ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRIA EN GERENCIA DE REDES Y TELECOMUNICACIONES

V PROMOCIÓN

TESIS DE GRADO

TEMA: "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"

AUTOR: MERA, ALEJANDRO SEBASTIÁN

DIRECTOR: BALDEÓN, MAURICIO JAVIER

SANGOLQUÍ, ENERO DEL 2014

UNIVERSIDAD DE LAS FUERZAS ARMADAS

MAESTRÍA EN GERENCIA DE REDES Y TELECOMUNICACIONES

CERTIFICAMOS

Que el trabajo titulado "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", realizado por el Ing. Alejandro Sebastián Mera Balseca, ha sido guiado y revisado periódicamente, y cumple las normas estatutarias establecidas en el reglamento de estudiantes de la Universidad de las Fuerzas Armadas.

Sangolquí, 07 de enero de 2014

_____	_____
Ing. Mauricio Baldeón MGS.	Ing. Fausto Granda MsC.
DIRECTOR	OPONENTE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

MAESTRÍA EN GERENCIA DE REDES Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, ING. ALEJANDRO SEBASTIÁN MERA BALSECA

DECLARO QUE:

El proyecto de grado denominado "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", ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan en el pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, 07 de enero de 2014

_____

Ing. Alejandro Mera B.

UNIVERSIDAD DE LAS FUERZAS ARMADAS

MAESTRÍA EN GERENCIA DE REDES Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, ING. ALEJANDRO SEBASTIAN MERA BALSECA, autorizo a la Universidad de las Fuerzas Amadas, la publicación en la Biblioteca Virtual de la Institución, de la tesis: "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" cuyo contenido, ideas y criterio son de mi exclusiva responsabilidad y autoría.

Sangolquí, 07 de enero de 2014

_____

Ing. Alejandro Mera B.

DEDICATORIA

A mis padres, quienes me han brindado el calor de un hogar y el ejemplo para conseguir mis objetivos con dedicación y esfuerzo.

AGRADECIMIENTO

A mis padres y hermanos por su apoyo incondicional en todas mis actividades laborales y académicas.

A mi tutor, Mauricio Baldeón por sus consejos y crítica constructiva en la realización de esta tesis.

A las autoridades, compañeros y amigos de EP PETROECUADOR por el soporte administrativo y técnico.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

La presente investigación propone un modelo de gestión de seguridad de la información para el sistema ERP 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; analizando información de la normativa interna de la empresa, informes de hacking ético, recomendaciones de consultoría, servicios de TI, 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: seguridad de la información, COBIT 5, ISO/IEC 27002, ERP (Enterprise Resource Planning), EP PETROECUADOR.

ABSTRACT

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

Key words: information security, COBIT 5, ISO/IEC 27002, ERP (Enterprise Resource Planning), EP PETROECUADOR.

1 Capítulo I Introducción

1.1 Justificación e importancia.

Debido a la presencia de las TIC[1] en casi todos los aspectos de la vida moderna, es fácil reconocer que estas tecnologías han transformado la forma en que las personas realizan sus actividades diarias estableciendo nuevas reglas de juego en aspectos como la salud, educación, comunicación, gobierno, negocios, entre otros. Una de las características principales de esta transformación, es la gestión[2] automatizada de grandes cantidades de información, lo que a su vez trae como consecuencia la imperativa necesidad de asegurar dicha información como uno de los activos más importantes de todo ente organizativo.

Bajo este contexto, la S-I[3] ha tomado relevancia tanto en ámbitos empresariales como académicos y ha sido objeto de varias investigaciones que tratan de describir los aspectos tecnológicos, sociales, regulatorios y demográficos que influyen en la seguridad; formando bases de conocimiento y definiendo marcos de referencia orientados a que los riesgos de la S-I sean conocidos, asumidos, minimizados y gestionados por las organizaciones de una forma documentada, sistemática, estructurada, continua, eficiente y adaptada a los cambios que se produzcan (ISO27000.ES, 2013).

Proteger información valiosa y sensible, se ha convertido en algo esencial para la sostenibilidad de una empresa; por tanto, un manejo inapropiado de los riesgos

---

[1] TIC: Tecnologías de la Información y Comunicación

[2] Gestión: En este contexto se refiere a la creación, modificación, transmisión, almacenamiento y explotación de información.

[3] S-I: Seguridad de la Información

asociados con las TI[4], por falta o mal diseño de un SGSI[5] que gestione la información como uno de los activos más importantes, podría afectar directamente la rentabilidad o incluso disminuir el valor general de la empresa. En consecuencia, varias son las empresas que a nivel mundial han incluido un SGSI en sus organizaciones, y en el ámbito local las empresas Telconet y Telefónica Movistar han obtenido certificaciones de sus Sistemas de Gestión Seguridad de la Información bajo la Norma ISO 27001, como un medio para fortalecer su posicionamiento en el mercado estableciendo una ventaja competitiva.

Para el caso de EP PETROECUADOR, la implementación del sistema ERP[6] como parte de las iniciativas tecnológicas de modernización, representa un cambio profundo en los procesos y actividades de negocio de la empresa; generando ventajas operativas mediante la gestión eficiente de información y la reducción de los costos generales de operación. Estas ventajas operativas, por si solas, no representan una garantía de éxito en el proceso de modernización de la empresa, en este sentido los modelos de gestión de S-I son complementos claves que potencian los beneficios de las TIC brindando soporte a las metas corporativas, minimizando los riesgos asociados con la nueva plataforma tecnológica y garantizando la confidencialidad, integridad y disponibilidad de la información bajo la utilización de estándares y buenas prácticas normalmente aceptadas. En el aspecto regulatorio, el modelo de gestión de S-I permitirá que EP PETROECUADOR se encamine hacia el cumplimiento del acuerdo ministerial No. 166 del 19 de septiembre de 2013, publicado por la Secretaría Nacional

[4] TI: Tecnologías de la Información

[5] SGSI: Sistema de Gestión de Seguridad de la Información

[6] ERP: Sistema de Planificación de Recursos Empresariales, o Enterprise Resource Planning por sus siglas en inglés

de Administración Pública; dicho acuerdo dispone a las entidades de la Administración Pública Central, Institucional y que dependan de la Función Ejecutiva el uso obligatorio de las normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información. Cabe aclarar que este acuerdo, además de reconocer la importancia de mantener la seguridad en la información que se genera y custodia en las entidades de la Administración Pública, forma parte de los proyectos de estandarización de procesos y calidad impulsados por la Secretaria Nacional de administración pública, para optimizar el uso de las TIC en el cumplimiento de la gestión institucional e interinstitucional.

1.2 Planteamiento del problema.

La normativa interna de EP PETROECUADOR, relacionada a la S-I, no evidencia un conjunto completo de políticas estructuradas que se ajusten a estándares internacionales y que contemplen las necesidades específicas del sistema ERP; por tanto, el soporte que este sistema brinda a los procesos operativos y administrativos de la empresa puede verse afectado por los siguientes inconvenientes:

- Indisponibilidad del sistema por tareas de mantenimiento o eventos no programados.
- Duplicidad en tareas de respaldo o administración de la plataforma.
- Perdida de información.
- Acceso o fuga de información sensible por medios no establecidos.
- Retraso en los procesos y responsabilidades contractuales.
- Pérdida de la imagen institucional ante proveedores, entidades públicas y organismos de control.
- Pérdida de confianza en la plataforma tecnológica y en la gestión de la Subgerencia de Tecnologías de la Información y Comunicación.

- Incapacidad de remediar de forma sistemática las vulnerabilidades, detectadas por consultorías externas, en la plataforma tecnológica de la empresa.
- Incapacidad de identificar y minimizar los riesgos relacionados con las tecnologías de la información.

1.3 Formulación del problema a resolver.

Las preguntas de investigación planteadas son las siguientes:

¿Puede la falta de un modelo de gestión de S-I poner en riesgo los procesos empresariales soportados por el sistema ERP de EP PETROECUADOR?

¿Qué relación existe entre la falta de un modelo de gestión de S-I y las vulnerabilidades de la plataforma tecnológica de EP PETROECUADOR?

¿Facilitan las políticas de S-I la gestión eficiente de la información de los procesos implementados en el sistema ERP de EP PETROECUADOR?

1.4 Hipótesis.

La Subgerencia de Tecnologías de Información y Comunicación requiere de un modelo de gestión de S-I alineado a mejores prácticas y estándares internacionales los cuales influirán positivamente en la optimización de los procesos empresariales implementados en el sistema ERP de EP PETROECUADOR.

1.5 Objetivo General.

Diseñar un modelo de gestión de S-I, utilizando el estándar ISO/IEC 27002 y el marco de trabajo COBIT [7] 5, para facilitar la optimización de los procesos empresariales implementados en el sistema ERP de EP PETROECUADOR.

1.6 Objetivos Específicos.

[7] COBIT: Objetivos de Control para Información y Tecnologías Relacionadas, Control Objectives for Information and related Technology, por sus siglas en inglés.

- Describir el estado de la normativa de gestión y de procesos de EP PETROECUADOR relacionada con la S-I.
- Analizar la relación y aplicabilidad, de manera conjunta, de la norma ISO 27002 y el marco de trabajo COBIT 5 en un sistema de gestión de S-I.
- Elaborar una propuesta para el modelo de gestión de S-I del sistema ERP de EP PETROECUADOR.
- Determinar la forma en que los procesos empresariales implementados en el sistema ERP se beneficiarán de un modelo de gestión de S-I.

1.7 Alcance

La presente investigación complementa las definiciones del subproceso "GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS", perteneciente al macro proceso "TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES" de la Normativa Interna de EP PETROECUADOR, considerando las características propias de los procesos de manufactura, finanzas y abastecimientos implementados en el sistema ERP de EP PETROECUADOR, en su primera fase.

Los siguientes capítulos de esta investigación se encuentran divididos, de forma congruente con el proceso de investigación, de la siguiente manera:

- Capítulo 2 Marco teórico.- Presenta de manera resumida el estado del arte de la S-I, enfocándose en definiciones, aspectos económicos y estadísticas, amenazas actuales, la gestión de riesgos , los modelos de gestión de S-I, el sistema ERP E-Business Suite, el marco de referencia COBIT 5 e ISO/IEC 27002.
- Capítulo 3 Estado del arte de la S-I de EP PETROECUADOR.- Este capítulo brinda información descriptiva de varios aspectos relacionados con la S-I de EP PETROECUADOR, pasando desde una breve

descripción de la cadena de valor de la empresa, la normativa interna y los servicios de TI; hasta el análisis de informes de hacking ético y el análisis de riesgos de S-I para el sistema ERP en función de la información crítica identificada para cada proceso.

