Diseño del modelo de gestión de seguridad de la información del sistema ERP de EP PETROECUADOR de acuerdo a norma ISO/IEC 27002 y COBIT 5

Alejandro Sebastián Mera Balseca

Departamento de Eléctrica y Electrónica; Escuela Politécnica del Ejército, Sangolquí Ecuador
alejoseb@gmail.com

Resumen: El presente artículo propone un modelo de gestión de seguridad de la información para el sistema ERP[1] de EP PETROCUADOR, basado en el marco de trabajo COBIT 5 y la norma ISO/IEC 27002, para optimizar los procesos empresariales implementados y obtener el mayor beneficio de la plataforma tecnológica adquirida. La caracterización del modelo se realizó identificando la información crítica del sistema y sus amenazas mediante la metodología de análisis de riesgo MAGERIT[2]; analizando información de la normativa interna de la empresa, informes de hacking ético, recomendaciones de consultoría, servicios de TI[3], acuerdos ministeriales, entre otros documentos; logrando describir el estado del arte de la seguridad de la información de EP PETROECUADOR y su relación con las metas corporativas del sistema ERP. Los hallazgos más importantes están relacionados con el nivel de riesgo de la plataforma tecnológica de la empresa, la falta de políticas especializadas, las amenazas de la información del ERP y la manera en que COBIT 5 puede ser utilizado como un marco integrador para el gobierno y gestión de TI bajo un esquema de seguridad de la información, complementado con otros marcos o manuales de buenas prácticas en función de las necesidades de la empresa y de sus partes interesadas.

Palabras clave: *COBIT 5, ISO/IEC 27002, ERP (Enterprise Resource Planning), EP PETROECUADOR, seguridad de la información.*

Abstract: This article proposes a managing model for information security for the EP PETROCUADOR'S ERP system, based on the COBIT 5 framework and ISO / IEC 27002, to optimize business processes and to get the most benefit from the acquired technology platform. The characterization of the model was performed identifying the critical system information and threats by MAGERIT risk analysis methodology; analyzing information of internal company regulations, ethical hacking reports, consultancy recommendations, IT services, ministerial agreements, among other documents; managing to describe the state of the art of information security of EP PETROECUADOR and its relationship with the corporate goals of the ERP system. The most important findings are related to the risk level of the technological platform of the company, the lack of specialized policies, threats of ERP'S information and how COBIT 5 can be used as an integrating framework for the government and IT management under a scheme of information security, complemented with

[1] ERP: Enterprise Resource Planning

[2] MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

[3] TI: Tecnologías de la Información

other frameworks or manual of good practices based on the needs of the company and its stakeholders.

I. Introducción

El modelo de gestión de seguridad de la información es un conjunto de políticas, procesos, procedimientos, controles y estructuras organizacionales basado en marcos de referencia, estándares y buenas prácticas, que permitirá a EP PETROECUADOR conocer los riesgos de la S-I[4], asumirlos, minimizarlos y gestionarlos de una forma documentada, sistemática, estructurada, continua, eficiente y adaptada a los cambios o necesidades que se presenten (ISO/IEC, 2005). Su estudio se llevó a cabo debido a que la normativa interna de EP PETROECUADOR no evidencia un modelo completo de gestión de S-I que esté acorde con las necesidades de protección de la información de los procesos implementados en el sistema ERP, exponiendo a la empresa a riesgos relacionados con la indisponibilidad del sistema, fuga de información, duplicidad de tareas, retraso en procesos contractuales y pérdida de la imagen institucional.

La caracterización de este modelo se realizó mediante una investigación descriptiva del estado del arte de la S-I en EP PETROECUADOR, utilizando técnicas documentales que permitieron recopilar y analizar temas relacionados con la normativa de procesos, informes de hacking ético, consultorías, estructura organizacional y análisis de riesgo del sistema ERP; para definir una línea base sobre la cual es establezca un modelo de gestión de S-I completo y personalizado. La priorización y simplificación del modelo basado en COBIT 5 e ISO/IEC 27002, se realizó utilizando las metas corporativas que la empresa planteó con la implementación del sistema ERP como proyecto estratégico, de esta manera se logró que las metas de TI soporten las metas corporativas y los intereses de las partes interesadas, evitando elaborar marcos desenfocados o demasiado extensos.

