DISEÑO DE UN SISTEMA DE GESTIÓN EN CONTROL Y SEGURIDAD BASADO EN LA NORMA BASC PARA LA EMPRESA TRANSPORTES Y SERVICIOS ASOCIADOS SYTSA CÍA. LTDA.

Erika Moncayo, Mauricio Campaña, Fernando Solís

1 Universidad de las Fuerzas Armadas ESPE, Ecuador, erikapatriciamoncayosalas@hotmail.com

2 Universidad de las Fuerzas Armadas ESPE, Ecuador, emcampania@espe.edu.ec

3 Universidad de las Fuerzas Armadas ESPE, Ecuador, efsolis@espe.edu.ec

RESUMEN

El presente proyecto constituye la elaboración de un Sistema de Gestión en Control y Seguridad para la Empresa Transportes y Servicios Asociados Sytsa, con la finalidad de generar una cultura de seguridad en la organización como requerimiento de sus clientes en vista de las constantes irregularidades que existen en el área del comercio y segundo porque requieren de establecer políticas y procedimientos aplicados a los Sistemas de Información que permitan la obtención de la Certificación Basc en una de sus áreas de auditoría. Este proceso inicia con una evaluación de la situación actual de la empresa mediante la recopilación de información a través de encuestas, entrevistas, formularios, etc. Posteriormente se elabora el Análisis de Riesgos donde se establecen los activos, las amenazas y las salvaguardas. Para este proceso se utilizó la metodología MAGERIT, procedimiento para realizar Análisis de Riesgos, donde se obtiene como resultado el Impacto y los Riesgos que recae sobre los recursos informáticos de la empresa. Como producto final de este análisis se propone un Sistema de Gestión y Control mediante la generación de políticas y procedimientos según lo que recomienda la ISO 27001 para que posteriormente sean implementadas en la empresa y puedan cumplir con los requisitos de obtención de la certificación.

Palabras Clave: sistema de gestión, transporte terrestre, Norma BASC, políticas, seguridad.

ABSTRACT

This project is the development of a Management System Control and Security for Transportes y Servicios Asociados Sytsa Organization, in order to create a safety culture as clients requirements in view of the irregularities that exist in the trade area and second because they require to stablish policies and procedures applied to the Information System that allow obtaining the Certification Basc in one of their areas to audit. This process starts with an assessment of the current situation of the company by collecting information through surveys, interviews, forms and others. Later Risk Analysis where assets are set, the threats and safeguards is made. MAGERIT methodology procedure was used to perform risk analysis which is obtained as a result the Impact and Risks borne by the computing resources of the company for this process. The final product of this Analysis is proposed a Management and Control System through the development of policies and procedures as recommended by the ISO 27001 to be subsequently implemented in the company and can meet the requirements for obtaining certification.

KeyWords: management system, ground transportation, Norma BASC, security, policies.

1. INTRODUCCIÓN

Transportes y Servicios Asociados SYTSA, es una empresa ecuatoriana nacida en el año de 1996, dedicada al Transporte por carretera de mercancía nacional e internacional sean estos productos refrigerados, perecibles, secos o gases; su matriz está ubicada en la ciudad de Quito, lugar donde se realizan procedimientos logísticos, administrativos, financieros y mantenimiento de unidades y que va a hacer nuestro objeto de investigación.

Actualmente está iniciando un proceso de impulsar una cultura de seguridad al querer establecer políticas, procedimientos y controles con el deseo de minimizar los riesgos que pueden afectar a sus operaciones. Es por ende que antes ésta necesidad y en base a los requerimientos exigidos por la Norma BASC, en la etapa de Seguridad a la Información, se decidió realizar un Sistema de Gestión y Control enfocado a la seguridad de los recursos informáticos donde su activo más sensible constituye la información.

Para el desarrollo de este Sistema de Gestión inicialmente se realizó una evaluación del estado actual de la empresa, a través de encuestas y entrevistas tanto a usuarios como a propietarios y al encargado del área de sistemas. Posteriormente se realizó el establecimiento y clasificación de los activos con los que cuenta la empresa, con esta información se dio inicio al Análisis de Gestión de Riesgos, de donde se obtuvo como resultado el impacto y los riesgos a los activos informáticos de la empresa.

La solución que se obtuvo como resultado de esta investigación o análisis fue la de generar un Plan que consta de políticas y procedimientos que serán implementadas posteriormente para su beneficio.