- Capítulo 4 Propuesta del Modelo de gestión de seguridad de la información del sistema ERP de EP PETROECUADOR.- Propone un conjunto de políticas, procesos, estructura organizacional, cultura y ética, información, servicios, habilidades y competencias; basadas en COBIT 5 e ISO/IEC 27002 con un enfoque y priorización acuerdo a las metas corporativas del sistema ERP.
- Capítulo 5 Conclusiones y recomendaciones.- Recoge los hallazgos más importantes de la investigación, detallados en los capítulos anteriores, y los sintetiza presentándolos de forma clara y precisa. Se complementa con algunas recomendaciones relacionadas a la gestión y buen.as prácticas aplicables en EP PETROECUADOR

2 Capítulo II Marco Teórico

2.1 Estado del arte

La adopción de las TIC, en todos los niveles de las actividades humanas, ha sido un medio para fomentar la denominada "Sociedad de la Información", en donde los modelos tradicionales de generación de riqueza, representada por productos tangibles, se han trasladado hacia la generación, intercambio y almacenamiento de todo tipo de información; creando nuevas formas y oportunidades de negocio. Este concepto de trasladar valor hacia la información, ha generado gran interés en su aseguramiento y ha provocado que las actividades criminales evolucionen a un ritmo acelerado, adaptándose para explotar las vulnerabilidades de los modelos organizacionales y socioeconómicos que se están formando en base a las TIC.

2.1.1 *El contexto económico del ciber-crimen*

El ciber-crimen, como se ha denominado a las actividades criminales en un ambiente cibernético[8], no difiere en esencia del crimen tradicional; sin embargo, debido a su fondo tecnológico se enfoca principalmente en las transacciones financieras, privacidad, robo de identidad, daño a la reputación, daño a sistemas críticos, terrorismo y otros. Estudios actuales demuestran que el costo de las actividades del ciber-crimen, lo cual incluye pérdidas económicas e inversión en S-I, es comparable a las actividades del tráfico de drogas, accidentes automovilísticos o la piratería, como se muestra en la Figura 1.

[8] CIBERNÉTICO: Creado y regulado mediante computadora u ordenador.

Putting Malicious Cyber Activity in Context			
CRIMINAL ACTION	ESTIMATED COST	PERCENT OF GDP	SOURCE
GLOBAL			
Piracy	$1 billion to $16 billion	0.008% to 0.02%	IMB
Drug Trafficking	$600 billion	5%	UNODC
Global cyber activity	$300 billion to $1 trillion	0.4% to 1.4%	Various
US ONLY			
Car Crashes	$99 billion to $168 billion	0.7% to 1.2%	CDC, AAA
Pilferage	$70 billion to $280 billion	0.5% to 2%	NRF
US- cyber activity	$24 billion to $120 billion	0.2% to 0.8%	Various

Figura 1 Costo estimado del Ciber-crimen global y en EEUU (McAfee, 2013)

Según datos del Banco Central, el PIB[9] del Ecuador para el año 2012 fue de 84,04 billones[10] de dólares, por tanto se puede estimar que las pérdidas económicas por las actividades del ciber-crimen en EEUU podrían representar, comparativamente, desde el 28,05% hasta el 142,79% del total del PIB del Ecuador.

2.1.2 *Las actuales amenazas a la seguridad de la información*

Los estudios realizados en el ámbito de la S-I han determinado que los dispositivos móviles se han convertido en potenciales riesgos para las redes de las organizaciones o los sistemas corporativos. Una de las causas de este fenómeno es el incremento de malware[11] que se ha detectado en este tipo de dispositivos. De acuerdo a los resultados presentados por McAfee Labs para el segundo cuatrimestre de 2013, se han detectado

[9] PIB: Producto Interno Bruto, o GDP por sus siglas en inglés.

[10] BILLÓN: en el contexto de la cita y por uso generalizado en EEUU un billón equivale a 1000 millones y no a $1x10^{12}$ como sería su uso correcto en el Sistema Internacional de Unidades.

[11] MALWARE: término general para referirse a software o pedazos de código malicioso, reconocido como virus, gusano, troyano, etc.

más de 30000 registros de malware nuevo en lo que va del año, siendo Android la plataforma mayormente afectada.

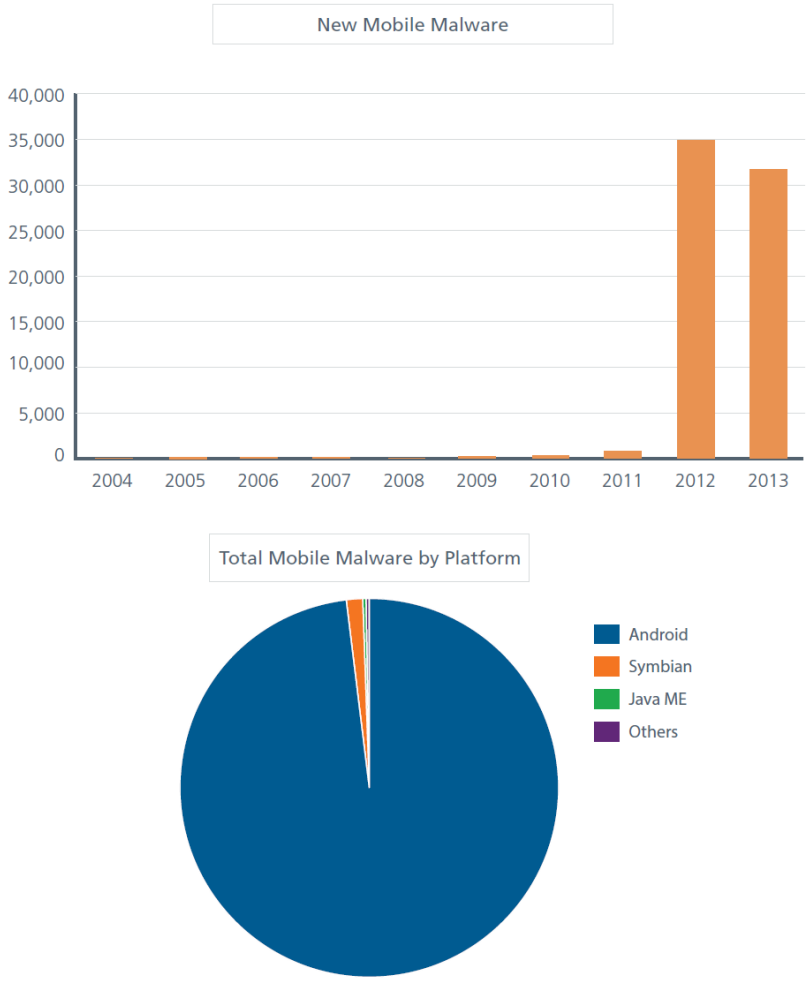

Figura 2 Malware detectado en dispositivos móviles (McAfee Labs, 2013)

Estas cifras se ratifican en estudios realizados por el Ponemon Insitute, los cuales se llevaron a cabo con una muestra representativa de especialistas o personal relacionado con la S-I, en empresas con 1000 o más empleados. El gráfico de la Figura 3 representa en color azul los incidentes más comunes en las organizaciones y en rojo los incidentes que mayores problemas trajeron a la organización; verificándose que el malware es la causa más común de incidentes de seguridad, mientras que los ataques persistentes fueron los que mayores problemas provocaron en las organizaciones.

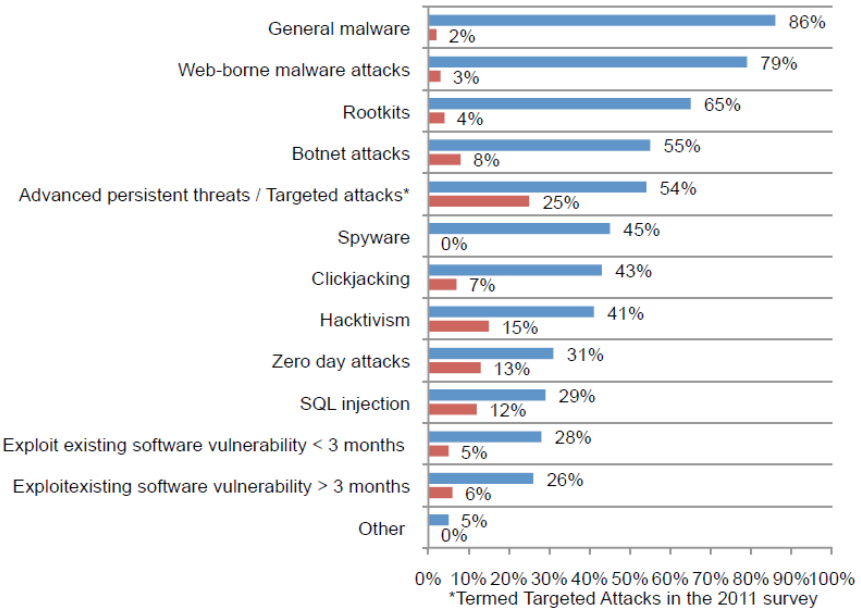

Figura 3 Causas de incidentes frecuentes de S-I (Ponemon Institute, 2012)

El Hacktivismo[12], sin ser un fenómeno nuevo dentro del ambiente cibernético, ha tomado relevancia dentro de las amenazas de la S-I, debido a que esta actividad ha derivado en otros fenómenos más radicales y dirigidos. El caso de Anonymous, aun sin perder protagonismo, ha experimentado un descenso en su visibilidad política, causado por un estancamiento en su sofisticación tecnológica, falta de claridad ideológica y descoordinación en los ataques realizados; sin embargo grupos denominados como "ejércitos cibernéticos" o "Cyberarmies" han aparecido en la escena del hacktivismo, mostrando motivaciones políticas más profundas y en muchos casos declarando total alineamiento y apoyo a gobiernos específicos. Un ejemplo de estos grupos es "The Syrian Electronic Army", alineado con el presidente Bashar al-

[12] HACKTIVISMO: Actividades con fines políticos que utilizan el hacking (redes y sistemas computacionales) como medio de expresión.

Assad, cuyos objetivos de ataque en los primeros meses del 2013 se muestran en la Figura 4.

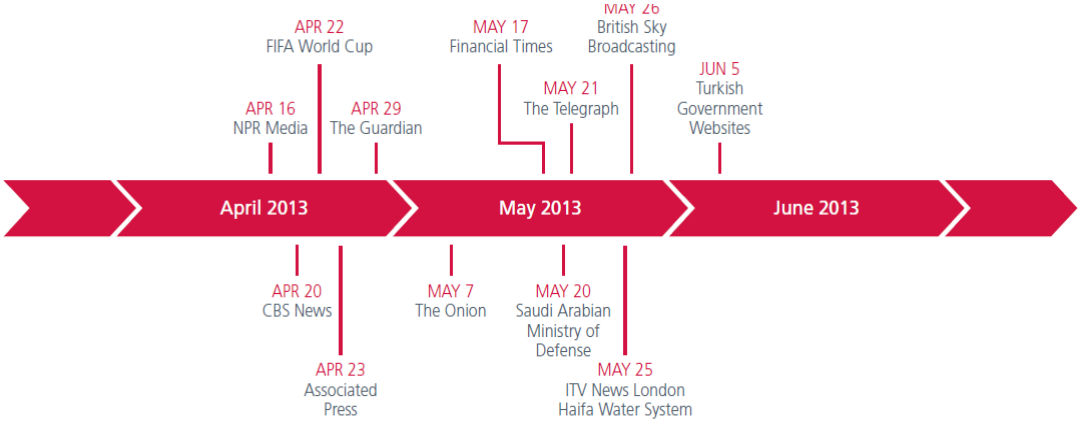

Figura 4 Objetivos de ataque de la Syrian Electronic Armie (McAfee Labs, 2013)

2.1.3 *La seguridad de la información en las empresas*

Las empresas y de forma específica los altos ejecutivos, han reconocido que el aseguramiento y protección de la información es un medio para mantener sus empresas rentables y competitivas. Este acercamiento del alto nivel ejecutivo hacia la S-I ha provocado que los profesionales de seguridad hayan sido obligados a cumplir con marcos de trabajo y estándares fragmentados para actuar de forma reactiva frente a riesgos, amenazas, aspectos culturales y organizativos, legislación cambiante e infracciones o incidentes; sin embargo, este enfoque de seguridad ha dejado de lado el desarrollo de métodos más efectivos para la gestión de la S-I, mediante modelos que estudien todos los factores que provocan incertidumbre y su relación con las necesidades de la empresa.

