EVALUACIÓN TÉCNICA DE LA SEGURIDAD INFORMÁTICA DEL DATA CENTER DE LA BRIGADA DE FUERZAS ESPECIALES NO. 9 "PATRIA"

Monserrath Viteri Díaz[1], Gabriel Chiriboga[2], Victor Páliz[3]

1 Escuela Politécnica del Ejército, Ecuador, monserath_viteri@yahoo.com

2 Escuela Politécnica del Ejército, Ecuador, gchiriboga@espe.edu.ec

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

RESUMEN

En la actualidad el uso del internet se ha vuelto muy necesario en el ámbito de la tecnología, economía, educación entre otros. Sin tener en cuenta que conlleva a tener mayor posibilidad de presentar amenazas y vulnerabilidades dentro de las organizaciones.

El presente trabajo se enfoca en el uso de las normas ISO 27000, dedicada a especificar los requisitos necesarios para: implantar, mejorar y mantener un sistema de gestión de la información y así tener menos riesgos de amenazas y vulnerabilidades informáticas.

De acuerdo a este escenario se aplicó la metodología MAGERIT que es el método formal para investigar los riesgos que soportan los sistemas de información y tomar medidas apropiadas para controlarlos. Simultáneamente se utilizo la herramienta PILAR, que está basada en la metodología MAGERIT.

El resto del trabajo ha sido organizado como sigue: La sección 2 muestra la metodología que fue seguida para evaluar y obtener el diagnostico previo de la seguridad informática de la institución. La sección 3 se presenta los materiales y métodos utilizados para el análisis. En la sección 4 se muestra los resultados obtenidos. En la sección 5, se analizan algunos trabajos relacionados. dentro de la sección 6, se presentan las conclusiones y líneas de trabajo futuro sobre la base de los resultados obtenidos. Finalmente las secciones 7 y 8 se da a conocer los agradecimientos y las referencias bibliográficas, respectivamente

Palabras Clave: **Normas ISO:** Organización Internacional de Normalización, **MAGERIT:** Metodología De Análisis y Gestión de Riesgos de los Sistemas de Información, **PILAR:** Software que ayuda a analizar y gestionar riesgos de un sistema de información siguiendo la metodología Magerit

ABSTRACT

At present the use of the internet has become very necessary in the field of technology, economics, education, etc. Regardless of which leads to have a greater possibility of threats and vulnerabilities within organizations.

This work focuses on the use of ISO standards 27000, dedicated to specify the requirements to: establish, improve and maintain a system of information management and so have less risk of computer threats and vulnerabilities. According to this scenario methodology was applied MAGERIT which is the formal method to investigate the risks that support information systems and take appropriate measures to

control them. Simultaneously use the tool PILAR, which is based on the methodology MAGERIT.

The rest of the paper is organized as follows: Section 2 shows the methodology that was followed to assess and obtain the prior diagnosis of the computer security of the institution. Section 3 presents the materials and methods used for analysis. Section 4 shows the results obtained. In Section 5 discusses some related work. In section 6 presents conclusions and future work are based on the results. Finally, sections 7 and 8 there is provided the acknowledgments and references, respectively.

KeyWords: **ISO Standards:** International Standarization Organization, **MAGERIT:** Risk Analysis and Management Methodology for Information Systems, **PILAR:** Software that helps you analyze and manage risks of an information system following the methodology Magerit

1. INTRODUCCIÓN

Las instituciones militares reciben cada año a miles de aspirantes a las diferentes áreas de instrucción militar, y para mantener políticas y controles de acceso a la información se deben establecer políticas de seguridad de la información. Es por este motivo que se accedió a realizar la Evaluación Técnica de la Seguridad Informática, teniendo como caso de estudio la Brigada de Fuerzas Especiales No. 9 “Patria”.

Para dar a conocer los riesgos existentes a los encargados del área informática fue necesario aplicar controles basados en la Norma ISO 27002 para conocer la situación actual.

Durante el análisis se tomo como guía la metodología MAGERIT, que 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.