Al no existir lineamientos claramente definidos que permitan implementar políticas de seguridad informática, al ser auditados por BASC no cumplirían con los requerimientos establecidos por esta entidad, lo que ocasionaría la no obtención de la certificación y pérdida de contratos con clientes que exigen que sus proveedores cuenten con normas de seguridad certificadas.

A partir de la realización de este Sistema de Gestión SYTSA al realizar la implementación en lo posterior estará en la capacidad de ser auditada para la obtención del certificado y lo más importante estará estableciendo una cultura de seguridad informática entre sus colaboradores.

El artículo se ha organizado de la siguiente manera: en la Sección 2 se describe la Metodología utilizada y la herramienta de apoyo para la realización del Análisis de Riesgos con la finalidad de obtener Impacto y Riesgos, y la base sobre la que se generó las políticas y procedimientos. En la Sección 3 se hace mención a las herramientas y métodos utilizados. En la sección 4 se describe los trabajos relacionados que sirvieron de apoyo y guía para la elaboración del proyecto. La Sección 5 describe los resultados obtenidos y finalmente la Sección 6 se detallas las conclusiones y trabajos futuros.

2. METODOLOGÍA

2.1 Introducción

En primera instancia se debe tomar en cuenta que los sistemas de gestión de seguridad de la información están formados por 4 etapas cíclicas (Plan Do, Check y Act). (EL PORTAL DE ISO 27000)

Figura 1 Ciclo Continuo PDCA. Fuente ISO 27000

Tal como se muestra en la Figura1, la primera etapa de Planificación interviene el Análisis de Riesgo, en este caso inicialmente se debe definir el alcance y los límites del análisis, establecer la metodología en este caso la metodología que se utilizó para realizar el Análisis de Gestión de Riesgo fue la metodología Magerit. En la segunda etapa "DO" se define el Plan para el tratamiento de los Riesgos y se implementan los controles. En la tercera etapa de "Check" es una etapa de ejecución de procedimientos de monitorización y revisión, se detectan errores, se identifica incidentes de seguridad y se mide la efectividad de los controles. En la última "Act" es una etapa de mantenimiento y mejoras. (EL PORTAL DE ISO 27000)

Enseguida se inicia con el Análisis de Gestión de Riesgos, como se mencionó anteriormente la metodología que se utilizó fue la de Magerit es una metodología que permite conocer el riesgo que puede alcanzar un activo para poder realizar su gestión. (EAR PILAR/MAGERIT, 2012)

Las etapas del Análisis de Riesgo que sigue Magerit se muestran en la Figura No.2 y son:

a. Modelo de Valor
b. Mapa de Riesgos
c. Evaluación de Salvaguardas
d. Estado de Riesgo

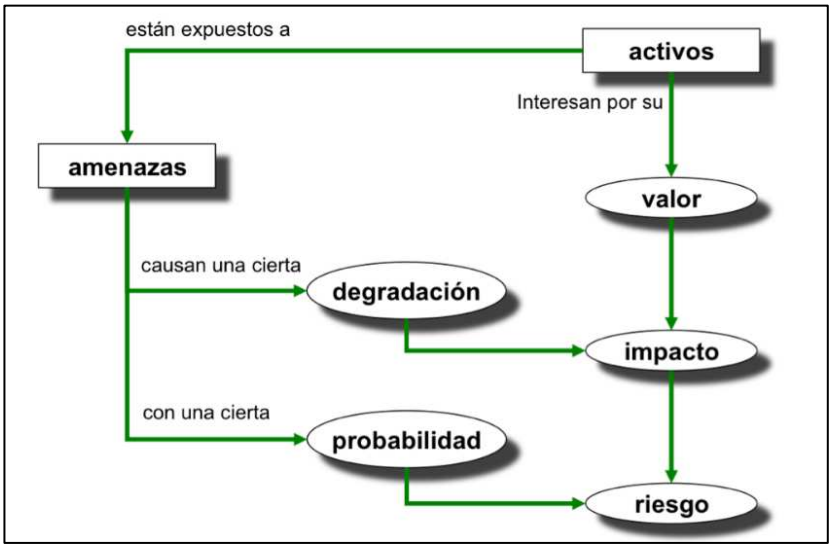


Figura 2 Elementos del análisis de riesgos potenciales.

. A continuación se describirá cada uno de estas etapas de acuerdo a la información obtenida en la empresa, por medio de encuesta, entrevista, formularios.