Aun cuando las empresas han invertido grandes cantidades de dinero en tecnologías de seguridad como firewalls, IDS[13], IPS[14], y de la misma manera se han focalizado aspectos regulatorios o se han incentivado las inversiones para la S-I; no se ha evidenciado una disminución de los incidentes de S-I en una escala equivalente. (Roessing, 2010) Algunas de las causas que pueden explicar este fenómeno apunta a que los profesionales de seguridad siguen actuando de forma reactiva en lugar de implementar soluciones proactivas, una segunda causa estaría relacionada con el comportamiento negligente o la mayor frecuencia de los errores humanos debido al incremento del uso de las TI en los métodos de hacer negocios y una tercera causa es que el uso de las TI se ha vuelto omnipresente en nuestras vidas diarias.

Actualmente los SGSI representan dos aspectos principales para la empresa: el método para proteger la información corporativa y un habilitante para la consecución de los objetivos de negocio. Es por estos aspectos que los enfoques actuales de gestión de S-I, se encuentran integrados dentro del negocio facilitando la aplicación de soluciones estratégicas para la creación de oportunidades y reducción de riesgos. Los enfoques aislados o que no consideran el negocio como un conjunto de elementos integrados y dinámicos, tienden a dar soluciones puntuales minimizando los beneficios de los SGSI.

2.1.1 *La seguridad de la información en el Ecuador*

En el ámbito local, la investigación en el campo de la S-I se ha enfocado en la realización de proyectos conjuntos entre las entidades del estado como la Superintendencia de Telecomunicaciones y centros de educación superior. Estos

[13] IDS: Sistema de Detección de Intrusos

[14] IPS: Sistema de Prevención de Intrusos

proyectos tienen como principales objetivos organizar actividades para facilitar la transferencia de conocimiento y tecnología, así como formar una línea base para determinar los avances en materia de seguridad. (Barrazueta, 2012)

De manera adicional, la Superintendencia de Telecomunicaciones ha impulsado la creación del CERT[15] Ecuador, el mismo que inicialmente tendrá como objetivo proporcionar servicios de respuesta a incidentes a nivel de instituciones del Estado, con énfasis en el apoyo a los entes relacionados en el sector de las telecomunicaciones. (SUPERTEL, 2012)

2.2 La seguridad de la Información.

"La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales" (ISO/IEC, 2005)**.**

Este concepto ubica a la información como uno de los activos comerciales más importantes de una organización, y por tanto su gestión y aseguramiento son aspectos que generan valor para una organización o empresa. A diferencia de la Seguridad Informática, la cual se encarga de los aspectos técnicos y metodológicos para mantener la plataforma de los SI[16] segura, la S-I es más amplia e involucra de forma obligatoria a los líderes de negocio, ejecutivos y directorio, ya que considera adicionalmente los procesos administrativos, operativos y productivos que intervienen en el negocio. (Meyer, 2008)

---

[15] CERT: Centro de Respuesta a Incidentes Informáticos

[16] SI: Sistemas de información

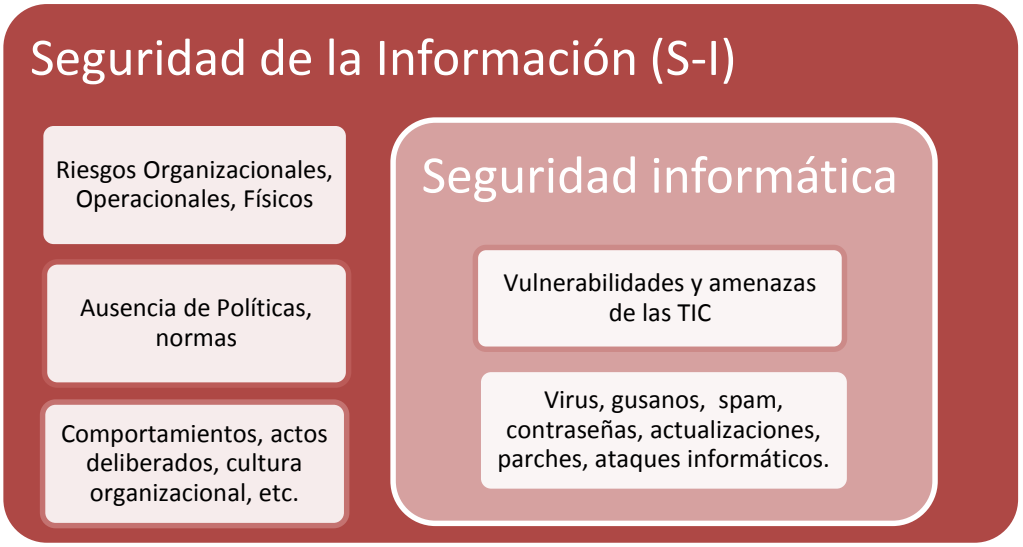

Figura 5 Seguridad de la Información y Seguridad informática (Meyer, 2008)

La S-I, como se detalla en la Figura 6, se sustenta en tres principios: confidencialidad, integridad y disponibilidad (ISO/IEC, 2005); los mismos que todo sistema informático, proceso, medio de almacenamiento, canal de comunicación, entre otros, debe garantizar para ser considerado como seguro.

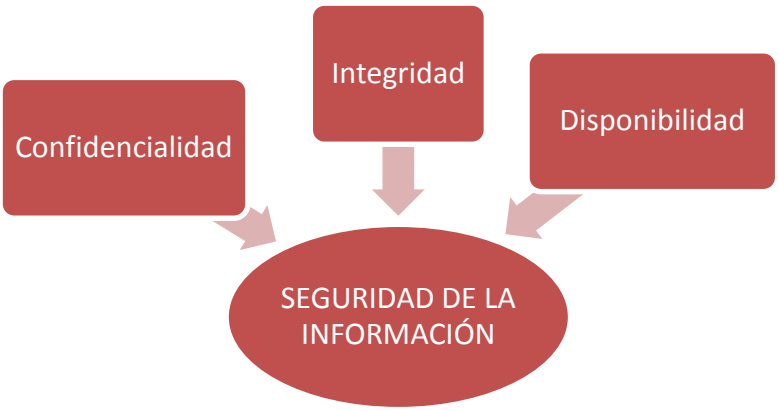

Figura 6 Principios de Seguridad de la Información

2.3 Los Sistemas de Gestión de Seguridad de la Información.

Los SGSI, son un conjunto de políticas, normas, procedimientos y métodos de control que permiten a las organizaciones formar estructuras completas para gestionar la información de forma óptima y segura; los cuales no solamente están limitados a

medidas de seguridad, sino que ofrecen un conjunto completo de esquemas para evaluar, comprender y minimizar los riesgos asociados con las TI.

El modelo de un SGSI, es una descripción esquematizada de dicho sistema que facilita su comprensión, control y uso. Por tanto, necesita ser flexible para cubrir las necesidades del mundo de los negocios, debe estar sometido a evaluaciones periódicas que permitan determinar si se mantiene aplicable o si se ajusta a la finalidad prevista, debe incluir ajustes para mantener su validez a través del tiempo y los cambios de entorno asociados. (Roessing, 2010)

2.4 El riesgo

El riesgo se define como el efecto de la incertidumbre sobre los objetivos empresariales (ISO, 2009). Bajo este contexto, el efecto se considera una desviación positiva o negativa de un resultado esperado, y la incertidumbre como una falta total o parcial de información relacionada con la comprensión o conocimiento de un evento, su probabilidad de ocurrencia y consecuencias.

2.4.1 *La gestión de riesgos*

La gestión de riesgos es un proceso sistemático, que comprende la identificación, análisis y evaluación de riesgos; para determinar si estos deben ser modificados satisfaciendo los criterios de cada organización. Durante la ejecución de este proceso se consulta y comunica a los miembros de la organización, mientras se monitorea y revisa los controles que están modificando el riesgo, hasta que se determina que este ya no necesita más tratamiento.

De acuerdo a la norma ISO 31000, el proceso para la gestión de riesgos, visto desde un enfoque de alto nivel, se muestra en la Figura 7.

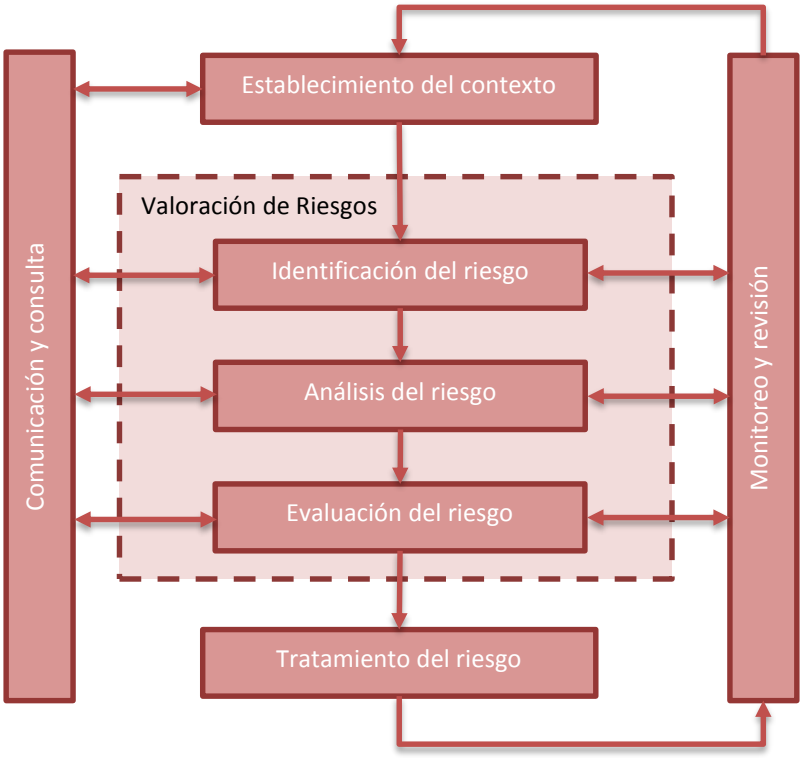

Figura 7 Proceso de Gestión de Riesgos (ISO, 2009)

El proceso de gestión de riesgos, debido a su característica iterativa, puede ser integrado en las fases PDCA[17] de un SGSI; facilitando que el alcance y límite de los controles implementados en estos sistemas cumplan con el requerimiento de ser elaborados bajo un enfoque de riesgos. En la Tabla 1 se muestra como un SGSI y el proceso de gestión de riesgos pueden alinearse bajo un mismo enfoque.

