ESTUDIO DEL ESTÁNDAR ISO 27001:2013 Y SU DISEÑO PARA LA APLICACIÓN A LA FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN DE LA ESPOL

Pamela Solange Zambrano Martínez
Jorge Enmanuel Rendón Zambrano
Facultad de Ingeniería en Electricidad y Computación
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil-Ecuador
pszambra@espol.edu.ec
jorendon@espol.edu.ec
Director de Tesis: José Roberto Patiño Sánchez
Email: jpatino@espol.edu.ec

Resumen

Nuestro estudio realza el manejo de la información, dentro de una organización educativa. Analizamos el uso de la norma ISO 27001:2013 porque las instituciones deben mantener un alto grado de integridad, confidencialidad y seguridad de los datos, y sistemas que manejen el desarrollo de sus tareas, ya que el uso de este estándar reduciría la interrupción del flujo normal de actividades o pérdida de información vital. El estudio va dirigido a un segmento de la Facultad de Ingeniería en Electricidad y Computación (FIEC), con el fin de comprobar el cumplimiento de la ISO mencionada y presentar propuestas en caso de encontrarse fallos o vulnerabilidades. Se empleó la metodología MAGERIT para el análisis y gestión de riesgos del hardware y software. Al final se mostrarán los resultados en un reporte, junto con las recomendaciones para que la facultad llegue a la obtención de la certificación si lo requiere.

Palabras Claves: *Seguridad de la Información, ISO 27001:2013, MAGERIT, SGSI.*

Abstract

Our study highlights the management of information in an educational organization. We analyze the use of ISO 27001:2013 because the institutions must maintain a high level of integrity, confidentiality and security of the data and the systems that manage the performance of their duties, since the use of this standard would reduce the flow interruption of the normal activities or loss of vital information. The study is aimed to a segment of the Faculty of Electrical and Computer Engineering (FIEC for their acronym in Spanish) in order to verify the compliance with the mentioned ISO and present proposals if flaws and vulnerabilities are found. For the hardware and software analysis and risk management, the MAGERIT methodology was used. At the end the results will be shown in a report, along with the recommendations for the faculty so they can comply with the certification requirements

Keywords*: ISO 27001:2013, MAGERIT, SGSI.*

1. Antecedentes

Conforme mejora la tecnología, las distancias tienden a reducirse, y se vuelve más sencillo comunicarse, esto a su vez indica que mucha información pasa por estos canales, corriendo graves riesgos de que esta pueda filtrarse o perderse en su recorrido, esto requiere que exista algún sistema para evitar que algo malo suceda, para esto necesitaremos un Sistema de Gestión de Seguridad de la Información (SGSI), el cual nos ofrece un conjunto de normas y reglas que garantizan que la información sea tratada de la forma más profesional y segura posible.

Y es de aquí donde se desprende la ISO 27001, la cual se desarrolla en base a la norma Británica 7799-2, donde se crea la ISO 27001:2005 que fue la primera revisión, y actualmente con ciertos cambios se dio la ISO 27001:2013. El SGSI se debe certificar con los requerimientos de estudio, como un seguimiento de las

personas, los procesos y sistemas TI que se lleven a cabo en la empresa. [1]

Es necesario el incentivo de implantar esta ISO en centros de estudios que tenga su misión, visión bien planteadas, para alcanzar las categorías exigidas por los departamentos gubernamentales y ser una referencia frente a las demás, y por supuesto el desarrollo en conjunto como organización brindando excelencia a nivel educativo, automatización en las gestiones de procesos, tecnología informática y trabajo de quienes conformen la institución educativa.

2. Justificación

En la actualidad, las empresas grandes, medianas y/o pequeñas; las instituciones educativas, financieras, sociales, solo consideren como activo maquinarias, equipos de oficina, dispositivos portables, servidores, entre otros. Uno de los activos más importantes es la información, que se maneja dentro del negocio, como tarifas de precios, propiedad intelectual, cartera de clientes, nombres de proyecto, etc.