En la actualidad ha ido creciendo el interés en mejorar el Sistema de Gestión de la Seguridad de la Información a nivel institucional teniendo en cuenta escenarios similares al que se describió anteriormente y valiéndose de las normas ISO.

La principal contribución que quiere presentar en el presente trabajo son 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.

2. METODOLOGÍA

2.1 Encuesta basada en la NORMA ISO 27004

Se utilizo una encuesta como primer instrumento para recoger, proponer y analizar la información, el mismo partió de un cuestionario como registro de la información obtenida.

La encuesta propuesta fue dividida en siete secciones, correspondientes a cada dominio de la NORMA ISO 27004, las mismas que contienen los criterios de medición de la eficacia de un SGSI.

Al momento de procesar la información de forma general y forma detallada fue mostrada porcentajes y manera gráfica de acuerdo a los dominios que se obtuvo durante la creación y aplicación del cuestionario.

2.2 Aplicación de MAGERIT

Durante la aplicación de la metodología MAGERIT, se realizaron cinco pasos: Identificar los activos, Determinar las amenazas a las que se encuentra expuestas los activos identificados anteriormente, determinación del impacto, determinación del riesgo y aplicación de salvaguardas.

Las valoraciones del impacto y riesgos fueron realizadas sin salvaguardas desplegadas, con el objetivo de obtener estimaciones reales del impacto o riesgo potencial, para luego proceder a aplicar las salvaguardas

Durante la identificación de los activos, se tomo los activos más relevantes para la institución con cada una de sus relaciones, tomando en cuenta las dimensiones de seguridad y su respectiva valoración.

2.3 Aplicación de PILAR

Una vez realizado el análisis con MAGERIT, se procedió a ingresar los datos en la herramienta PILAR, la misma que ayudó a evaluar la situación actual del Centro de Datos, como un diagnóstico previo y mediante una planificación para luego proceder a proponer soluciones eventuales.

3. MATERIALES Y MÉTODOS

Para aplicar la metodología MAGERIT, se tiene que llevar a cabo el proceso (mostrado en la Fig.1)

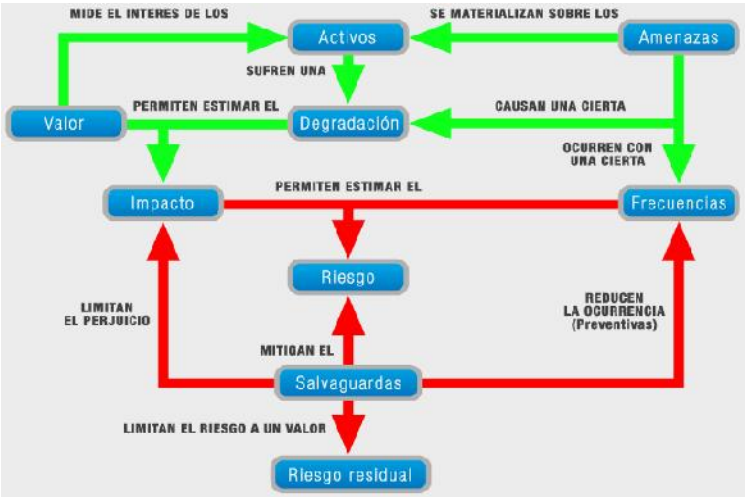

Fig 1. Procesos para aplicar MAGERIT

Para aplicar MAGERIT se deben seguir los siguientes pasos:

a. **Identificación de Activos:** Son los activos que posee la Organización clasificados de acuerdo a su función

b. **Valoración de Activos:** Es la valoración asignada al activo de acuerdo a la criticidad

c. **Identificación de Amenazas:** Son eventos que degradarían el valor de los activos

d. **Frecuencia:** Se refiere a los eventos que suceden en un tiempo determinado

e. **Degradación**: Es cuán perjudicado resultaría el activo al materializarse las amenazas

f. **Impacto**: Consecuencia que sobre un activo tiene la materialización de una amenaza.

g. **Riesgo:** Es la probabilidad de materialización de amenazas sobre el activo.

h. **Identificación y Valoración de Salvaguardas:** Son las medidas precisas a tomar para reducir el riesgo

i. **Riesgo Residual:** Es el riesgo remanente después de aplicar las salvaguardas.