.

a. **Modelo de Valor.** Está conformada por tres aspectos importante, primero la identificación de acti-

vos, segundo la dependencia de activos y tercero valoración de los mismos, la identificación de los activos informáticos de la empresa se lo realizó a través de encuestas, entrevistas y formularios. Los activos fueron divididos en grupos: Servicios, Datos, Aplicaciones, Equipos Informáticos, Redes de Comunicaciones, Soportes de Información Equipamiento Auxiliar, Servicios Subcontratados, Instalaciones y Personal.

Identificados los activos se puede observar que un activo depende de otro u otros activos inferiores, es decir forman un árbol donde los que se encuentran por debajo son apoyo de los activos que se encuentran más arriba.

Continuando con el proceso es necesario asignar un valor a cada activo dependiendo del grado de criticidad que tenga dentro de la empresa evaluado desde el punto de vista de la confidencialidad, disponibilidad e integridad, se lo hizo en base a encuestas realizadas al encargado del área de sistemas. El valor que se le da a cada activo también puede ser acumulado es decir que se le agrega también la suma del grado de criticidad que tengan los activos inferiores.

b. **El Mapa de Riesgos.** En este paso se identifican las amenazas de cada activo, Magerit cuenta con un Catálogo de Elementos de amenazas que pueden ocurrir normalmente. Se clasifican en amenazas de origen natural, del entorno, defectos de las aplicaciones, causadas por las personas de forma accidental o deliberada. De igual forma la amenaza debe ser valorada de acuerdo a la incidencia que tengo sobre un activo, mediante una Escala de Degradación que va desde un valor Muy Alto hasta un valor muy Bajo y de una Escala de Frecuencia que puede tener criterio de un día como de años.

c. **Evaluación de Salvaguardas.** Las salvaguardas constituyen aquellos procesos, políticas, procedimientos que hacen frente a una amenaza. Magerit de igual forma presenta un Catálogo de Salvaguardas las cuales fueron evaluadas colocando un porcentaje dependiendo del grado en que la empresa las haya o no aplicado para cada clasificación de activo. (EAR PILAR/MAGERIT, 2012)

d. **Estado de Riesgo.** Este proceso permite determinar los impactos y riesgos del que son sujetos los activos. El Impacto es la medida del daño sobre el activo derivado de la materialización de una amenaza. (EAR PILAR/MAGERIT, 2012)**.** El Riesgo es la medida del daño probable sobre un sistema. (EAR PILAR/MAGERIT, 2012). De igual forma ambos son clasificados de acuerdo al nivel de criticidad desde Extremadamente crítico a Despreciable.

La herramienta PILAR es un Software que utiliza para su gestión Magerit, este programa sirvió de gran apoyo para el procesamiento de los datos y resultados. Se puede realizar un análisis cualitativo o cuantitativo. En el caso de este proyecto se ha realizado un Análisis Cuantitativo. Pilar permite el ingreso de Activos, Amenazas y Salvaguardas (o las propias que tiene el software), para determinar la generación de Tablas de Impacto y Riesgos.

Después de realizado el Análisis de Gestión de Riesgos y conocedores de los impactos y los riesgos que posee la empresa, es hora de realizar el Sistema de Gestión de Control y Seguridad. En esta etapa se colocó controles de acuerdo a los riesgos encontrados sobre los activos. Se estableció políticas y procedimientos seguidas por los lineamientos que no da la ISO 27001.

3. MATERIALES Y MÉTODOS

Para la realización de este Sistema de Gestión se utilizaron las siguientes herramientas:

1. Metodología Magerit, es una metodología que permite realizar una Análisis de Gestión de Riesgos con el fin de conocer los riesgos, amenazas y de obtener una planificación de medidas para mantener los riesgos bajo control.

2. Lineamientos ISO 27001, este estándar contiene las directrices para evaluar y emitir políticas y procedimientos que proporciona la Guía de Buenas Prácticas donde hace referencia a los objetivos de control y controles recomendados respecto a la seguridad de la información.
3. Software Pilar Basic, constituye una herramienta de apoyo para la realización del Análisis de Riesgos, Esta herramienta utiliza la Metodología Magerit.

