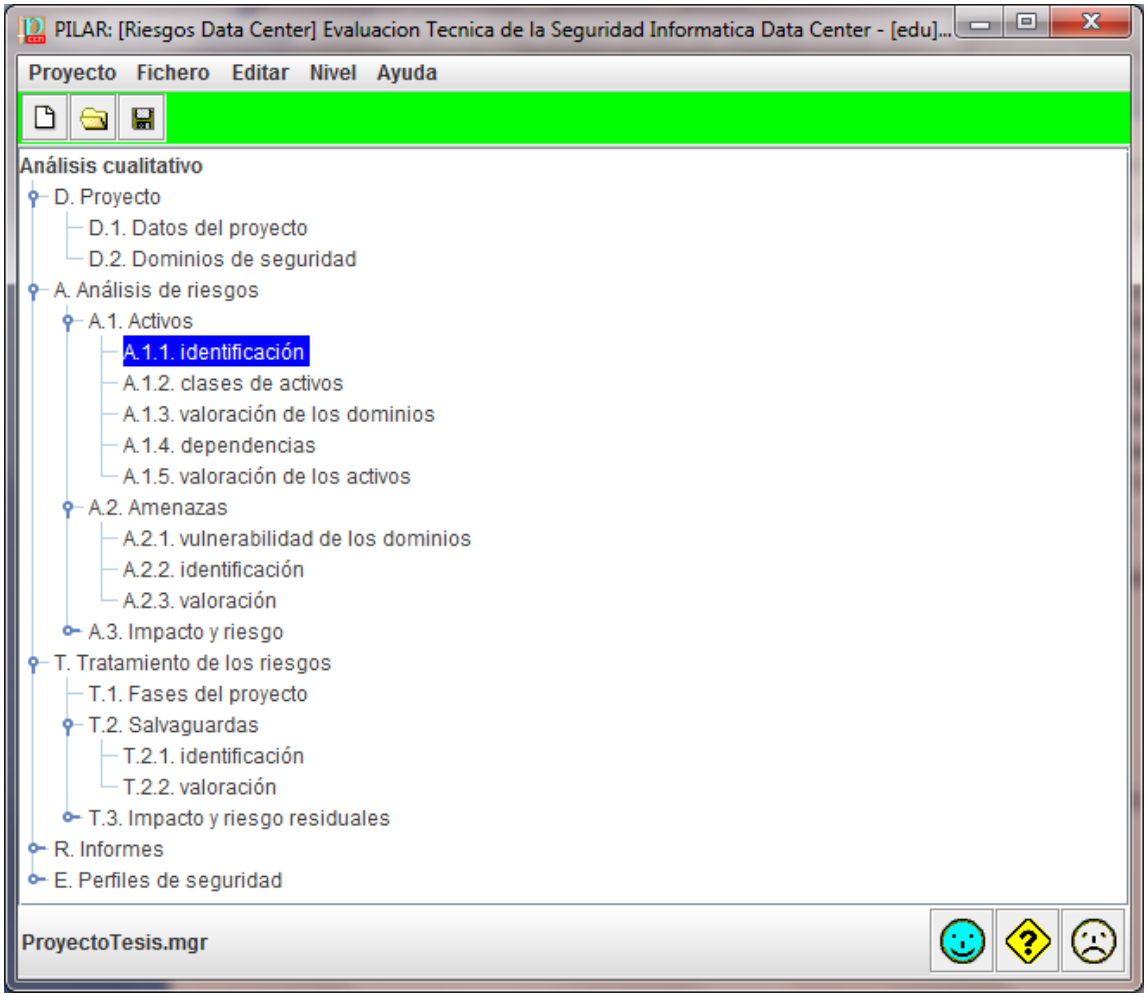

Figura4: Interfaz de Pilar v.4.4.2 para el Análisis de Riesgos.