Tabla 1 Alineamiento del SGSI y el proceso de gestión de riesgos (ISO, 2009)

Fases del SGSI	**Proceso de Gestión de Riesgos**
Planificar	Establecer el contexto, valoración del riesgo, desarrollo del plan de tratamiento, aceptación del riesgo.
Hacer	Implementación del plan de tratamiento del riesgo
Verificar	Continuo monitoreo y revisión de los riesgos
Actuar	Mantener y mejorar el proceso de gestión de riesgos.

[17] PDCA: Plan, Do, Check, Act

2.4.2 *Metodologías para análisis riesgos de la seguridad de la información*

Las metodologías para el análisis de riesgos son procedimientos documentados, que se alinean y complementan los marcos de referencia, como las normas ISO 31000[18] y la ISO 27005[19]. Cada metodología puede estar orientada a satisfacer las necesidades de un conjunto particular de organizaciones, de acuerdo a característica como: el ámbito o giro de negocio, los niveles aceptables de riesgos, o la perspectiva de medición de los mismos. Sin embargo, la mayoría de metodologías se enfocarán de manera general en el análisis del riesgo como tal, y de esta manera los planes de tratamiento podrán diversificarse a partir de esta fase del proceso.

Las principales metodologías para el análisis de riesgos relacionadas con TI son las siguientes: CRAMM, MAGERIT, OCTAVE, NIST SP 800-30.

2.4.2.1 Metodología CRAMM[20]

Esta metodología, inicialmente desarrollada por el gobierno del Reino Unido y que actualmente es mantenida por SIEMENS, ofrece un enfoque ordenado y disciplinado, que abarca los componentes tecnológicos y no tecnológicos relacionados con la seguridad de la información; esto incluye el software, hardware, áreas físicas, talento humano, entre otros aspectos. Las fases que la metodología CRAMM define para el análisis de riesgo son:

- La identificación y valoración de activos

---

[18] ISO 30001: La gestión de riesgos – principios y directrices

[19] ISO 27005: Tecnología de la información - Técnicas de seguridad - La gestión de riesgos de seguridad de la información

[20] CRAAM: CCTA Risk Analysis and Management Method, por sus siglas en inglés

- Identificación de Amenazas y la vulnerabilidades
- Selección de contramedidas y recomendaciones

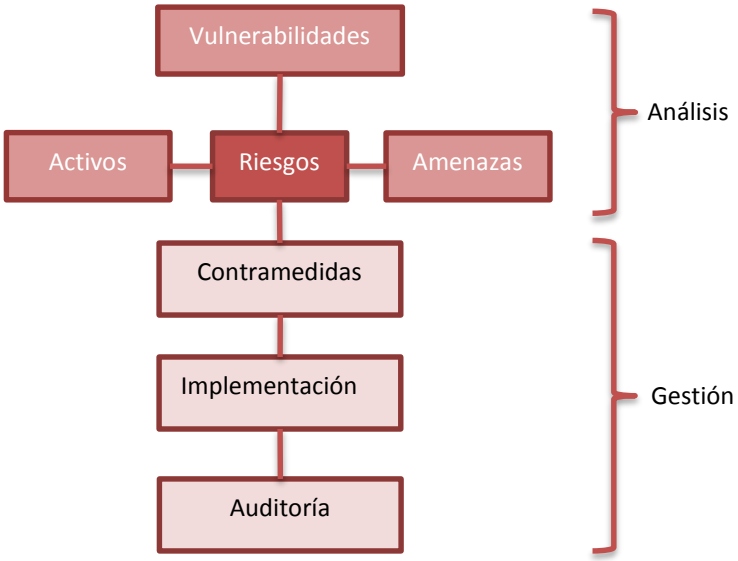

Figura 8 Metodología CRAAM para análisis de riesgos (Siemens Enterprise, 2013)

2.4.2.2 Metodología MAGERIT

MAGERIT[21] es una metodología para el análisis y gestión de riesgos desarrollada por el Consejo Superior de Administración Electrónica de España. Se ajusta al proceso de gestión de riesgos definido en la ISO 31000; por tanto, puede ser integrada en las fases de un SGSI manteniendo el enfoque de riesgos, gracias a que ofrece un guía muy completa y detallada de cómo realizar el análisis de riesgos, sin dejar espacio a la improvisación o la arbitrariedad de quienes la utilicen. Se presenta distribuida en 3 libros, de acuerdo a la siguiente descripción:

1. El método: presenta los conceptos, detalla los pasos y formaliza las actividades para el análisis de riesgos. Define la utilidad de la gestión de riesgos como parte del desarrollo de los SI.

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

2. El catálogo de elementos: facilita la diferenciación y clasificación de los activos, amenazas, vulnerabilidades, y las salvaguardas a considerar en los SI.
3. La guía de técnicas: brinda información adicional relacionada con las técnicas utilizadas para el análisis y gestión de riesgos como el análisis mediante tablas, análisis algorítmico, árboles de ataque, técnicas gráficas, entrevistas, reuniones, entre otras.

En la Figura 9 se detalla como MAGERIT puede formar parte del marco de trabajo definido por la ISO 31000.

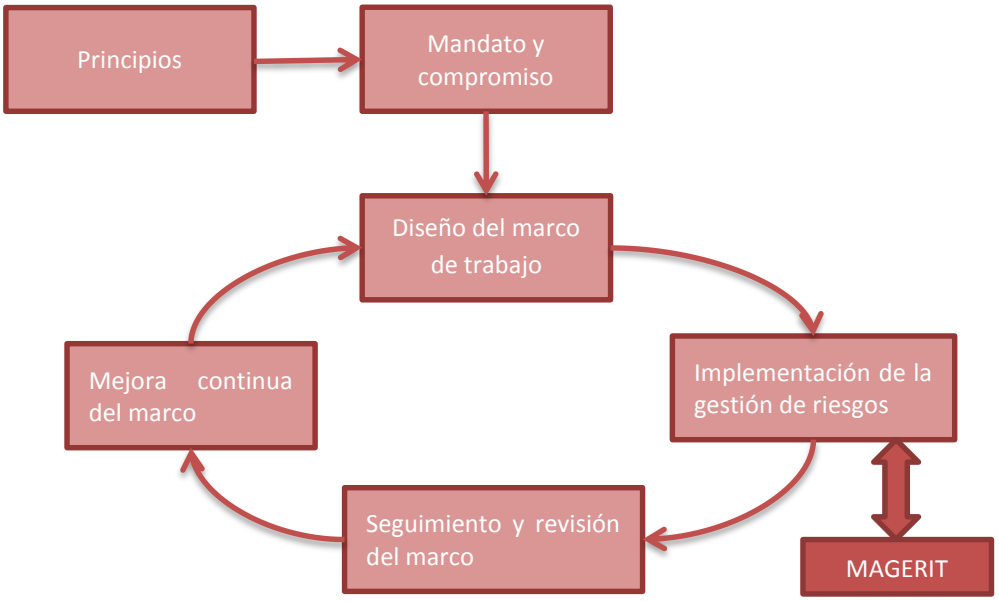

Figura 9 MAGERIT y el marco de gestión de riesgos ISO 31000 (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

2.4.2.3 Metodología OCTAVE[22]

Es una metodología desarrollada por el CERT como parte del Software Engineering Institute, es considerado como un método integral de evaluación de riesgos, dirigido a empresas grandes, que mantiene un enfoque sistemático, orientado bajo contextos y auto dirigido.

El método OCTAVE define tres fases para examinar los problemas de la organización y la tecnología, manteniendo un enfoque global de las necesidades empresariales de seguridad de la información. Cada fase consiste de varios procesos, y cada proceso tiene uno o varios talleres liderados o conducidos por el equipo de análisis. Las fases definidas en el proceso de la Figura 10 se detallan a continuación:

1. Construir perfiles de amenazas basadas en activos: de manera general consiste en la evaluación empresarial, identificando los activos críticos y la manera en que actualmente son protegidos.
2. Identificar las vulnerabilidades de la infraestructura: consiste en la evaluación de la información de la infraestructura.
3. Desarrollar la estrategia de seguridad y planes: En esta fase el equipo de análisis identifica los riesgos organizacionales de los activos críticos, y decide que se puede hacer con estos.

[22] OCTAVE: Operationally Critical Threat, Asset, and Vulnerability Evaluation, por sus siglas en ingles.

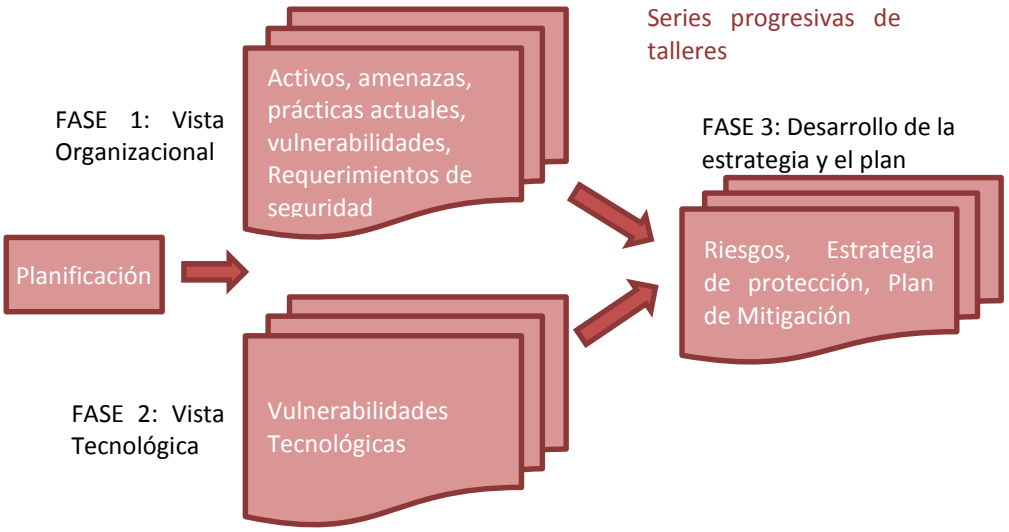

Figura 10 Proceso de la metodología OCTAVE

2.4.2.4 Metodología NIST SP[23] 800-30

Esta metodología, publicada por el Instituto Nacional de Estándares y Tecnología, tiene como objetivo proporcionar una guía para conducir una valoración de riesgos de sistemas de información federales y organizaciones. Su contenido se enfoca principalmente a la valoración de riesgos, como parte de un modelo holístico para la gestión de riesgos de la información, de acuerdo a como se define en la SP 800-39 del NIST.