Los resultados obtenidos en esta investigación revelan, un marco de gestión incompleto, nivel de riesgo alto de la plataforma tecnológica de EP PETROECUADOR, así como riesgos importantes relacionados sobre todo con amenazas internas. En el ámbito de la propuesta del modelo de gestión se verificó la necesidad del involucramiento de la alta gerencia en todas las iniciativas empresariales relacionadas con la S-I, así como se determinó la importancia de un modelo de gestión de S-I, como complemento clave de un proyecto estratégico, que contemple no solo aspectos técnicos sino también estructurales, de cultura organizacional, comportamiento y habilidades del personal involucrado.

El contenido de este artículo se encuentra organizado de la siguiente manera: La sección II describe los métodos e insumos tomados en cuenta para adaptar COBIT 5 según las metas corporativas del sistema ERP de EP PETROECUADOR y las buenas prácticas descritas en ISO/IEC27002. La sección III presenta y discute los resultados más relevantes de la investigación relacionados con los riesgos de la plataforma tecnológica y la propuesta del modelo de gestión de S-I. La sección IV presenta las conclusiones de la presente investigación que se pueden considerar para trabajos futuros o relacionados.

II. Metodología

A. El sistema ERP de EP PETROECUADOR

Los sistemas ERP son soluciones de software que integran y automatizan varios de los procesos y actividades del negocio de una empresa. La misión principal de un ERP es recolectar y poner a disposición de los usuarios del sistema información actualizada del

[4] S-I: Seguridad de la información

estado y actividades de los departamentos de una empresa. Son herramientas que por su naturaleza gestionan grandes cantidades de información de forma eficiente, reduciendo los costos generales de operación; y a un nivel gerencial, pueden apoyar en la toma de decisiones estratégicas.

El sistema ERP implementando en EP PETROECUADOR corresponde al conjunto de aplicaciones E-Business Suite 12.3 de Oracle Corporation, y forma parte de los proyectos tecnológicos implementados dentro del proceso de modernización y cambio del modelo de gestión, que está llevando a cabo la empresa. Las metas corporativas que se han planteado con la implementación del sistema ERP, son las siguientes:

- Integrar la información administrativa
- Alcanzar la gestión eficiente
- Mejorar el control de la empresa

Figura 1 Módulos del ERP Oracle E-Business Suite (EP PETROECUADOR, 2013)

B. Estado del arte de la S-I de EP PETROECUADOR

Los insumos para la definición del estado del arte de la S-I, fueron obtenidos mediante la recopilación de documentos relacionados con la normativa interna de la empresa, regulación relevante para empresas públicas, informes de hacking ético, consultorías y catálogo de servicios. Cada insumo fue revisado, categorizado y sintetizado, con el objeto de extraer información relacionada con la S-I de la empresa y los métodos de gestión. En algunos casos, fue posible obtener valores cualitativos sobre el nivel de riesgos de la plataforma tecnológica al comparar las vulnerabilidades detectadas en equipos de la empresa con el CVSS[5]. Para el caso de la normativa interna, se verificó la existencia de otros marcos de referencia, o

[5] CVSS: Sistema de Calificación de Vulnerabilidades Comunes

estándares relacionados, así como políticas, procesos y procedimientos de gestión para las TI.

Para describir los riesgos específicos relacionados con el sistema ERP, se realizó la identificación de información crítica de los procesos de Abastecimientos, Manufactura y Finanzas implementados en la primera fase de este proyecto. Esta información fue obtenida mediante reuniones de trabajo mantenidas con los líderes de cada proceso; en donde los puntos claves analizados fueron los siguientes:

- Transacciones (compras, aprobaciones, actualizaciones)
- Necesidades de auditoría
- Nivel de acceso
- Confidencialidad de la información
- Encriptación de campos de base de datos para ambiente de producción y backups.