En primer lugar se identifican los Activos y se los asigna dentro de una clasificación como sigue: [B] Capa de Negocio, en donde las letras como en este caso [B] se identifica en inglés como Business o Capa de Negocio. Aquí estarán los Activos de mayor importancia para la organización; [IS] Servicios Internos, contienen los Activos de servicio, como por ejemplo correo electrónico; [E] Equipamiento, se identifican en esta sección: [SW] Aplicaciones, [HW] Equipos, [COM] Comunicaciones y [AUX] Elementos Auxiliares; [SS] Servicios subcontratados, como por ejemplo Conexión a Internet; [L] Instalaciones, y finalmente [P] de Personal.

Luego se crean las dependencias empezando por los activos superiores o padre hacia los activos hijo que tienen alguna relación directa. Esta fase es muy importante ya que es necesario estén bien definidas las dependencias para proceder con los pasos subsiguientes.

En la etapa de Valoración de Activos se debe seleccionar por lo menos un nivel según el criterio de importancia entre el activo y sus vulnerabilidades. Los Niveles se encuentran en escala desde el 0 al 10, cada uno de ellos tiene las posibles vulnerabilidades que afectarían al activo, como se ha mencionado los Pilares que intervienen son: Disponibilidad, Integridad, Confidencialidad, Autenticidad, y Trazabilidad de la Información.

Posteriormente se deben identificar las amenazas, Pilar provee de una biblioteca y clasifica las amenazas automáticamente de acuerdo con el tipo de activo al que pertenece, también se puede elegir las amenazas que intervienen manualmente. Se deben asignar amenazas para cada uno de los activos creados en Pilar.

Luego se deben valorar las amenazas ingresando la frecuencia o probabilidad de que una amenaza se materialice según los criterios de Pilar, y luego ingresar la degradación por nivel o porcentaje.

En este punto Pilar genera las matrices de Impacto y Riesgo iniciales automáticamente. En la Opción Tratamiento de Riesgos se puede realizar un esquema de planificación para aplicar salvaguardas desde un estado current hacia un estado target u objetivo a cumplir. También se puede asignar el tiempo más conveniente entre esos estados como por ejemplo: el estado a tres meses (3m) y a un año (1y). Luego de ello se procede a identifican las salvaguardas, pudiendo utilizar el estándar que sugiere Pilar, el que es basado en un profundo análisis.

Una vez terminado este paso, se puede valorar las salvaguardas previamente aplicadas al proyecto, en donde se asignara a cada salvaguarda desde L0 a L5 el nivel correspondiente, empezando por current o situación actual y a los otros estados que por lo general estarán más cerca de un L5. Siendo L0 equivalente a salvaguarda inexistente, L1: Aplicadas inicialmente, L2: Reproducible pero intuitivo, L3: Proceso definido, L4: Gestionable y medible, L5: Optimizado.

Posterior a esto la herramienta presentará las salvaguardas con ciertos colores que representan los estados de madurez de la salvaguarda, siendo los de mayor criticidad los que están en rojo, que ameritan una solución inmediata.

Con este último paso se obtendrán como resultados las matrices de impacto y riesgos residuales, y también se tiene acceso a los informes textuales y gráficas para su respectivo análisis.

4. EVALUACION DE RESULTADOS

Para poder evaluar los resultados de las técnicas, se considero los resultados finales a la encuesta realizada a UTIC'S de la ESPE (ver Fig. 5); tomada como referencia los controles de la Norma ISO 27002: "Código de Buenas Prácticas"; obteniendo como resultado lo siguiente:

Figura5: Situación General del Data Center, aplicando la Norma ISO 27002

Aplicando la metodología MAGERIT los resultados generales obtenidos son más exactos, porque se basan en datos procesados con la herramienta Pilar al finalizar el Tratamiento de Riesgos, con un 34.55% (ver Fig. 5), que al utilizar la encuesta teniendo un resultado de 52.88% (ver Fig. 6).

En el siguiente resultado, se identifica en el eje de las abscisas la situación de la institución en el tiempo aplicando las salvaguardas y recomendaciones; y en el eje de la ordenada el nivel de seguridad porcentual de 0 a 100.