4. TRABAJOS RELACIONADOS

En esta sección se cita al trabajo realizado por Adrián Bermúdez y Gabriela Salazar en el año 2010 mediante la Elaboración de un Plan de Seguridad Informática para la Escuela Superior Militar “Eloy Alfaro”, (ADRIAN & SALAZAR GABRIELA, 2010) donde se elabora un trabajo basado en la Metodología Magerit para el Análisis de Riesgos con el uso y aplicación de la Herramienta Pilar como apoyo en el procesamiento datos y obtención de resultados.

También cabe anotar el trabajo realizado por Patricio Moscoso y Ricardo Guagalando en el año 2011 con la Evaluación Técnica de la Seguridad Informática del Datacenter de la Escuela Politécnica del Ejército, (MOSCOSO & GUAGALANGO, 2011)donde aplican también la Metodología Magerit pero adicionalmente presentan un Plan ejecutivo donde muestran normas y procedimientos de seguridad tomando como referencia la ISO 27001.

5. RESULTADOS

- Al efectuar el Análisis de Gestión de Riesgos se pudo obtener los siguientes resultados:

Impacto Acumulado: que es el valor acumulado del activo y las amenazas a las que está expuesto. (EAR PILAR/MAGERIT, 2012)

potencial | actual | objetivo | PILAR

activo	[D]	[I]	[C]
ACTIVOS	[10]	[10]	[10]
[SI] SOPORTES DE INFORMACION			
[D] DATOS/INFORMACION	[9]	[10]	[10]
[INF_SYT] INFORMACION LOGISTICA	[9]	[10]	[10]
[INT_SYT] INFORMACION POR DEPARTAMENTO	[9]	[10]	
[LOG] INFORMACION DE REGISTROS DE INGRESOS SOBRE LOS SERVIDORES	[8]	[9]	[9]
[PER_B_SYT] INFORMACION PERSONAL DE CADA USUARIO	[2]	[3]	[3]
[B] Activos esenciales	[8]		
[IS] Servicios internos	[9]	[9]	[2]
[E] Equipamiento	[10]	[10]	[10]
[SW] APLICACIONES	[10]	[10]	[10]
[HW] EQUIPOS	[10]	[10]	[10]
[SBD_SYT] SERVIDOR DE DATOS	[10]	[10]	[10]
[FIREWALL_SYT] FIREWALL	[10]	[8]	
[DESKTOP_SYT] COMPUTADORAS DE ESCRITORIO	[3]	[1]	[7]
[LATOPS_SYT] COMPUTADORAS PORTATILES	[3]	[1]	[6]
[SCAN_SYT] SCANNER	[0]	[0]	[0]
[PRINT1_SYT] IMPRESORAS MATRICIALES	[1]		
[PRINT2_SYT] IMPRESORA LASER	[1]		
[SWITCH_SYT] SWITCH	[10]	[8]	[9]
[ROUTER_SYT] ROUTER	[10]	[8]	
[GTWY_SYT] GATEWAY	[10]	[8]	[9]
[WIFI_SYT] PUNTOS DE ACCESOS WIRELESS	[10]	[8]	[9]
[PABX_SYT] CENTRAL TELEFONICA	[7]	[5]	
[COM] Comunicaciones	[9]	[8]	[9]
[AUX] Elementos auxiliares	[10]	[4]	[9]
[SS] Servicios subcontratados			
[L] Instalaciones	[10]	[7]	[9]
[P] Personal			[10]

Figura 3 Matriz Impacto Acumulado.

En la Figura 5 se muestra el Impacto Acumulado donde se puede determinar que el mayor impacto recae sobre la Información Logística, servidor de datos y equipos (Hw) como son el Switch, router, Gateway.

Impacto Repercutido: Se toma en cuenta el Valor propio mas las amenazas a las que está expuesto los activos de los que dependen.