La información recopilada fue categorizada y agrupada en función de parámetros comunes como módulos del sistema ERP, fechas de ejecución de cambios y usuarios de sistema; para finalmente realizar un análisis cualitativo de riesgos utilizando la metodología MAGERIT.

La elección de la metodología MAGERIT para el análisis de riesgos se basó en los siguientes parámetros: total compatibilidad con COBIT 5 al estar basada en ISO 31000[6], uso y acceso libre a toda la documentación en varios idiomas (español, inglés e italiano), contenido actualizado (versión 3 año 2012), cuenta con el respaldo del Ministerio de Hacienda y Administraciones Públicas del gobierno de España.

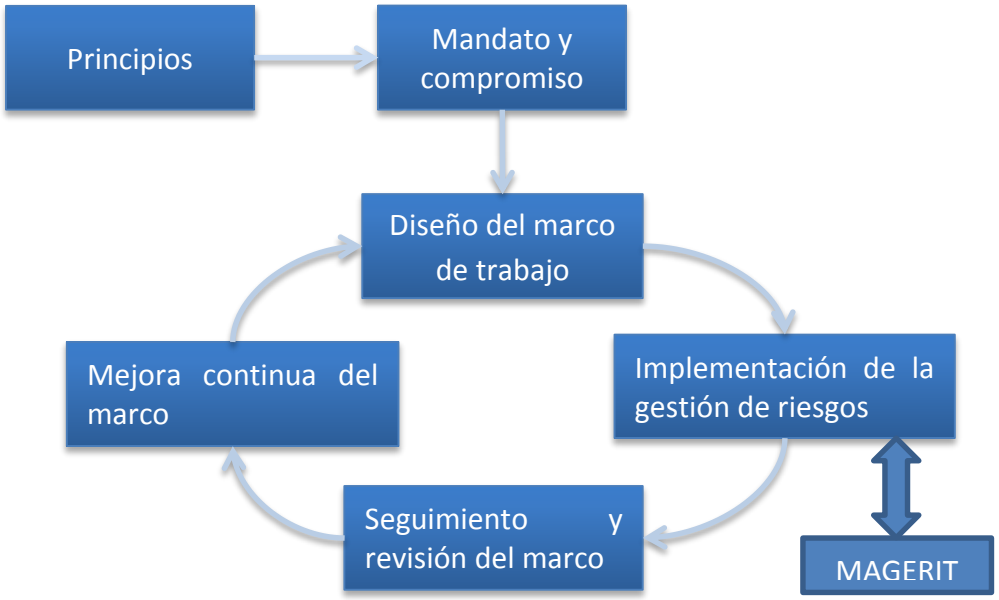

Figura 2 MAGERIT y el marco de gestión de riesgos ISO 31000 (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

C. Marco de referencia y estándares

COBIT 5 es un marco de trabajo integral para el gobierno y gestión de las TI corporativas. Tiene como objetivo principal, ayudar a las empresas a generar el valor óptimo desde las TI manteniendo el equilibrio entre los beneficios, la optimización de los niveles de riesgo y el uso de recursos. (ISACA, 2012). Su evolución lo ha transformado desde un marco de

[6] ISO 31000: Grupo de normas relacionadas con la gestión de riesgos.

auditoría hasta un marco principal de gobierno corporativo, aceptado ampliamente en la industria de TI. Está basado en los más recientes marcos y normas relevantes, tales como ISO 9000[7], ISO/IEC 38500[8], ITIL[9], ISO/IEC 27002, PMBOK[10]; lo que permite utilizar COBIT 5 como un marco integrador único, bajo el cual es posible alinear otros estándares para describir áreas discretas que son tratadas con más detalle.

Bajo el criterio antes mencionado, ISO/IEC 27002 proporciona una guía de buenas prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información (ISO/IEC, 2005), lo que facilita su integración con el marco COBIT 5 complementándolo según las necesidades de cada empresa.