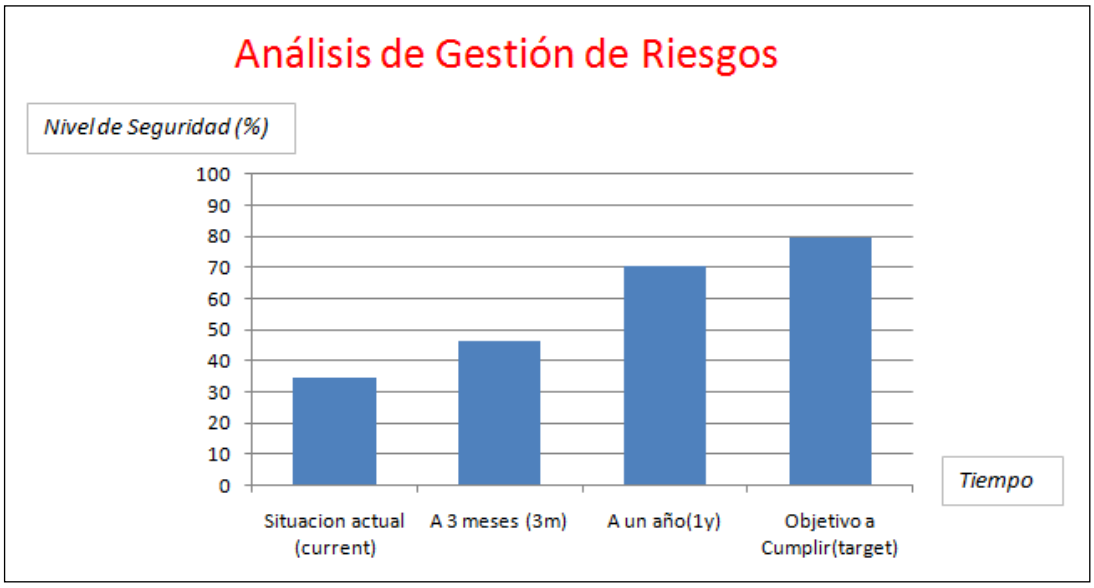

Figura6: Tiempo al aplicar las salvaguardas de PILAR, para el Análisis de Gestión de Riesgos.

La siguiente tabla (ver tabla 1), muestra los resultados anteriores (ver Fig. 6), de cada control y dominio de seguridad de la Norma ISO 27002, obtenidos en el resultado mediante la información ingresada en la herramienta PILAR:

Tabla1: Análisis de Gestión de Riesgos Aplicando Salvaguardas de PILAR.

base] Base | Fuentes de información

reco...	control	dudas	fuen...	apli...	com...	current	[3m]	[1y]	target
	[27002:2005] Código de buenas prácticas para la Gestión de la Seguridad de la Inf								
7	[5] Política de seguridad					21%	40%	58%	74%
8	[6] Aspectos organizativos de la seguridad de la información					55%	63%	77%	86%
9	[7] Gestión de activos					32%	41%	69%	69%
8	[8] Seguridad relacionada con los recursos humanos					90%	90%	95%	95%
9	[9] Seguridad física y del entorno					43%	53%	75%	82%
10	[10] Gestión de comunicaciones y operaciones					22%	40%	68%	77%
10	[11] Control de acceso					35%	43%	67%	76%
9	[12] Adquisición, desarrollo y mantenimiento de los sistemas de informaci					23%	38%	67%	79%
9	[13] Gestión de incidentes de seguridad de información					14%	23%	60%	68%
4	[14] Gestión de la continuidad del negocio					15%	38%	77%	92%
9	[15] Cumplimiento					30%	41%	64%	76%

5. TRABAJOS RELACIONADOS

En esta sección se han incluido los trabajos relacionados de la tesis. En lo que se refiere a la aplicación de la Norma ISO 27002, anteriormente llamada ISO 17799, Alberto Rusbel y Duchi Bastidas [11], realizaron un estudio de definición de políticas y plan de contingencias aplicables al centro de computo de la UPS apoyandondose en el código de práctica para la administración de la seguridad de la información. De igual manera y aplicando la norma mencionada Fanny Paulina Flores Estévez y Diana Carolina Jiménez Núñez [12], diseñaron un sistema de gestión de seguridad de la información para la empresa MEGADATOS S.A. en la ciudad de Quito

En este ámbito Alarcón Chávez y Rómulo Vladimir [13], aplicaron la Norma técnica ISO 27001:2005 para la gestión de la seguridad de la información en el Instituto Ecuatoriano de

Seguridad Social (IESS), haciendo un caso práctico a través de la dirección de desarrollo institucional y definiendo políticas de seguridad, plan y procedimientos para solucionar los problemas.