El Objetivo de este estudio es conocer sobre la última actualización de la ISO 27001:2013 y elaborar un diseño con esta norma en la Facultad de Ingeniería en Electricidad y Computación (FIEC), perteneciente a la Escuela Superior Politécnica del Litoral (ESPOL). La FIEC como facultad enfocada al estudio de carreras del área de computación, telecomunicaciones y afines, mantiene altos estándares por lo que actualmente cuenta con certificaciones Nacionales e Internacionales como la acreditación ABET y la Certificación de Calidad ISO 9001:2000.

3. Objetivos

Objetivo General

Analizar la norma ISO/IEC 27001:2013 y realizar un estudio de una parte de la red de la FIEC para comprobar su cumplimiento con los requisitos de este estándar, y presentar propuestas en el caso de encontrarse fallas en el tratamiento de la información en la misma.

Objetivos Específicos

- ✓ Analizar la norma y como esta puede adaptarse para centro de estudios superiores, usando la FIEC como base.
- ✓ Levantar la información de la red de la facultad.
- ✓ Analizar la información obtenida.
- ✓ Definir un sistema de gestión de riesgos adecuado para nuestro estudio.

4. Metodología: MAGERIT

MAGERIT es la metodología de análisis y gestión de riesgos de los sistemas de información. Este sistema se creó en España por el consejo Superior de Administración Electrónica, con el fin de ayudar a crear el Sistema de Gestión de Seguridad de la Información (SGSI).

Esta metodología recoge los siguientes informes y conclusiones, en síntesis:

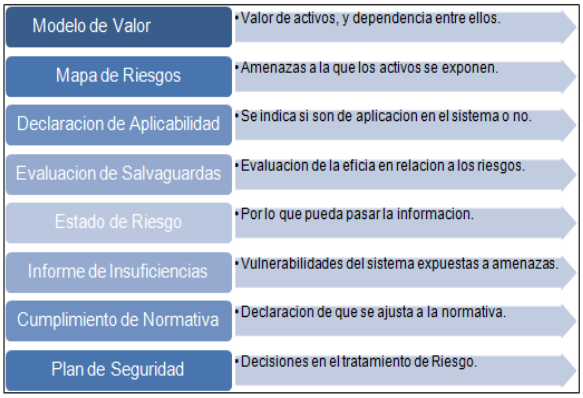

Figura 1 Informes y Conclusiones que persigue MAGERIT [2]

5. ISO 27001:2013

ISO 27001:2013 es un estándar internacional que gestiona el tratamiento de la seguridad de la información de toda nuestra organización, siendo la 27001:2013 su última revisión. El nombre completo de este estándar es "Information Technology – Security Techniques; Information security management systems – Requirements", traducido sería "Tecnologías de la información – Técnicas de seguridad; Sistemas de gestión de la seguridad de información – Requerimientos", este nombre se refiere a las 2 secciones principales del estándar. [3]

Esta norma busca evaluar y tratar los riesgos a los cuales nuestros datos son expuestos en el día a día, con el fin de implementar medidas de seguridad. Por lo que el objetivo de esta norma es basada en la gestión de riesgos para luego tratarlos.

ISO/IEC 27001:2013 se divide en 11 secciones, además del Anexo A, las secciones 0 a 3 son introductorias y opcionales, 4 a 10 son obligatorias para su implementación, entre estas tenemos: [4]

- ➢ Sección 0: Introducción.
- ➢ Sección 1: Alcance.
- ➢ Sección 2: Referencias Normativas.
- ➢ Sección 3: Términos y definiciones.
- ➢ Sección 4: Contexto de la organización.
- ➢ Sección 5: Liderazgo.

- Sección 6: Planeación.
- Sección 7: Soporte.
- Sección 8: Operación.
- Sección 9: Evaluación de rendimiento.
- Seccion 10: Mejoras.
- Anexo A.