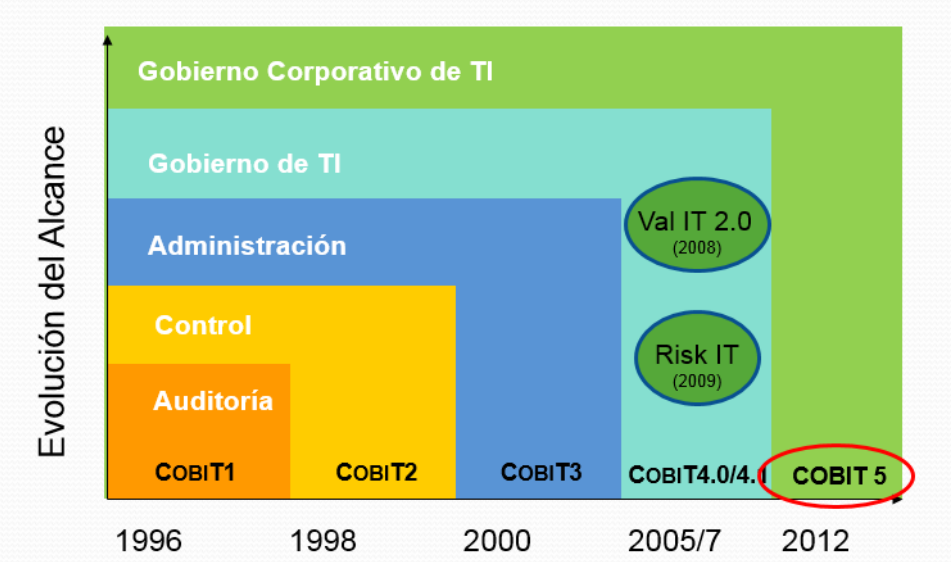

Figura 3 Evolución del marco de referencia COBIT (ISACA, 2012)

D. Simplificación del marco de referencia

Para el caso de esta investigación, el modelo de gestión de seguridad de la información fue caracterizado utilizando los 7 catalizadores y la cascada de metas definidos en el marco COBIT 5. Este enfoque permite simplificar el marco principal utilizando las metas corporativas del sistema ERP de EP PETROECUADOR como punto de partida; para luego traducir estas metas a metas de TI, las cuales, en el mismo sentido, se soportan en las metas de cada uno de los catalizadores.

Es importante aclarar que cada catalizador fue complementado utilizando ISO/IEC 27002, de acuerdo a las características del estado del arte de la S-I de EP PETROECUADOR (normativa interna, vulnerabilidades de plataforma tecnológica, riesgos del sistema ERP) concentrándose específicamente en los siguientes dominios:

- Política de seguridad
- Gestión de comunicaciones y operaciones

[7] ISO 9000: Grupo de normas relacionadas con la calidad y la gestión de la calidad.

[8] ISO 38500: Norma relacionada con el gobierno de TI. Proporciona un marco para evaluar, dirigir y monitorear las TI.

[9] ITIL: Information Technology Infrastructure Library, por sus siglas en inglés, es un conjunto de conceptos y prácticas para la gestión, desarrollo y operación de las TI.

[10] PMBOK: Project Management Body of Knowledge, por sus siglas en inglés, constituye la guía de buenas prácticas para la gestión de proyectos publicada por el Project Management Institute.