En el mismo contexto; para la institución ESPE, en el año 2008; se hizo una evaluación y auditoría del sistema de información de la ESPE, los autores fueron María Ángeles Salcedo Salgado y María Alexandra Tapia Mendieta [14], que utilizando el modelo COBIT evaluaron el cumplimiento de los controles citados en él, e identificaron falencias y formularon recomendaciones.

En cuanto al uso y aplicación de la metodología MAGERIT, la herramienta PILAR y la Norma ISO 27002, Adrián Bermúdez y Gabriela Salazar [15], en el año 2010; elaboraron un Plan de Seguridad Informática para la Escuela Superior Militar "Eloy Alfaro", en base a estándares internacionales para proteger los recursos informáticos y asegurar la viabilidad de las operaciones de la misma. Adicionalmente en la presente investigación se aplicó la Norma ISO 27004 para el diagnóstico de la seguridad informática en el Data Center, ya que los controles determinaron las vulnerabilidades que tienen y que son comparadas con los resultados generales (ver Fig.3 y Fig.4), entre la herramienta de la metodología y la Norma aplicada.

En España el trabajo propuesto por David Rodríguez Sánchez [16], aplicando la Norma Internacional ISO 27002, realizó un control y auditoría de correos electrónicos en Lotus Notes, resaltando de esta manera la importancia y el auge que tiene la aplicación de esta Norma.

6. CONCLUSIONES Y TRABAJO FUTURO

Con los datos recopilados se puede concluir la importancia que debe tener el SGSI Sistema de Gestión de Seguridad de la Información al usar los controles de la Norma ISO 27000 y la metodología MAGERIT con la herramienta software, determinando una mejora para la seguridad Informática del Data Center de la Escuela Politécnica del Ejército. Se consiguió que la investigación de los riesgos actuales que soportan los Sistemas de Información de UTIC´S sea de entendimiento entre los interesados y se ponga énfasis en los resultados obtenidos para que al implementar el nuevo Data Center se aplique las salvaguardas, normas y procedimientos necesarios para la seguridad informática sin olvidar los pilares de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Si bien los resultados muestran una mejora a nivel de seguridad informática y reducción del riesgo de la situación actual de 65.4% a 29.3%; estos números pueden mejorar a medida que se tome en cuenta la planificación propuesta y los correctivos necesarios planteados por la herramienta PILAR y de esta manera llegar al objetivo propuesto de 20.5%, mitigando en gran porcentaje a las amenazas y vulnerabilidades encontradas en la investigación.

Como trabajo futuro, La Unidad de tecnologías de Información puede tomar en cuenta los resultados obtenidos para aplicar en la construcción del nuevo Data Center y también proponer el Desarrollo del Plan de Seguridad Informático, e iniciar la certificación ISO 27001.

7. AGRADECIMIENTOS

Agradecemos a la Escuela Politecnica del Ejercito (ESPE), que a través de la facilidad de los recursos técnicos y humanos, de parte de la Unidad de Tecnologías de Información (UTIC'S), han hecho realidad la consecución de este proyecto. Un cordial agradecimiento al Ing. Mario Ron por la sugerencia en el tema de tesis inicial, al Ing. Walter Fuertes PhD. Director de Tesis, al Ing. Romel Aldas Codirector de Tesis y al Ing. Santiago Salvador delegado de UTIC'S, quienes han compartido sus conociminetos desinteresadamente, siendo guías y respaldo a lo largo de la elaboración del proyecto. A nuestros padres por su amor, comprensión y apoyo incondicional, que han fomentado valores y enseñanzas que nos han ayudado durante toda la carrera de Ingeniería en Sistemas.