[23] SP: Special Publication

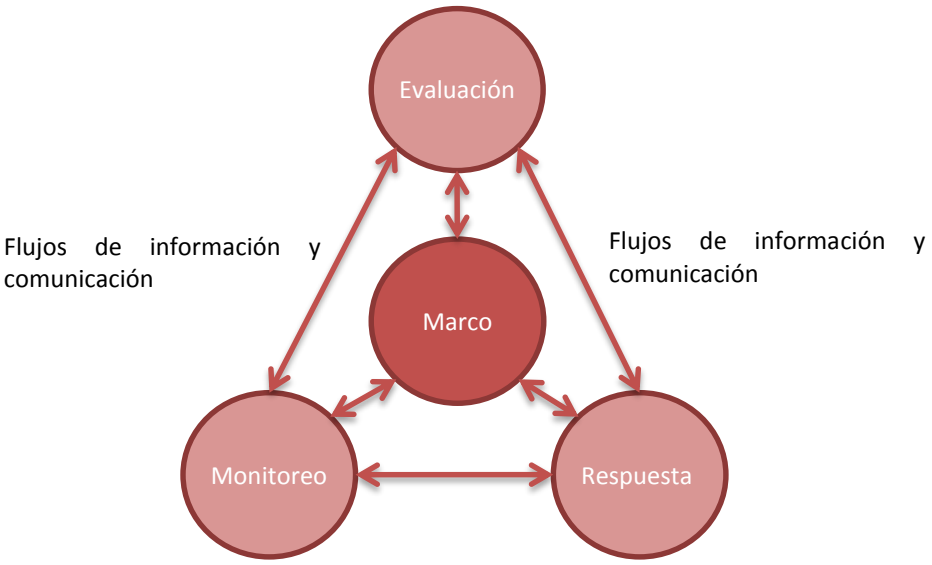

Figura 11 La valoración de riesgos dentro del modelo de gestión de riesgos (NIST, 2012)

Esta publicación se enfoca en el componente de valoración proporcionando guías detalladas paso a paso, para los siguientes procesos del modelo de gestión de riesgos:

- Preparar la valoración de riesgos
- Conducir la valoración de riesgos
- Comunicar los resultados de la valoración a la alta gerencia
- Mantener la valoración de riesgos en el tiempo

2.5 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 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 de EP PETROECUADOR forma parte de los proyectos tecnológicos implementados como parte del proceso de modernización y cambio del modelo de gestión de la empresa. Contempla, en su primera fase, la implementación de los procesos de manufactura, abastecimientos y finanzas. En una fase posterior el sistema se extenderá a áreas adicionales de manufactura e incluirá los procesos de comercialización relacionados con la facturación de combustibles.

EP PETROECUADOR, de acuerdo a los lineamientos de la empresa consultora Deloitte, se encuentra implementando el grupo de aplicaciones ERP E-Business Suite de Oracle Corporation.

2.5.1 *Aplicaciones de E-Business Suite*

E-Business Suite está compuesto por un completo portafolio de aplicaciones empresariales integradas, las cuales pueden ser implementadas de forma modular de acuerdo a las necesidades propias de cada empresa. Las aplicaciones y módulos pueden ser licenciados de forma separada; permitiendo flexibilidad, personalización y escalabilidad. En la Figura 12 se detalla los principales módulos que conforman esta herramienta de acuerdo al nombre comercial que Oracle los ha identificado, resaltando en color más oscuro los módulos actualmente implementados en EP PETROECUADOR.

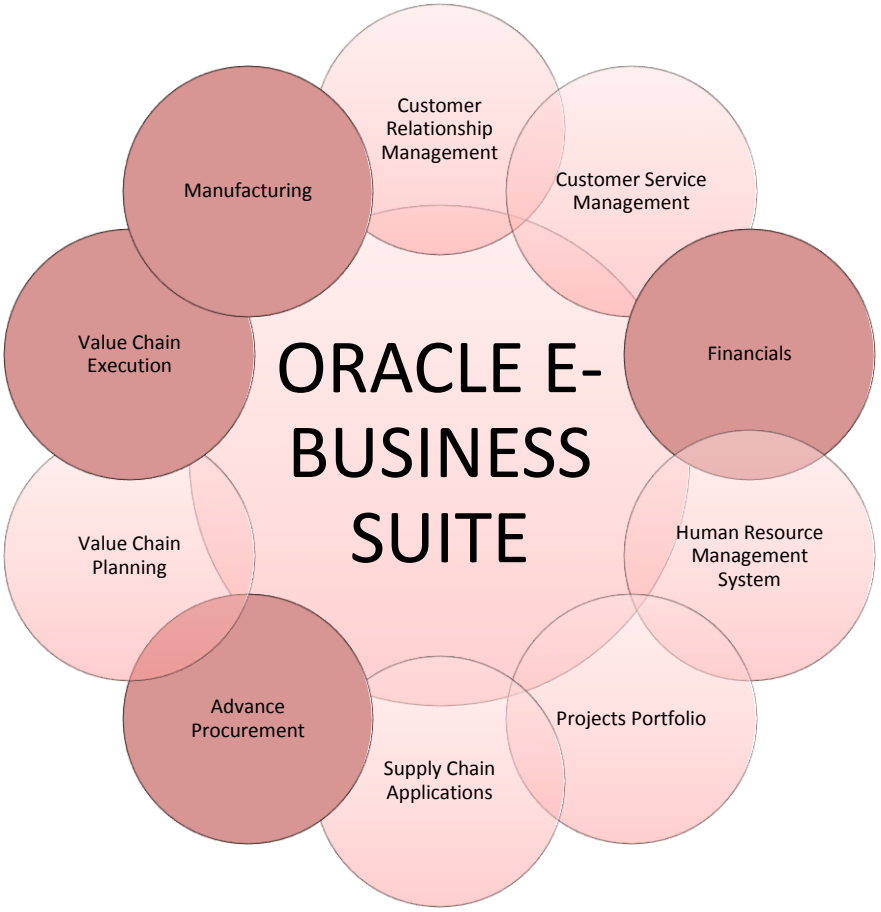

Figura 12 Aplicaciones E-Business Suite

2.5.2 *Arquitectura Lógica de E-Business Suite 12.1*

La arquitectura lógica de EBS[24] se define en 3 capas: Cliente, Aplicación y Base de datos, tal como se detalla en la Figura 13.

[24] EBS: E-Business Suite, por sus siglas en inglés.

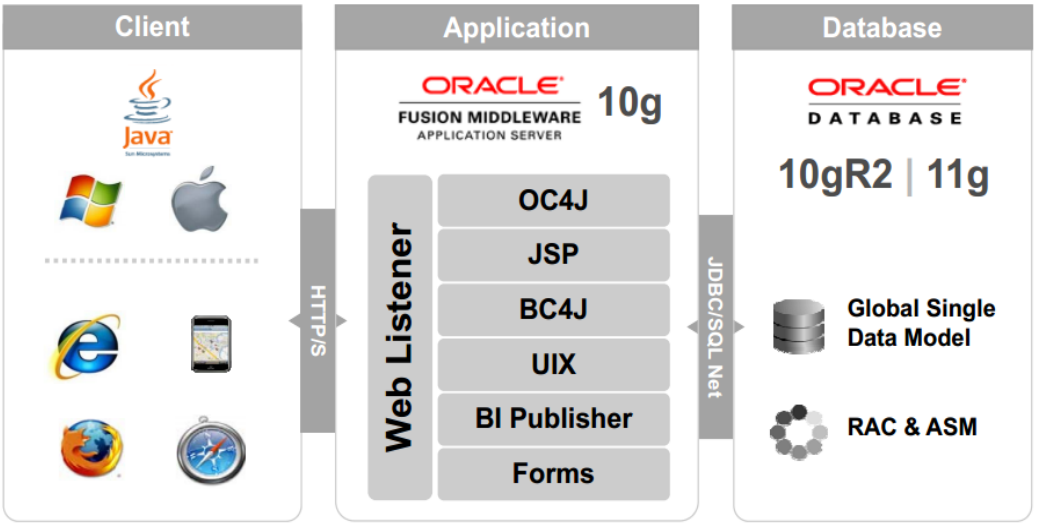

Figura 13 Arquitectura lógica E-Business Suite (Oracle Corporation, 2013)

2.5.2.1 Capa de Cliente

La interfaz del cliente se realiza a través de HTML[25] para las aplicaciones basadas en HTML, y a través de un applet[26] de Java en un navegador Web para la interfaz tradicional basada en formularios. En Oracle Applications Release 12, cada usuario se conecta a las aplicaciones de Oracle a través de la página de inicio de E–Business Suite en un cliente de navegador web de escritorio La página de inicio de E -Business proporciona un punto único de acceso a las aplicaciones basadas en HTML, aplicaciones basadas en formularios y aplicaciones de Inteligencia de Negocios.

[25] HTML: HyperText Markup Language por sus siglas en inglés, corresponde al estándar para elaborar páginas web.

[26] APPLET: fragmento de código que se ejecuta en el contexto de otro programa, como por ejemplo un navegador web.

2.5.2.2 Capa de aplicación

La capa de aplicación hospeda los diversos servicios que procesan la lógica de negocio y gestiona la comunicación entre la capa de escritorio y la capa de base datos. Esta capa ejecuta el servidor web y los procesos asociados, servidor de procesamiento concurrente, la interacción y el servidor de cumplimiento Oracle.

2.5.2.3 Capa de Base de datos

La capa de base de datos contiene el servidor de base de datos Oracle que almacena todos los datos mantenidos por las aplicaciones de Oracle. Esta capa tiene los archivos del servidor de datos Oracle y las aplicaciones ejecutables de la base de datos Oracle que almacenan físicamente las tablas, índices y otros objetos de base de datos en el sistema.

2.5.2.4 OPMN

Oracle Process Manager y el servidor de notificación (OPMN) está instalado y configurado en cada capa designada para ejecutar la aplicación web. OPMN proporciona una forma integrada para gestionar todos los componentes del servidor de aplicaciones Oracle. OPMN consta de dos partes principales: el Administrador de Procesos y el Servidor de Notificaciones. El Administrador de procesos (PM) es el mecanismo de gestión de procesos centralizado en el servidor de aplicaciones Oracle y se utiliza para gestionar todos los procesos del Servidor de aplicaciones Oracle. El PM inicia, reinicia, detiene y controla todos los procesos que gestiona. También lleva a cabo la detección y reinicio automático de los procesos muertos. El servidor de notificaciones Oracle (ONS) es el mecanismo de transporte para las notificaciones de falla, recuperación, puesta en marcha y otras relacionadas, entre los componentes del servidor de aplicaciones de Oracle.

2.5.2.5 OHS

Oracle HTTP Server (OHS) está instalado y configurado en cada capa que está designada para ejecutar la aplicación web. Proporciona la infraestructura clave necesaria para servir el contenido estático y dinámico generado por los productos de Oracle E Business Suite.

2.5.2.6 OC4J

Contenedores Oracle para J2EE (OC4J) es el núcleo de la plataforma Java 2 Enterprise Edition (J2EE) del para el componente de tiempo de ejecución del Servidor de aplicaciones Oracle. Está instalado y configurado en cada capa que está designada para ejecutar la aplicación web. Se trata de un contenedor J2EE 1.5 totalmente compatible que se ejecuta en un archivo estándar basado en el JDK 1.5 de la Máquina virtual de Java y proporciona soporte completo para Java Server Pages (JSP), servlets, Enterprise Java Beans (EJB) , Servicios Web y todos los servicios J2EE .

2.5.3 *Posicionamiento en el mercado de E-Business Suite 12.1*

Oracle EBS está considerado dentro del segmento de los sistemas ERP corporativos grandes; sin embargo, debido a su gran cantidad de aplicaciones y su característica modular de licenciamiento, es posible utilizar sus herramientas en varios tipos y tamaños de empresas.