SYT: impacto repercutido - sin licencia

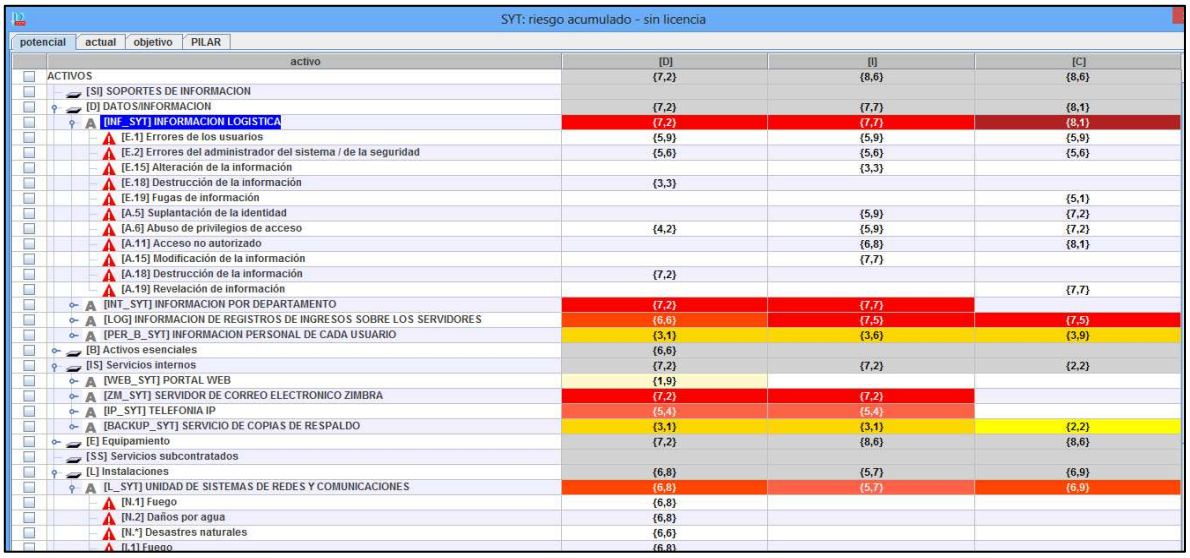
potencial | actual | objetivo | PILAR

activo	[D]	[I]	[C]
ACTIVOS	[10]	[10]	[10]
[INF_SYT] INFORMACION LOGISTICA	[10]	[10]	[10]
[INT_SYT] INFORMACION POR DEPARTAMENTO	[7]	[7]	
[LOG] INFORMACION DE REGISTROS DE INGRESOS SOBRE LOS SERVIDORES	[9]	[9]	[9]
[PER_B_SYT] INFORMACION PERSONAL DE CADA USUARIO	[0]	[0]	[0]
[TC_SYT] TRANSPORTE DE MECANCIA REFRIGERADA/SECA	[9]		
[AC_SYT] ALQUILER DE CONTENEDORES	[6]		
[SMD_SYT] SERVICIO DE MONTAJE Y DESMONTAJE	[6]		
[WEB_SYT] PORTAL WEB	[1]		
[ZM_SYT] SERVIDOR DE CORREO ELECTRONICO ZIMBRA	[10]	[10]	
[IP_SYT] TELEFONIA IP	[7]	[6]	

Figura 4 Matriz Impacto Repercutido

En la Figura 6 se muestra el Impacto Repercutido, el cual recae en un mayor grado de criticidad sobre la Información Logística, el servidor de correo electrónico y servidor de base de datos

Riesgo Acumulado: es el producto del impacto acumulado sobre un activo por la frecuencia de la amenaza.



activo	[D]	[I]	[C]
ACTIVOS	{7,2}	{8,6}	{8,6}
[SI] SOPORTES DE INFORMACION			
[D] DATOS/INFORMACION	{7,2}	{7,7}	{8,1}
[INF_SYT] INFORMACION LOGISTICA	{7,2}	{7,7}	{8,1}
[E.1] Errores de los usuarios	{5,9}	{5,9}	{5,9}
[E.2] Errores del administrador del sistema / de la seguridad	{5,6}	{5,6}	{5,6}
[E.15] Alteración de la información		{3,3}	
[E.18] Destrucción de la información	{3,3}		
[E.19] Fugas de información			{5,1}
[A.5] Suplantación de la identidad		{5,9}	{7,2}
[A.6] Abuso de privilegios de acceso	{4,2}	{5,9}	{7,2}
[A.11] Acceso no autorizado		{6,8}	{8,1}
[A.15] Modificación de la información		{7,7}	
[A.18] Destrucción de la información	{7,2}		
[A.19] Revelación de información			{7,7}
[INT_SYT] INFORMACION POR DEPARTAMENTO	{7,2}	{7,7}	
[LOG] INFORMACION DE REGISTROS DE INGRESOS SOBRE LOS SERVIDORES	{6,6}	{7,5}	{7,5}
[PER_B_SYT] INFORMACION PERSONAL DE CADA USUARIO	{3,1}	{3,6}	{3,9}
[B] Activos esenciales	{6,6}		
[IS] Servicios internos	{7,2}	{7,2}	{2,2}
[WEB_SYT] PORTAL WEB	{1,9}		
[ZM_SYT] SERVIDOR DE CORREO ELECTRONICO ZIMBRA	{7,2}	{7,2}	
[IP_SYT] TELEFONIA IP	{5,4}	{5,4}	
[BACKUP_SYT] SERVICIO DE COPIAS DE RESPALDO	{3,1}	{3,1}	{2,2}
[E] Equipamiento	{7,2}	{8,6}	{8,6}
[SS] Servicios subcontratados			
[L] Instalaciones	{6,8}	{5,7}	{6,9}
[L_SYT] UNIDAD DE SISTEMAS DE REDES Y COMUNICACIONES	{6,8}	{5,7}	{6,9}
[N.1] Fuego	{6,8}		
[N.2] Daños por agua	{6,8}		
[N.*] Desastres naturales	{6,6}		
[I.1] Fuego	{6,8}		