6. Beneficios de implementar ISO 27001:2013

Existen varios beneficios en su implementación como:

- ✓ Mayor seguridad en el manejo de información.
- ✓ Capacidad de prevención a posibles fallas de seguridad y reacción ante ellas.
- ✓ Mayor nivel de competitividad al garantizar un manejo seguro de información.
- ✓ Reducción de costos al prevenir muchas brechas de seguridad.
- ✓ Mejor organización al tener todos los procesos documentados con sus respectivos responsables.
- ✓ Reducción de tiempo, tanto para el contratante como el contratado, ya que los procesos que la empresa maneja quedan definidos de manera organizada y categorizada.[5]

7. Análisis y Diseño

Nuestro estudio se basa en la información que manejan los laboratorios de computación y el edificio de gobierno, (marcados en la Figura 2 de color azul). Dado que nuestro estudio habla sobre la norma ISO de seguridad de la información y según el levantamiento de información, es aquí donde se registran procesos administrativos, flujo de datos, manejo de equipos, y personal técnico de Fiec.

A continuación la Figura 2 nos muestra las áreas que la Fiec posee, tales como: aulas, oficinas de Cisco, laboratorios de redes, de telecomunicaciones, de circuitos impresos, de maquinaria eléctrica. Al otro lado, cuenta con el edificio de Gobierno con aulas y laboratorios.

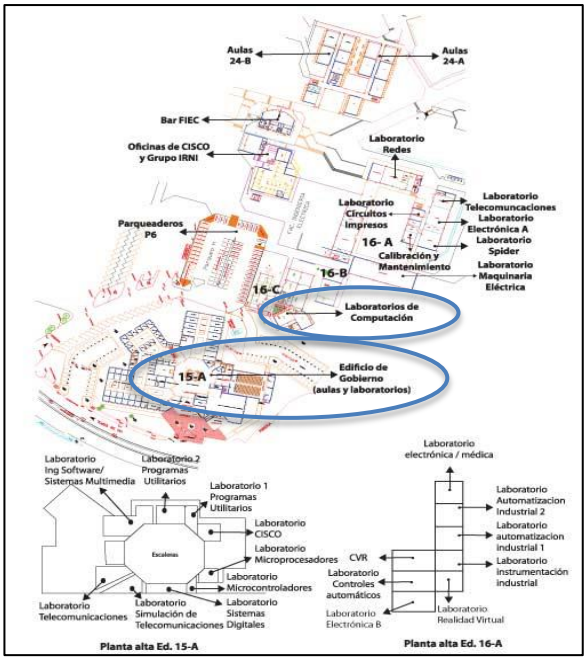

Figura 2 Tomada de la página de FIEC [6]

8. Identificación de amenazas

Luego de recopilar la información de la facultad, y haber analizado los activos que manejan, de categorizar cada uno de ellos, se procede a definir las posibles amenazas, con su posible probabilidad. La Tabla 1 nos muestra el modelo a seguir, para explicar cada una de estas.

Tabla 1 Descripción de la Amenaza

[CÓDIGO DE AMENAZA] Descripción de amenaza	
Lista de tipos de activos que pueden verse afectados.	Dimensiones de seguridad que se pueden ver afectadas por este tipo de amenazas, ordenadas por su relevancia, de mayor a menor.
Descripción detallada de la amenaza.	

9. Evaluación de Riesgos y Amenazas

Revisaremos los activos con cada posible amenaza, analizando los valores de degradación en el caso que éstos se vean afectados, y la probabilidad que suceda el inconveniente.

El impacto se determinará según los valores de degradación y probabilidad en que se presente el problema, y usaremos la siguiente tabla para determinar el nivel del mismo.

Tabla 2 Evaluación de Riesgos y Amenazas

		Degradación				
	Impacto	*1*	*2*	*3*	*4*	5
Ocurrencia	*1*	*1*	*2*	*3*	*4*	5
	2	*2*	*4*	*6*	*8*	10
	3	*3*	*6*	*9*	*12*	15
	4	*4*	*8*	*12*	*16*	20
	5	*5*	*10*	*15*	*20*	25

A continuación la tabla 2 muestra los resultados de la FIEC basado en el análisis de MAGERIT. Presentamos los activos con mayor promedio de impacto según la tabla de Ocurrencia VS Degradación.