La Figura 14, muestra la matriz BCG[27] para los sistemas ERP grandes, dentro del cual se ha considerado que EBS está ubicado en el cuadrante “Cash Cow” que significa un crecimiento poco apreciable en el mercado pero acompañado de ingresos sostenidos de buen nivel y utilidad.

[27] BCG: Matriz de Crecimiento – Participación, o matriz Boston Consulting Group, utilizada para el análisis y planificación estratégica.

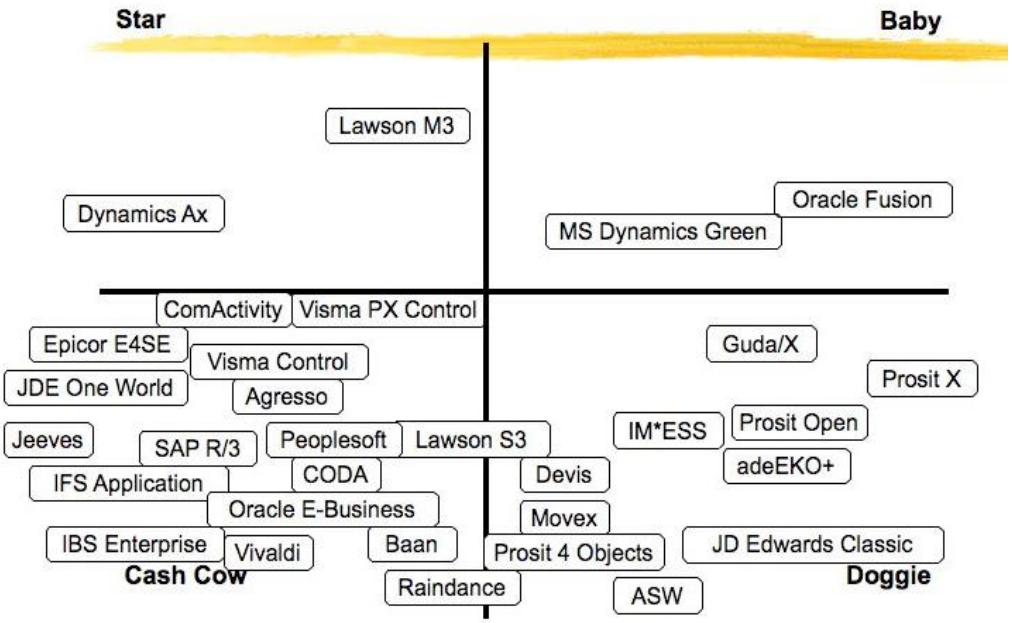

Figura 14 Matriz BCG de los Sistemas ERP grandes (Data Research DPU, 2012)

2.6 El Marco de Trabajo COBIT 5.

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[28] manteniendo el equilibrio entre los beneficios y la optimización de los niveles de riesgo y el uso de recursos. (ISACA, 2012)

COBIT 5 corresponde a la última versión del marco de trabajo publicado y mantenido por ISACA[29], una asociación global, independiente sin fines de lucro que se involucra en el desarrollo, adopción y uso, de conocimiento y prácticas mundialmente aceptadas en la industria de los SI.

La Figura 15 detalla los productos que conforman la familia COBIT 5, la cual incluye el propio marco de trabajo y otras publicaciones que proporcionan orientación

[28] TI: Tecnologías de Información

[29] ISACA: Information Systems Audit and Control Association, por sus siglas en inglés.

adicional sobre los catalizadores dentro del marco o guías profesionales que se pueden utilizar de acuerdo a las necesidades de cada empresa.

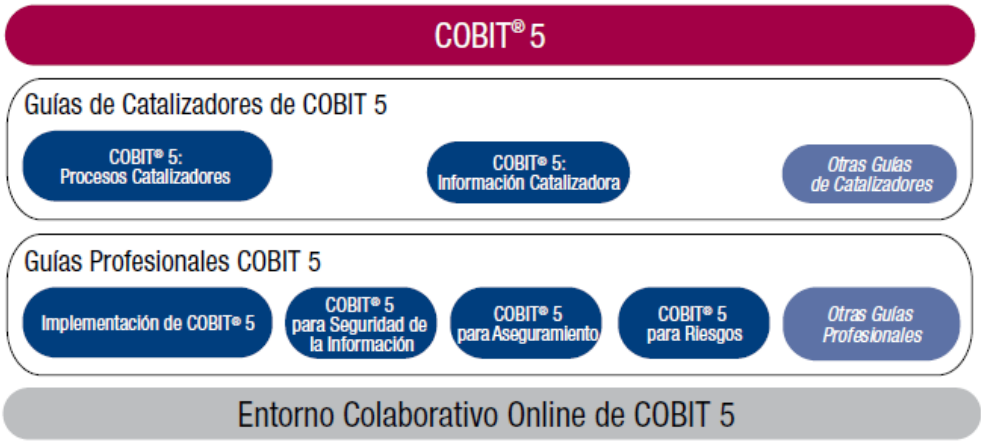

Figura 15 Familia de productos COBIT 5 (ISACA, 2012)

La Tabla 2 muestra de forma resumida y esquematizada las características principales de los productos actuales de la familia COBIT 5; se debe considerar que estos productos se encuentran en constante desarrollo por parte de ISACA, por tanto no representa la lista definitiva de los mismos.

Tabla 2 Resumen de productos de la familia COBIT 5

COBIT 5	Es el marco propiamente dicho, para el gobierno y la gestión de las TI corporativas. Documenta los 5 principios de COBIT 5 y define 7 categorías de catalizadores complementarios.	
GUÍAS DE CATALIZADORES COBIT 5	Procesos catalizadores	Detalla los procesos definidos en el modelo de referencia de COBIT 5. Incluye la cascada de metas , una explicación del modelo de procesos y los procesos de referencia.
	Información catalizadora	Profundiza el modelo de información (basado en el modelo de catalizadores genérica COBIT 5) y proporciona ejemplos de entidades de información totalmente elaborados.
GUÍAS PROFESIONALES COBIT 5	Implementación de COBIT 5	Porporciona un enfoque de buenas prácticas para la aplicación del Gobierno de TI, basado en un ciclo de mejora continua adaptado a las necesidades de la empresa.
	COBIT 5 para Seguridad de la Información	Se basa en el marco COBIT 5 y proporciona una guía más detallada y práctica para los profesionales de la seguridad de la información.
	COBIT 5 para Aseguramiento	Se centra en el aseguramiento empresarial, ofrece ejemplos de programas de auditoría/aseguramiento relacionados con la gestión de cambios, la gestión de riesgos, entre otros.
	COBIT 5 para Riesgos	Ofrece un enfoque y punto de vista, según COBIT 5, para la gestión de riesgos.
ENTORNO COLABORATIVO ONLINE DE COBIT 5	Ofrece ayuda en línea, a los miembros registrados de ISACA, para el uso de COBIT 5.	

2.6.1 ***Principios de COBIT 5.***

El marco de trabajo COBIT 5, y las guías profesionales construidas a partir de este, se basan en 5 principios claves que se detallan en la Figura 16.

Figura 16 Principios de COBIT 5 (ISACA, 2012)

2.6.1.1 Principio 1 satisfacer las necesidades de las partes interesadas.

Expresa el objetivo de toda empresa el cual es generar valor para sus partes interesadas[30] manteniendo el equilibrio entre los beneficios, optimización de riesgos y el uso de recursos.

[30] Partes Interesadas: En los principios y políticas, las partes interesadas pueden ser internas o externas a la empresa. Éstas incluyen el Consejo y el comité ejecutivo de dirección, directores de cumplimiento, gerentes de riesgos, auditores internos y externos, proveedores del servicio, clientes y agencias reguladoras. (ISACA, 2012)

2.6.1.2 Principio 2 cubrir la Empresa de extremo a extremo.

Integra el gobierno y la gestión de TI, en el gobierno corporativo y considera que los procesos habilitantes o catalizadores relacionados con TI deben ser a nivel de toda la empresa.

2.6.1.3 Principio 3 Aplicar un Marco de Referencia único integrado.

Permite alinearse con otros estándares y marcos de trabajo relevantes como las series ISO/IEC 27000, el estándar de buenas prácticas del Information Security Forum, y el BMIS. De esta manera COBIT 5 puede funcionar como marco de trabajo principal para la gestión de TI, manteniendo un lenguaje común no técnico e independiente a la tecnología, sin importar cuál sea esta.

2.6.1.4 Principio 4 Hacer posible un enfoque holístico.

Considera que una gestión efectiva y eficiente de TI, debe tener un enfoque holístico considerando varios componentes interactivos e integrados como parte de un todo, prescindiendo de un postulamiento reduccionista[31] para la gestión de TI. Para soportar la implementación de un sistema de gobierno y gestión comprensivo para las TI corporativas, COBIT 5 ha definido un grupo de catalizadores, los cuales deben entenderse como cualquier elemento que puede ayudar a conseguir los objetivos de la empresa y de forma específica pueden ser principios, políticas, procesos, estructuras organizativas, cultura, ética y comportamientos que se alinean bajo una cascada de metas[32].

---

[31] Reduccionismo: El reduccionismo científico postula que un sistema complejo puede ser explicado y comprendido mediante una reducción del mismo a las partes que lo componen.

[32] La cascada de metas está basada en la investigación realizada por la Escuela de Negocios de Alineamiento de TI de la Universidad de Amberes y el Instituto de Gobierno en Bélgica (ISACA, 2012).

2.6.1.5 Principio 5 Separar el gobierno de la Gestión.

Establece una clara distinción entre gobierno y gestión, definiendo diferentes actividades, estructuras funcionales y propósitos para cada una de ellas.

La visión de COBIT 5 para el gobierno de TI es:

Asegurar que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas. (ISACA, 2012)

En este mismo contexto la gestión planifica, elabora, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno, para alcanzar las metas empresariales.

2.6.2 ***Cascada de metas de COBIT 5.***

El objetivo principal de una empresa es la generación de valor para sus partes interesadas internas y externas. La generación de valor puede traducirse en la consecución de beneficios a cambio de una inversión, y estos beneficios pueden representarse o tomar diferentes formas de acuerdo a la naturaleza de la empresa y de las mismas partes interesadas.

La cascada de metas de COBIT 5, es el mecanismo que permite alinear los objetivos específicos, a cualquier nivel de la empresa, para satisfacer las necesidades de las partes interesadas. De acuerdo a la cascada de metas de la Figura 17, se puede determinar que el entorno, la evolución tecnológica, los cambios regulatorios, etc. son motivos que influyen y desencadenan las necesidades de las partes interesadas; estas necesidades se transforman en objetivos empresariales que en cascada generan objetivos relacionados con TI. Finalmente, se requiere la aplicación efectiva de uno o

varios catalizadores cuyas metas relevantes deben estar orientadas para apoyar los objetivos de TI.