Para complementar el análisis y gestión de riesgos fue necesario usar PILAR (mostrado en la Fig 2) software que utiliza la metodología MAGERIT, y posee una biblioteca estándar de propósito general que permite evaluar con puntaje a la seguridad informática.

Fig 2. Interface principal de PILAR

En el software PILAR se identifican los Activos y se los asigna dentro de una clasificación:

[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. 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.

Con la Norma 27001, se procedió a especificar los requisitos necesarios para establecer, implantar, mantener y mejorar un SGSI mediante el ciclo de Demig – PDCA (mostrado en la Fig. 3), el mismo que es acrónimo de: 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 3 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.

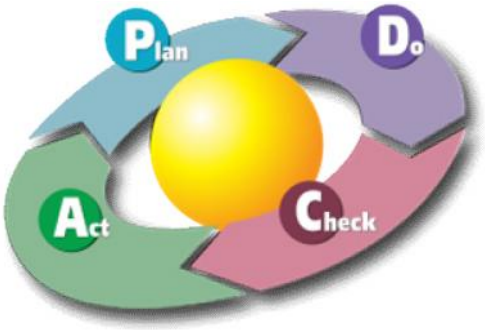

Fig 3: Ciclo continúo PDCA para establecer y gestionar un SGSI

Las normas utilizadas en el análisis y gestión de Riesgos para la Brigada de fuerzas Especiales BI -9 “Patria” , permitieron evaluar el nivel de seguridad del Centro de Datos de la Brigada y guiaron para el tratamiento del mismo, las principal guía fue la Norma ISO 27001, que en resumen contiene los requisitos del sistema de gestión de seguridad de la información, además la Norma ISO 27002, que es una guía de buenaprácticas que describe los objetivos de control y controles recomendables en cuanto a

seguridad de la información, 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.

4. RESULTADOS

Para poder evaluar los resultados de las técnicas, se considero los resultados finales de encuestas realizadas a los encargados del centro de datos de la Brigada de Fuerzas Especiales Bi - 9 "Patria" (mostrado en la Fig. 4), la encuesta tomo como guía los controles de la norma ISO 27002: "código de buenas prácticas"; obteniendo como resultado los siguientes porcentajes.

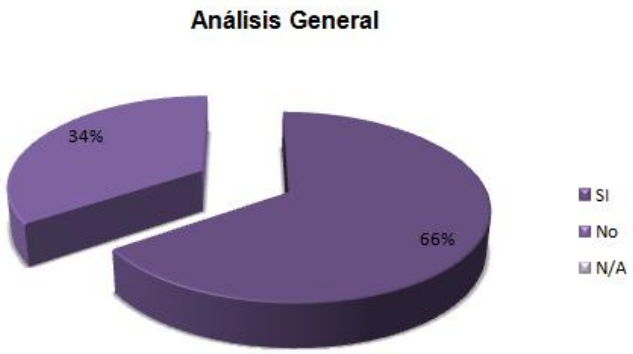

Fig 4: datos obtenidos de la encuesta

Durante la aplicación de la metodología MAGERIT, los resultados generales obtenidos se tornaron mas precisos, porque se utilizo la herramienta PILAR que se encargo de procesar los datos de forma casi automática.

Los resultados obtenidos a partir de PILAR son mostrados en la Fig.5, aquí se tiene cada control y dominio de Seguridad de la Norma ISO 27002, los mismos que fueron obtenidos a partir de la información ingresada en la herramienta PILAR.