- Adquisición, desarrollo y mantenimiento de sistemas de información

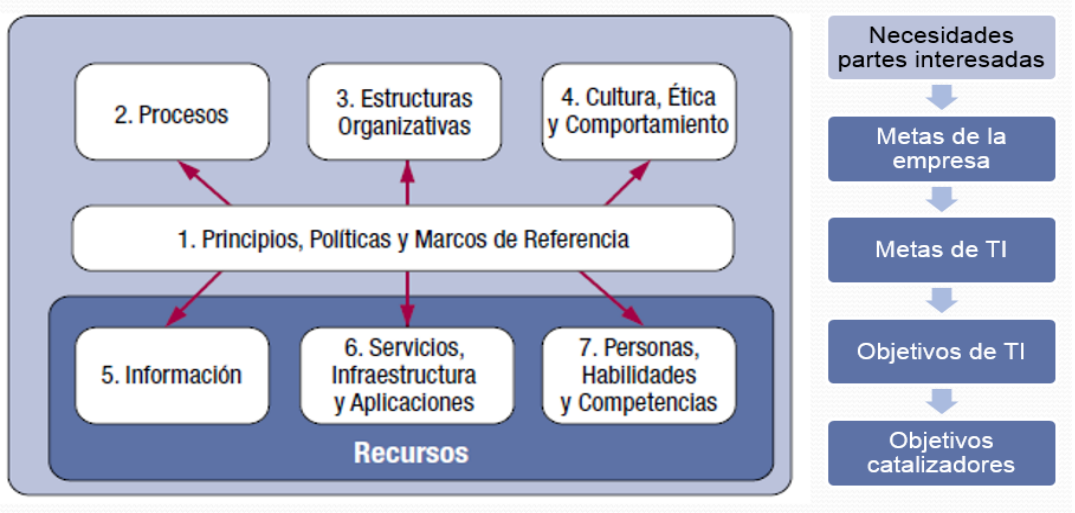

Figura 4 Catalizadores y cascada de metas COBIT 5 (ISACA, 2012)

III. Evaluación de resultados y discusión

A. Normativa interna

La normativa interna de EP PETROECUADOR relacionada con las TI cuenta con 26 procesos aprobados de acuerdo a la versión 4.1 de COBIT; por tanto, mantiene la organización de los procesos de nivel 1 dentro de los 4 dominios de esta versión de COBIT de la siguiente manera:

- Planear y Organizar TIC (PO)
- Adquirir e Implantar TIC (AI)
- Entregar y Dar Soporte de TIC (DS)
- Monitorear y evaluar TIC (ME)

B. Nivel de riesgo de la plataforma tecnológica de EP PETROECUADOR

Los informes de hacking ético, para pruebas internas y externas se resumen en los siguientes gráficos:

Figura 5 Pruebas externas hacking ético

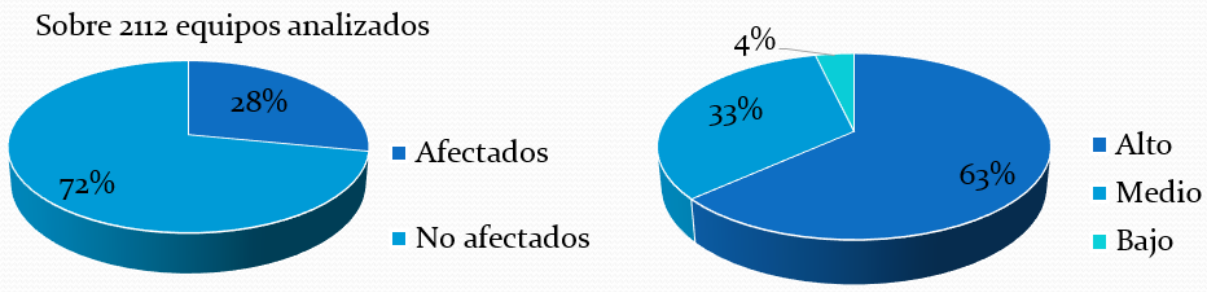

Figura 6 Pruebas internas de hacking ético

Las vulnerabilidades reportadas ubican a la plataforma tecnológica de EP PETROECUADOR en un nivel de riesgo alto, de acuerdo a los criterios del CVSS. Por ejemplo, la vulnerabilidad CVE-2011-1541, detectada en algunos servidores, tiene una calificación CVVS de 10 puntos y está relacionada con ataques remotos que evitan las restricciones de acceso previstos, y por lo tanto permite ejecutar código arbitrario a través de vectores desconocidos.