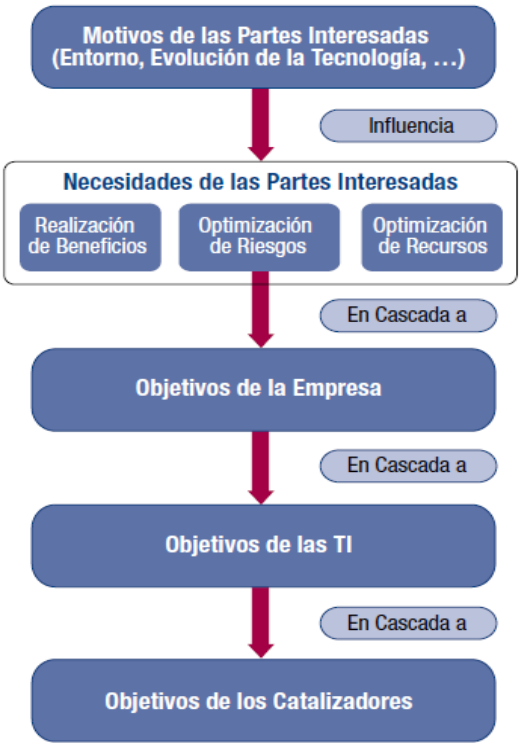

Figura 17 Cascada de metas de COBIT 5 (ISACA, 2012)

2.6.3 *Los catalizadores de COBIT 5.*

Los catalizadores son cualquier elemento que puede ayudar o facilitar la consecución de las metas de la empresa, por tanto son factores que influyen en el éxito o fracaso de una actividad. Los catalizadores son guiados por la cascada de metas y se rigen a las características explicadas en ese punto.

El marco de trabajo COBIT 5, considera 7 categorías de catalizadores tal como se muestra en la Figura 18.

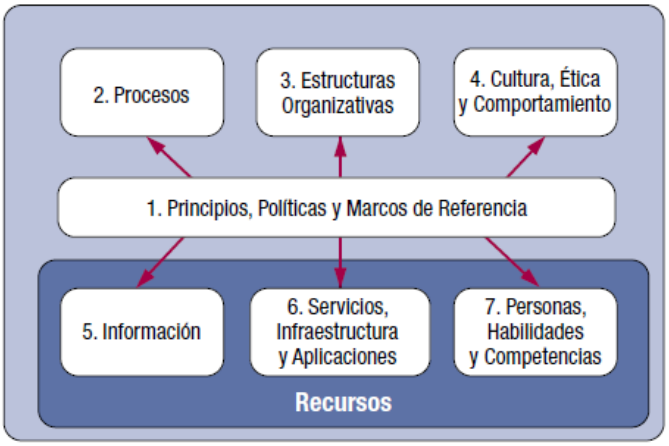

Figura 18 Categorías de catalizadores de COBIT 5 (ISACA, 2012)

Los procesos de COBIT 5 corresponden a la segunda categoría de los catalizadores, y representan el modelo de referencia sucesor del modelo de procesos de COBIT 4.1 incluyendo los modelos de procesos de Risk IT[33] y Val IT[34]. La Figura 19 muestra en la parte superior 5 procesos para el Gobierno de las TI empresariales y en la parte inferior 32 procesos para la Gestión de las TI, completando 37 procesos divididos dentro de los 5 dominios definidos por COBIT 5.

[33] Risk IT: Corresponde a un marco de referencia para el manejo de riesgos basado en COBIT, publicado por ISACA en el año 2009.

[34] Val IT: es un marco de gobernabilidad basado en COBIT que se puede utilizar para crear valor de negocio de las inversiones en TI.

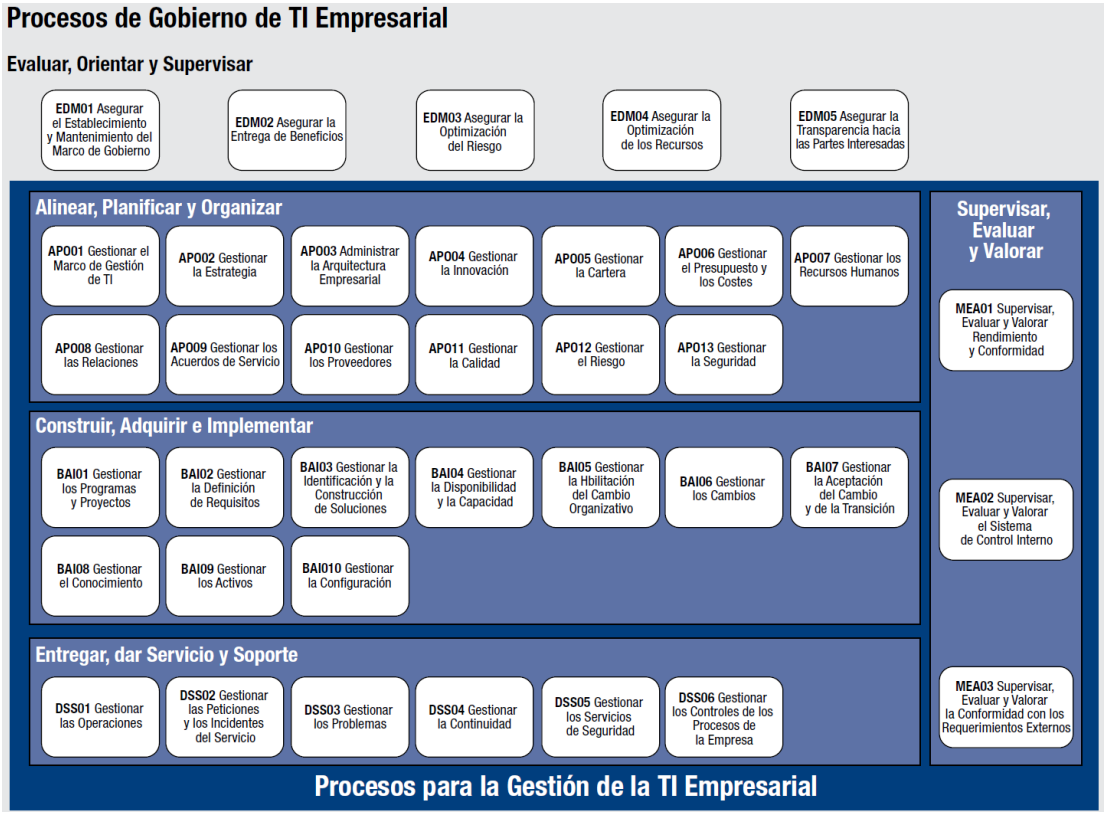

Figura 19 Procesos de COBIT 5 (ISACA, 2012)

2.7 ISO/IEC 27002.

ISO[35]/IEC[36] 27002, que anteriormente fue denominado ISO 17799, es un estándar internacional no certificable, que 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). Forma parte de la serie ISO/IEC 27000, preparada por el comité ISO/IEC JTC 1/SC 27, para la Seguridad de la Información que incluye Estándares Internacionales sobre requerimientos gestión del riesgo, métrica y medición, y el lineamiento de implementación del sistema de gestión de seguridad de la información.

[35] ISO: Organización Internacional de Estandarización, ISO por sus siglas en inglés.

[36] IEC: Comisión Electrotécnica Internacional, IEC por sus siglas en inglés.

2.7.1 *Estructura del estándar ISO/IEC 27002.*

El estándar ISO/IEC 27002 contiene 11 cláusulas de control de seguridad, las cuales colectivamente contienen un total de 39 categorías de seguridades principales y una cláusula introductoria que representa la evaluación y tratamiento del riesgo.

Las cláusulas y el número de categorías de seguridad principales de cada una se muestra en la siguiente tabla.

Tabla 3 Cláusulas y número de categorías de ISO/IEC 27002

CLAÚSULA	NÚMERO DE CATEGORÍAS DE SEGURIDAD
Política de Seguridad	1
Organización de la Seguridad de la Información	2
Gestión de Activos	2
Seguridad de recursos Humanos	3
Seguridad Física y Ambiental	2
Gestión de comunicaciones y Operaciones	10
Control de acceso	7
Adquisición, desarrollo y mantenimiento de Sistemas de Información	6
Gestión de Incidentes de Seguridad de la Información	2
Gestión de la Continuidad Comercial	1
Conformidad	3

2.7.2 *Categorías de seguridad y controles de ISO/IEC 27002.*

Cada categoría de seguridad contiene un objetivo que establece lo que se debiera lograr, y uno o más controles que se pueden aplicar para lograr el objetivo de control. El estándar contempla un total de 133 controles.

Cada control a su vez está definido con un enunciado específico para satisfacer el objetivo de control, el lineamiento de implementación del control y de manera opcional información que puede estar relacionada con aspectos legales u otros estándares. En la

Tabla 4 se resume cada una de las cláusulas con sus respectivas categorías, caracterizadas por su objetivo de control y sus controles.

Tabla 4 Objetivos de control y controles de ISO 27002

Cláusula	**Categoría / Objetivo de control**	**Control**
5. POLÍTICA DE SEGURIDAD.	5.1 Política de seguridad de la información.	5.1.1 Documento de política de seguridad de la información.
		5.1.2 Revisión de la política de seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	6.1 Organización interna.	6.1.1 Compromiso de la Dirección con la seguridad de la información.
		6.1.2 Coordinación de la seguridad de la información.
		6.1.3 Asignación de responsabilidades relativas a la seguridad de la información.
		6.1.4 Proceso de autorización de recursos para el tratamiento de la información.
		6.1.5 Acuerdos de confidencialidad.
		6.1.6 Contacto con las autoridades.
		6.1.7 Contacto con grupos de especial interés.
		6.1.8 Revisión independiente de la seguridad de la información.
	6.2 Terceros.	6.2.1 Identificación de los riesgos derivados del acceso de terceros.
		6.2.2 Tratamiento de la seguridad en la relación con los clientes.
		6.2.3 Tratamiento de la seguridad en contratos con terceros.
7. GESTIÓN DE ACTIVOS.	7.1 Responsabilidad sobre los activos.	7.1.1 Inventario de activos.
		7.1.2 Propiedad de los activos.
		7.1.3 Uso aceptable de los activos.
	7.2 Clasificación de la información.	7.2.1 Directrices de clasificación.
		7.2.2 Etiquetado y manipulado de la información.

Continúa →

Cláusula	Categoría / Objetivo de control	Control
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	8.1 Antes del empleo.	8.1.1 Funciones y responsabilidades.
		8.1.2 Investigación de antecedentes.
		8.1.3 Términos y condiciones de contratación.
	8.2 Durante el empleo.	8.2.1 Responsabilidades de la Dirección.
		8.2.2 Concienciación, formación y capacitación en seguridad. de la información
		8.2.3 Proceso disciplinario.
	8.3 Cese del empleo o cambio de puesto de trabajo.	8.3.1 Responsabilidad del cese o cambio.
		8.3.2 Devolución de activos.
		8.3.3 Retirada de los derechos de acceso.
9. SEGURIDAD FÍSICA Y DEL ENTORNO.	9.1 Áreas seguras.	9.1.1 Perímetro de seguridad física.
		9.1.2 Controles físicos de entrada.
		9.1.3 Seguridad de oficinas, despachos e instalaciones.
		9.1.4 Protección contra las amenazas externas y de origen ambiental.
		9.1.5 Trabajo en áreas seguras.
		9.1.6 Áreas de acceso público y de carga y descarga.
	9.2 Seguridad de los equipos.	9.2.1 Emplazamiento y protección de equipos.
		9.2.2 Instalaciones de suministro.
		9.2.3 Seguridad del cableado.
		9.2.4 Mantenimiento de los equipos.
		9.2.5 Seguridad de los equipos fuera de las instalaciones.
		9.2.6 Reutilización o retirada segura de equipos.
		9.2.7 Retirada de materiales propiedad de la empresa.