Tabla 3 Resultados del análisis de Riesgos y Amenazas

[files] Archivos de los equipos de la fiec	8.89
[conf] Datos de configuración de equipos y equipos de red	7.42
[auth] Datos de autenticación para su uso en portal cautivo.	7.65
[int] Servicios internos ofrecidos a estudiantes y trabajadores	9.95
[host] Servidor de la FIEC	7.15
[pc] Equipos de escritorio de oficinas	8.35
[pc] Equipos de escritorio de laboratorios	12.38
[peripheral] Impresoras y scanneres(all in one)	8.44

10. Recomendaciones

- ✓ Se debe crear un manual de políticas de seguridad, el cual debe ser de fácil acceso a todos los trabajadores de la facultad, este puede ser físico o digital.
- ✓ La creación de una intranet podría ayudar a la difusión de la información no solo a nivel docente y estudiantil, sino también al personal técnico.
- ✓ Se debe concientizar a todos los usuarios de los servicios, desde los estudiantes hasta los directivos acerca del tratamiento correcto de la información mediante políticas.
- ✓ A pesar de que no exista un interés en adquirir la certificación ISO/IEC 27001:2013, es bastante recomendable que se trabaje en la implementación de un SGSI por motivos preventivos, ya que ha existido en los últimos meses bastante casos de fugas de información por parte de algunas organizaciones a nivel mundial.
- ✓ Se debería aumentar el área de cobertura de la red inalámbrica segura, en ciertos sectores de la facultad donde no es posible conectarse a la misma, limitando al estudiante la disponibilidad de los servicios.
- ✓ Según los resultados de este estudio, se debería en un plazo no mayor a 6 meses corregir las áreas determinadas de mayor afectación, y luego realizar otra auditoría.

11. Conclusiones

- ❖ ISO/IEC 27001:2013 es un estándar que se enfoca en la seguridad en el tratamiento de la información, además de ayudarnos a la creación de un SGSI.
- ❖ La implementación de un SGSI permite una mejor administración de los recursos y servicios de la información, pues nos permitirá prevenir y reducir daños o fugas de información, así como recuperarse en poco tiempo luego de sufrir problemas en la seguridad.
- ❖ Determinamos que la sección de la red de la FIEC en la cual realizamos nuestro estudio, no cumple con los requerimientos de la certificación ISO/IEC 27001:2013, al no existir políticas de seguridad documentadas, aun así, se considera que la red tiene un nivel alto de seguridad.

12. Agradecimientos

Al Ing. Rayner Durango por ser el promotor de este estudio. A nuestro guía y director de tesis, José Patino. A la Ing. Margarita Filian, Jefa de Laboratorio de Computación y la Ing. Katherine Campos, Asistente Técnico de Redes, por la supervisión y tiempo que nos brindaron para el desarrollo de este proyecto.

Gracias por ayudarnos en la recopilación de información de la FIEC, la cual pudimos analizar y dar un breve reporte de mejoras para que la facultad pueda obtener la certificación en caso que la requiera.

13. Referencias

[1] U. H. &. U. Nayak, The InfoSec Handbook: An Introduction to Information Security, Rekha Umesh, 2014.
[2] P. d. a. electrónica, «PAE,» [En línea]. Available: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

[3] SGSI, «SGSI,» 14 08 2013. [En línea]. Available: http://www.pmg-ssi.com/2013/08/la-nch-iso-27001-origen-y-evolucion/.
[4] 27001Academy, «27001Academy,» [En línea]. Available: http://advisera.com/27001academy/what-is-iso-27001/
[5] 27001Academy, «27001Academy,» [En línea]. Available: http://advisera.com/27001academy/what-is-iso-27001/ (Benefits of ISO 27001).
[6] .FIEC, [En línea]. Available: https://www.fiec.espol.edu.ec/index.php/en/ubicacion-geografica/mapadelafacultad