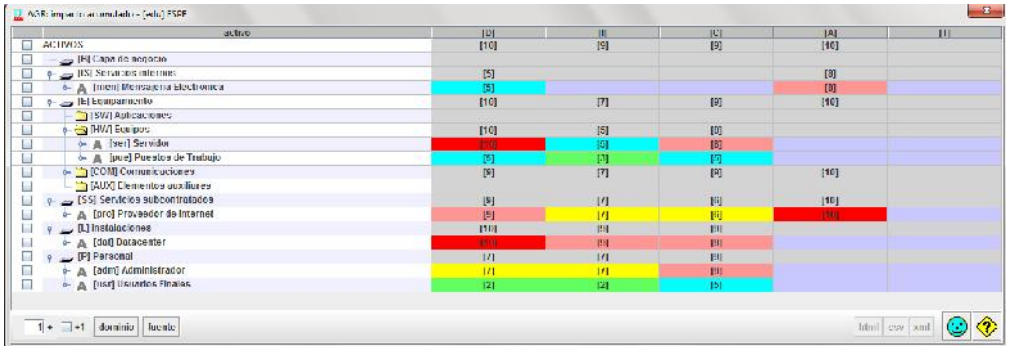

Fig 5. Matriz de riesgo acumulado

5. TRABAJOS RELACIONADOS

Los temas relacionados fueron: Elaboración del Plan de Seguridad Informática para la Escuela

Superior Militar “Eloy Alfaro”, con el soporte de la metodología MAGERIT, la herramienta PILAR y la Norma ISO 27002, los encargados de la elaboración fueron: Adrián Bermúdez y Gabriela Salazar , en el año 2010;

Análisis de la Seguridad Informática para la Escuela politécnica del ejército (ESPE) con la ayuda de MAGERIT, PILAR y las NORMAS ISO 27000, los que elaboraron el proyecto fueron Patricio Moscoso y Ricardo Guagualango, en año 2011.

6. CONCLUSIONES Y TRABAJO FUTURO

El análisis y gestión de riesgos de la información es importante dentro de las organizaciones, ya que sebe tener en cuenta que el activo más es la información.

Las normas ISO desempeñan un papel importante dentro del análisis y gestión de riesgos.

Cuando se quiera expandir o crear un nuevo centro de datos dentro de la brigada de fuerzas especiales BI -9 “Patria”, se tendrá como referencia el presente estudio para aplicar las salvaguardas, normas y procedimientos necesarios para mantener la seguridad informática, pero sin olvidar los aspectos fundamentales de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

Una vez concluido el análisis de gestión de riesgos y con los resultados obtenidos se puede decir que esto ayudará a desarrollar un nuevo proyecto de investigación para implementar un Plan de Contingencia.

7. AGRADECIMIENTOS

Agradezco a la Brigada de Fuerzas Especiales Bi -9 “Patria”, que a través de la facilidad de los recursos técnicos y humanos, de parte de la unidad de tecnologías de información, hicieron posible el desarrollo del presente proyecto. También agradezco al Ing. Mario Ron por su ayuda con respecto al tema de tesis, al Ec. Gabriel Chiriboga director de tesis, al Ing. Víctor Paliz codirector de tesis y al Crnl. Luis Castro Director de la Brigada “Patria”, quienes han compartido sus conocimientos y apoyo desinteresadamente, siendo guías y respaldo a lo largo de la elaboración del proyecto.

También agradezco a mis padres y familiares cercanos, los mismos que día a día me saben apoyar y dar su amor, comprensión y apoyo incondicional, que han fomentado valores y enseñanzas durante mis años de estudio.

8. REFERENCIAS BIBLIOGRÁFICAS

Publicación Del Ministerio De Administraciones Públicas De España,”Libro De Magerit 2”, Resumen Magerit Versión 2 [Citado El: 19 De Junio2011] [Online:]

Estándar Internacional Iso/Iec 27002 International Standard Book Numbering (Isbn) [Citado El: 19 De Junio 2011].

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

Libro De Magerit 2 – Publicación Del Ministerio De Administraciones Públicas De España [En Línea] Productos Y Servicios Complementarios [Online:]

EAR / PILAR / Documentación, Análisis De Riesgos[Citado El: 20 De Enero 2012] [Online:]

Guía De Seguridad De Las Tic, Manual De Usuario PILAR [Citado El: 15 De Febrero 2012] [Online:]