8. REFERENCIAS BIBLIOGRÁFICAS

[1.] William P. Leonard, "La evaluación de la gestión: Una Evaluación de los métodos de gestión y desempeño Englewood Cliffs, McGraw-Hill glosario de términos y siglas Pág.5, Prentice Hall, 1962 [Citado el: 19 de Junio2011], Sebastián Firtman "Seguridad Informática", Pág. 18, MP Ediciones, 2005 [Citado el: 19 de Junio2011]

[2.] Publicación del Ministerio de Administraciones Públicas de España,"Libro de MAGERIT 2", Resumen MAGERIT versión 2 [Citado el: 19 de Junio2011] [Online:] http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184#

[3.] Estándar Internacional ISO/IEC 27002 (página 2) International Standard Book Numbering (ISBN) [Citado el: 19 de Junio 2011].

[4.] El portal de ISO 27001 Pág. 4, Publicada el 1 de Mayo de 2009. [Citado el: 19 de Junio 2011] [Online:] http://www.iso27000.es/sgsi.html#section2d

[5.] Martin Pérez, "Sociedad de la Información, Telecomunicaciones e Internet, Nuevas Tecnologías, Seguridad de la Información", 25 de 02 de 2007 [Citado el: 19 de Junio 2011] [Online:] http://sociedaddelainformacion.wordpress.com/2007/02/25/la-familia-de-normas-isoiec-27000/

[6.] El portal de ISO 27001, Publicada el 1 de Mayo de 2009. [Citado el: 19 de Junio 2011] [Online:] http://www.iso27000.es/iso27000.html

[7.] El portal de ISO 27001, Publicada el 1 de Julio de 2007 [Citado el: 19 de Junio 2011]

[8.] El portal de ISO 27001, Publicada el 7 de Diciembre de 2009. [Citado el: 19 de Junio 2011]

[9.] El portal de ISO 27001, Publicada el 4 de Junio de 2008. [Citado el: 19 de Junio 2011]

[10.] Libro de MAGERIT 2 – Publicación del Ministerio de Administraciones Publicas de España [En línea] Productos y servicios complementarios [Online:] https://www.ccn-cert.cni.es/index.php?option=com_wrapper&view=wrapper&Itemid=187&lang=es

[11.] Alberto Rusbel y Duchi Bastidas, Tesis: "Estudio y definición de Políticas Plan de contingencias aplicables al Centro de Computo de la UPS", Escuela Politécnica del Ejército, Sangolquí – Ecuador, 2002.

[12.] Fanny Paulina Flores Estévez y Diana Carolina Jiménez Núñez, Tesis: "Diseño de un sistema de gestión de seguridad de la información para la empresa MEGADATOS S.A. en la ciudad de Quito, aplicando las Normas ISO 27001 e IS0 27002", Escuela Politécnica Nacional, Quito-Ecuador, 2010.

[13.] Alarcón Chávez y Rómulo Vladimir, Tesis: Aplicación de la Norma técnica ISO 27001:2005 para la gestión de la seguridad de la información en el IESS. Caso práctico, dirección de desarrollo institucional, Escuela Politécnica del Ejército, Sangolquí – Ecuador, 2009.

[14.] María Angeles Salcedo Salgado y María Alexandra Tapia Mendieta, Tesis: "Evaluación y auditoría del sistema de información de la ESPE: dominio, planeación y organización", Escuela Politécnica del Ejército, Sangolquí – Ecuador, 2008.

[15.] Adrián Bermúdez y Gabriela Salazar, Tesis: Plan de Seguridad Informática para la Escuela Superior Militar "Eloy Alfaro", Escuela Politécnica del Ejército, Sangolquí – Ecuador, 2010.

[16.] David Rodríguez Sánchez, Tesis: "Control y Auditoría de correos electrónicos en Lotus Notes", Escuela Politécnica Superior Universidad Carlos III de Madrid, Leganés- España, 2.009.