C. Análisis de riesgo del sistema ERP

El análisis cualitativo de riesgo (función de impacto y probabilidad de ocurrencia) identificó un total de 43 amenazas, las cuales demostraron una relación inversa entre la probabilidad de ocurrencia y su impacto.

Adicionalmente, se identificó que las amenazas con mayor impacto están relacionadas con la modificación deliberada de información por parte de los usuarios del sistema, solamente comparable con el impacto de las amenazas identificadas como desastres naturales. En la Figura 7 se muestra la frecuencia del nivel de riesgo identificado para el sistema ERP.

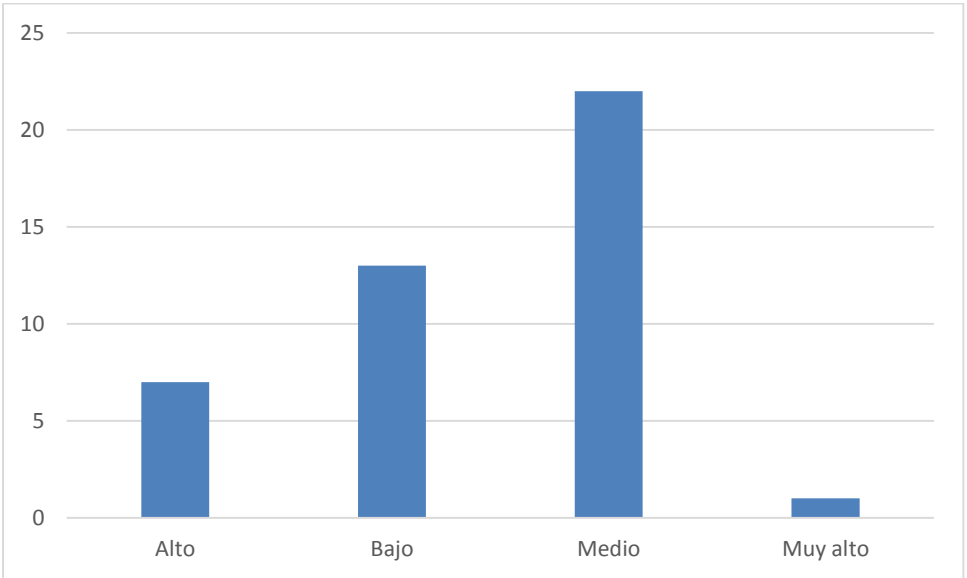

Figura 7 Frecuencia del riesgo del ERP EP PETROECUADOR

D. Propuesta del modelo

La propuesta del modelo de gestión de seguridad de la información considera los 7 catalizadores de COBIT 5, sin embargo de acuerdo al estado del arte de la S-I de EP PETROECUADOR los aspectos más importantes de los catalizadores se puede resumir de la siguiente manera:

- Política y principios: incluye definiciones para el uso del marco de referencia, responsabilidades, obligaciones y sanciones. En relación directa con la función seguridad se debe considerar el control de acceso, S-I de personal y la respuesta a incidentes. Las funciones dependientes están relacionadas con la gestión de comunicaciones, la adquisición y desarrollo de software.
- Los procesos priorizados en función de las metas corporativas y el marco de referencia COBIT 5 son:
    - EDM: EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno, EDM02 Asegurar la entrega de beneficios, EDM03 Asegurar la optimización de riesgos.
    - BAI: BAI01 Gestionar programas y proyectos, BAI02 Gestionar definiciones de requerimientos, BAI06 Gestionar los cambios
    - DSS: DSS05 Gestionar servicios de seguridad
    - APO: APO01 Gestionar el marco de gestión de TI, APO02 Gestionar el marco de gestión de TI, APO03 Gestionar la estrategia, APO07 Gestionar los recursos Humanos, APO08 Gestionar las Relaciones, APO12 Gestionar El riesgo, APO13 Gestionar la seguridad
    - MEA: MEA01 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.
- Estructuras: se propone un cambio a la estructura organizacional del área de seguridad acuerdo a la Figura 8, en la cual el área de seguridad mantiene alineamiento con las iniciativas de TI, pero evita que sus actividades se solapen por actividades puramente técnicas.