Figura 5 Riesgo Acumulado

En la Figura 7 se muestra el Riesgo Acumulado, donde se puede concluir que las Amenazas con un mayor grado de criticidad sobre el activo son:

- [A11] Acceso no autorizado
- [A3] Manipulación de los Registro de Actividad
- [A6] Abuso de privilegios de Acceso
- [A19] Revelación de la Información
- [A15] Modificación de la Información
- [E24] Caída del Sistema por Agotamiento de Recursos

- Después del análisis y evaluación realizadas de ha emitido políticas, procedimientos y controles con el fin de que en lo posterior la empresa implemente y pueda aplicar a la certificación Basc.

- Cabe notar en esta parte que uno de los mayores inconvenientes que muestra la empresa es el sitio de las Instalaciones que actualmente ocupan los recursos informáticos, el sitio actualmente no cuenta con las condiciones adecuadas en cuanto a infraestructura, climatización y seguridad, ha existido incluso daños por agua, existe con accesos de personal sin autorización y sin documentación.

6. CONCLUSIONES Y TRABAJO FUTURO

La Metodología y la Herramienta utilizada para el Análisis de Riesgo resulta adecuada porque permite comparar la información para la obtención de impactos y riesgos y que estos a su vez sean tratados de acuerdo al grado de criticidad de cada uno, en este caso la Información y las Instalaciones necesitan de una atención inmediata es por eso que se estableció políticas y controles que mitiguen los riesgos. Este es el inicio de una buena cultura de seguridad. Los integrantes de la empresa para la cual se definió este sistema se encuentran con la mejor disposición de implementar el plan y mejorar sustancialmente en todo lo correspondiente a seguridad

A futuro es muy importante que se realicen periódicamente auditorías planificadas, pueden ser internas realizadas por la propia empresa con el objetivo de efectuar una revisión periódica y realizar cambios o mejoras a lo que ya está planteado o auditorías solicitando personal externo para verificar el cumplimiento de las políticas y procedimientos aplicadas. Es importante tomar en cuenta que la empresa posterior a la implementación de este Sistema de Gestión estará en capacidad de aplicar a la Certificación Basc a la cual se encuentra afiliada actualmente.

7. REFERENCIAS BIBLIOGRÁFICAS

- LOPEZ, Francisco, AMUTO, Miguel, Javier 2006, MAGERIT-versión 2, Metodología de Análisis de Gestión de Riesgos de los Sistemas de Información II-Catálogo de Elementos,
- EL PORTAL DE ISO 27000. (s.f.). *GESTION DE SEGURIDAD DE LA INFORMACIÓN*. Obtenido de http://www.iso27000.es/sgsi.html
- EAR PILAR. (10 de 10 de 2012). *MAGERIT VERSION 3 ENTORNO DE ANÁLISIS DE RIESGOS*. Obtenido de https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/
- Fernández, C. M. (1988). Seguridad en Sistemas Informáticos. España: Ediciones Diaz de Santos S.A.
- Adrián Bermúdez y Gabriela Salazar, Tesis: Plan de Seguridad Informática para la Escuela Superior Militar “Eloy Alfaro”, Escuela Politécnica del Ejército, Sangolquí – Ecuador, 2010.
- Patricio Moscoso, Ricardo Guagalango, Tesis: Evaluación Técnica de la Seguridad Informática del DataCenter de la Escuela Politécnica el Ejército, Sangolquí-Ecuador, 2011.