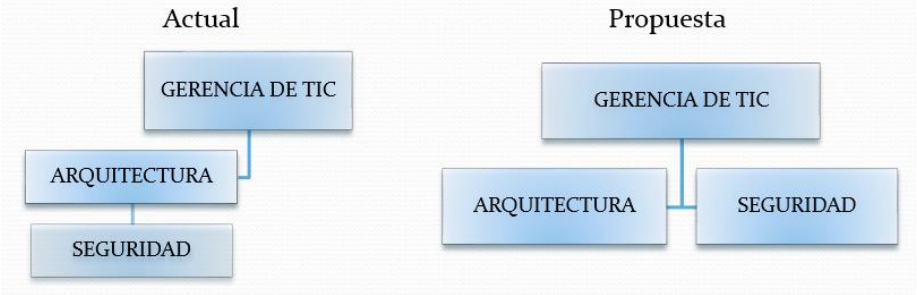

Figura 8 Estructura organizacional propuesta

- Servicios, infraestructura: Los servicios recomendados a implementar deben incluir seguridad de arquitectura, concienciación de seguridad, desarrollo seguro y configuración de sistemas. Cada servicio debe estar caracterizado mediante acuerdos (SLA) que permitan su verificación y evaluación.
- Cultura, ética y comportamientos: Comprende dos aspectos fundamentales, las actividades relacionadas con una cultura de S-I que influencie en las actitudes y comportamientos del personal, y el liderazgo relacionado con agentes de cambio o personal estratégico que demuestre la importancia de la S-I en la empresa; este último punto está estrechamente relacionado con el compromiso y apoyo de la alta gerencia.
- Gente habilidades y competencias: Asegura que se toman decisiones correctas y que todas las actividades relacionadas con la S-I son completadas satisfactoriamente. Se definen principalmente 2 roles encargados de la S-I empresarial, el jefe de seguridad de la información y el analista de seguridad e la información, encargados de aspectos estratégicos y el control del cumplimiento de las políticas y normas, respectivamente.

E. Discusión

Los resultados de esta investigación y la propuesta del modelo de gestión de seguridad de la información para el sistema ERP, no pueden ser considerados como reglas generales o resultados definitivos que puedan ser replicados en cualquier empresa o proyecto, debido a que los insumos considerados para su diseño son limitados a la información obtenida de EP PETROECUADOR, las metas estratégicas que se han planteado para el sistema ERP y de manera especial a la relativa importancia que cada empresa puede dar a su información. Sin embargo, el principal aporte de esta investigación se ve reflejado en el uso de COBIT 5, no solamente como un marco de referencia de procesos, sino más bien como un medio para potenciar un proyecto estratégico mediante el gobierno corporativo de TI, basado en el análisis de riesgo, la protección y uso adecuado de uno de los activos más importantes de una organización "La información". Esta característica difiere claramente de los enfoques de versiones anteriores de COBIT (3, 4, 4.1), en los cuales el principal punto de análisis se centraba en los procesos, dejando el análisis y gestión de riesgo para que sea tratado mediante otro marco de referencia con sus propios procesos.

Por otro lado, los métodos de análisis presentados cuentan con una amplia aceptación en la industria de TI, debido a que están respaldados por varios estándares, y marcos de referencia; esta característica facilita que su utilización sea repetible en otros ambientes o empresas adaptándolos según sus propias necesidades.

IV. Conclusiones

EP PETROECUADOR requiere un sistema de gestión de seguridad de la información personalizado en función de sus metas corporativas, que le permita minimizar los riesgos mientras se optimiza los beneficios de sus inversiones en TI.

COBIT 5 e ISO/IEC 27002 pueden ser usados para el diseño de un modelo de gestión de seguridad de la información que establezca directrices que soporten las metas corporativas o de negocio basado en mejores prácticas ampliamente aceptadas por la industria de TI.

El éxito de toda iniciativa de aseguramiento de la información está relacionado con el apoyo y compromiso de la alta gerencia, quienes deben tener la capacidad de incluir las necesidades de todas las partes interesadas, para que sean atendidas.

La cascada de metas, definida en COBIT 5, permite caracterizar un modelo de gestión de S-I basado en: políticas, procesos, estructura organizativa, cultura organizacional, información, servicios-infraestructura y personas con sus habilidades, trasladando las metas corporativas a metas de TI.

Los beneficios del modelo de gestión de seguridad de la información relacionados con los procesos implementados en el sistema ERP son:

- Cumplimiento con requerimientos de normativa y regulación
- Reconocimiento y protección de información crítica de los procesos
- Facilidad para tareas de auditoría
- Definición de roles y responsabilidades
- Segregación de tareas
- Mantenimiento de la imagen empresarial

Investigaciones futuras pueden centrarse en definir subprocesos y procedimientos que complementen cada uno de los catalizadores, para que el modelo de gestión sea la herramienta de consulta principal que cubra todos los aspectos de gestión de la S-I de la empresa

Referencias bibliográficas

Barrazueta, P. (10 de 02 de 2012). *Universidad Técnica Particular de Loja*. Obtenido de sitio Web de la Universidad Técnica Particular de Loja: http://www.utpl.edu.ec/comunicacion/2012/02/proyecto-de-seguridad-de-la-informacion-utpl-supertel/

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

EP PETROECUADOR. (09 de 08 de 2011). *Normativa de Gestión de EP PETROECUADOR (v11).* Obtenido de http://normativa.eppetroecuador.ec:8080/web/guest/home/

EP PETROECUADOR. (10 de 02 de 2013). *EP PETROECUADOR*. Obtenido de Portal de EP PETROECUADOR: http://www.eppetroecuador.ec/Empresa/ResenaHistorica/index.htm

ISACA. (2012). *COBIT 5 for Information Security.* Rolling Meadows, IL: ISACA.

ISACA. (2012). *COBIT 5 Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* Rolling Meadows: ISACA.

ISO. (2009). Risk management — Principles and Guidelines. En ISO, *Risk management — Principles and Guidelines* (págs. 1,2).

ISO/IEC. (2005). ISO/IEC 27002. En ISO/IEC, *Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.*

ISO27000.ES. (01 de 02 de 2013). *ISO27000.ES, El portal de ISO 27001 en español*. Obtenido de ISO27000.ES: http://www.iso27000.es/sgsi.html

McAfee. (2013). *The Economic Impact of Cybercrime and Cyber Espionage.* Santa Clara, CA: McAfee.

Meyer, C. O. (22 de 10 de 2008). *ISO 27000.ES.* Obtenido de http://www.iso27000.es/download/seguridad%20informaticavsinformacion.pdf

MITRE. (21 de 06 de 2013). *Acerca CVE.* Obtenido de http://cve.mitre.org/about/

Oracle Corporation. (22 de 05 de 2013). *Portal de Oracle Corporation.* Obtenido de http://www.oracle.com/technetwork/apps-tech/ebs-techstack-roadmap-apr-2013-1940074.pdf

OWASP Foundation. (2008). *OWASP testing manual V3.* OWASSP. Obtenido de Portal de la Fundación OWASP : https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf

Ponemon Institute. (2012). *2013 State of the Endpoint.* Ponemon Institute.

Roessing, R. M. (2010). *The Business Model For Information Security.* ISACA.

Secretaría Nacional de la Administración Pública. (2013). Esquema gubernamental de la seguridad de la información (EGSI). Quito, Ecuador.

SUPERTEL. (2012). Desarrollo del Proyecto de Implementación del CERT. *Revista Institucional*(13), 6-13.

Tobón, S. (2008). La formación basada en competencias en la educación superior. Bogotá: Instituto Cife.

Tori, C. (2008). Hacking Ético. *Hacking Ético*. Rosario, Argentina: Carlos Tori.

Vacca, J. R. (2009). Computer and Information Security. En C. a. Handbook. Morgan Kaufmann.