Continúa →

Cláusula	Categoría / Objetivo de control	Control
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.	10.1 Responsabilidades y procedimientos de operación.	10.1.1 Documentación de los procedimientos de operación.
		10.1.2 Gestión de cambios.
		10.1.3 Segregación de tareas.
		10.1.4 Separación de los recursos de desarrollo, prueba y operación.
	10.2 Gestión de la provisión de servicios por terceros.	10.2.1 Provisión de servicios.
		10.2.2 Supervisión y revisión de los servicios prestados por terceros.
		10.2.3 Gestión del cambio en los servicios prestados por terceros.
	10.3 Planificación y aceptación del sistema.	10.3.1 Gestión de capacidades.
		10.3.2 Aceptación del sistema.
	10.4 Protección contra el código malicioso y descargable.	10.4.1 Controles contra el código malicioso.
		10.4.2 Controles contra el código descargado en el cliente.
	10.5 Copias de seguridad.	10.5.1 Copias de seguridad de la información.
	10.6 Gestión de la seguridad de las redes.	10.6.1 Controles de red.
		10.6.2 Seguridad de los servicios de red.
	10.7 Manipulación de los soportes.	10.7.1 Gestión de soportes extraíbles.
		10.7.2 Retirada de soportes.
		10.7.3 Procedimientos de manipulación de la información.
		10.7.4 Seguridad de la documentación del sistema.

Continúa →

Cláusula	Categoría / Objetivo de control	Control
11. CONTROL DE ACCESO.	10.8 Intercambio de información.	10.8.1 Políticas y procedimientos de intercambio de información.
		10.8.2 Acuerdos de intercambio.
		10.8.3 Soportes físicos en tránsito.
		10.8.4 Mensajería electrónica.
		10.8.5 Sistemas de información empresariales.
	10.9 Servicios de comercio electrónico.	10.9.1 Comercio electrónico.
		10.9.2 Transacciones en línea.
		10.9.3 Información públicamente disponible.
	10.10 Supervisión.	10.10.1 Registros de auditoría.
		10.10.2 Supervisión del uso del sistema.
		10.10.3 Protección de la información de los registros.
		10.10.4 Registros de administración y operación.
		10.10.5 Registro de fallos.
		10.10.6 Sincronización del reloj.
	11.1 Requisitos de negocio para el control de acceso.	11.1.1 Política de control de acceso.
	11.2 Gestión de acceso de usuario.	11.2.1 Registro de usuario.
		11.2.2 Gestión de privilegios.
		11.2.3 Gestión de contraseñas de usuario.
		11.2.4 Revisión de los derechos de acceso de usuario.
	11.3 Responsabilidades de usuario.	11.3.1 Uso de contraseñas.
		11.3.2 Equipo de usuario desatendido.

Continúa →

Cláusula	Categoría / Objetivo de control	Control
	11.4 Control de acceso a la red.	11.3.3 Política de puesto de trabajo despejado y pantalla limpia.
		11.4.1 Política de uso de los servicios en red.
		11.4.2 Autenticación de usuario para conexiones externas.
		11.4.3 Identificación de los equipos en las redes.
		11.4.4 Protección de los puertos de diagnóstico y configuración remotos.
		11.4.5 Segregación de las redes.
		11.4.6 Control de la conexión a la red.
		11.4.7 Control de encaminamiento (routing) de red.
	11.5 Control de acceso al sistema operativo.	11.5.1 Procedimientos seguros de inicio de sesión.
		11.5.2 Identificación y autenticación de usuario.
		11.5.3 Sistema de gestión de contraseñas.
		11.5.4 Uso de los recursos del sistema.
		11.5.5 Desconexión automática de sesión.
		11.5.6 Limitación del tiempo de conexión.
	11.6 Control de acceso a las aplicaciones y a la información.	11.6.1 Restricción del acceso a la información.
		11.6.2 Aislamiento de sistemas sensibles.
	11.7 Ordenadores portátiles y teletrabajo.	11.7.1 Ordenadores portátiles y comunicaciones móviles.
		11.7.2 Teletrabajo.
12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.	12.1 Requisitos de seguridad de los sistemas de información.	12.1.1 Análisis y especificación de los requisitos de seguridad.
	12.2 Tratamiento correcto de las aplicaciones.	12.2.1 Validación de los datos de entrada.
		12.2.2 Control del procesamiento interno.

Continúa →

Cláusula	Categoría / Objetivo de control	Control
		12.2.3 Integridad de los mensajes.
		12.2.4 Validación de los datos de salida.
	12.3 Controles criptográficos.	12.3.1 Política de uso de los controles criptográficos.
		12.3.2 Gestión de claves.
	12.4 Seguridad de los archivos de sistema.	12.4.1 Control del software en explotación.
		12.4.2 Protección de los datos de prueba del sistema.
		12.4.3 Control de acceso al código fuente de los programas.
	12.5 Seguridad en los procesos de desarrollo y soporte.	12.5.1 Procedimientos de control de cambios.
		12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
		12.5.3 Restricciones a los cambios en los paquetes de software.
		12.5.4 Fugas de información.
		8.5.5 Externalización del desarrollo de software.
	12.6 Gestión de la vulnerabilidad técnica.	12.6.1 Control de las vulnerabilidades técnicas.
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	13.1 Notificación de eventos y puntos débiles de seguridad de la información.	13.1.1 Notificación de los eventos de seguridad de la información.
		13.1.2 Notificación de puntos débiles de seguridad.
	13.2 Gestión de incidentes y mejoras de seguridad de la información.	13.2.1 Responsabilidades y procedimientos.
		13.2.2 Aprendizaje de los incidentes de seguridad de la información.
		13.2.3 Recopilación de evidencias.
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
		14.1.2 Continuidad del negocio y evaluación de riesgos.

Continúa →

Cláusula	Categoría / Objetivo de control	Control
		14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
		14.1.4 Marco de referencia para la planificación de la continuidad del negocio.
		14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.
15. CUMPLIMIENTO.	15.1 Cumplimiento de los requisitos legales.	15.1.1 Identificación de la legislación aplicable.
		15.1.2 Derechos de propiedad intelectual (DPI).
		15.1.3 Protección de los documentos de la organización.
		15.1.4 Protección de datos y privacidad de la información de carácter personal.
		15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.
		15.1.6 Regulación de los controles criptográficos.
	15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.	15.2.1 Cumplimiento de las políticas y normas de seguridad.
		15.2.2 Comprobación del cumplimiento técnico.
	15.3 Consideraciones sobre las auditorías de los sistemas de información.	15.3.1 Controles de auditoría de los sistemas de información.
		15.3.2 Protección de las herramientas de auditoría de los sistemas de información

2.8 Análisis de COBIT 5 e ISO 27002 como estándares de gestión de TI

En la actualidad, varias son las empresas que se encuentran adoptando mejores prácticas de TI como parte de sus modelos de gestión, debido a requerimientos de negocio que exigen un cambio en los enfoques tradicionales de gestión de las TIC. Algunos de los indicadores que impulsan la adopción de buenas prácticas son los siguientes:

- La necesidad de obtener mayor retorno de las inversiones en TI
- Mayor complejidad de los riesgos asociados con la S-I
- Cumplimiento de requisitos regulatorios
- Reducción de costos operativos mediante la adopción de esquemas estandarizados de gestión en lugar de esquemas personalizados.
- Evaluación de cumplimiento de objetivos
- Comparación con otras empresas de la misma actividad comercial (benchmarking).
- Casos de éxito comprobados relacionados con la adopción de buenas prácticas normalmente aceptadas.

2.8.1 *Criterio general para la adopción de buenas prácticas*

Cada empresa necesita ajustar la utilización de estándares y prácticas a sus requerimientos individuales, es decir que su adopción no es una regla generalizada que se ajusta de manera directa y de forma exclusiva a las áreas de TI de todas las empresas, por el contrario requiere un análisis personalizado que debe involucrar de forma obligatoria a la alta gerencia, los directores, auditores, entes de control y los clientes; logrando que las buenas prácticas faciliten la entrega de servicios de TI eficientes y orientados con los objetivos empresariales. (ITGI, OCG, 2008).

En el ámbito de la S-I, la adopción de estándares y buenas prácticas, debe mantener compatibilidad con un marco de gestión de riesgos empresarial. Este requerimiento garantizará que las buenas prácticas puedan integrarse con otros métodos o prácticas más generales que se utilicen a nivel corporativo, es decir que se aprovechará la ventaja brindada por la estandarización al permitir ampliar las prácticas y procedimientos de forma natural e independiente de la plataforma tecnológica.

2.8.1 *Características y compatibilidad de COBIT 5 e ISO 27002*

COBIT 5 e ISO 27002 son marcos de referencia y estándares ampliamente utilizados, sus contenidos han evolucionado a través de los años y representan el aporte de expertos, consultores y profesionales de la industria de TI; por tanto, pueden ser de gran utilidad para establecer lineamientos claros para el diseño de un modelo de gestión de S-I consistente y bien fundamentado.

COBIT 5 está basado en los más recientes marcos y normas relevantes, tales como ISO 9000[37], ISO/IEC 38500[38], ITIL[39], ISO/IEC 27002, PMBOK[40], entre otros. Su enfoque holístico, diferencia claramente los roles de gobierno y gestión, describe responsabilidades en los distintos niveles de la empresa y cubre todas las etapas de proceso de principio a fin. Sin embargo, COBIT 5 no incluye una guía exhaustiva para la definición de procedimientos o tareas específicas de gestión de TI o S-I, es decir que

---

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

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

[39] 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.

[40] 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.

se enfoca en lo que una empresa necesita hacer pero no cómo lo tiene que hacer. La audiencia objetivo es la alta gerencia, los gerentes funcionales, los gerentes de TI y los auditores. Esta característica ubica a COBIT 5 como un marco de gestión y control, más no como un manual de referencia de procesos aun cuando esté orientado a los mismos.

El enfoque de COBIT, dirigido a un alto nivel gerencial, y el hecho de que está basado en muchos estándares y prácticas facilitan su utilización como un marco integrador único bajo el cual se pueden alinear varias prácticas de TI que cumplan con los requerimientos del negocio.

Por otro lado, el objetivo del estándar ISO/IEC 27002 es brindar información, a los responsables de la implementación de S-I, utilizable como un punto de partida para un proceso de aseguramiento. Su contenido representa los requisitos legales o las mejores prácticas generalmente aceptadas, que permiten mantener y desarrollar normas de seguridad y prácticas de gestión que garanticen la protección de la información

Considerando que COBIT 5 está basado en varios estándares, incluyendo la ISO/IEC 27002, es fácil identificar que la relación existente entre estos dos estándares es natural y amplia, identificándose aspectos comunes en todos los dominios de COBIT como se detalla en la Figura 20.

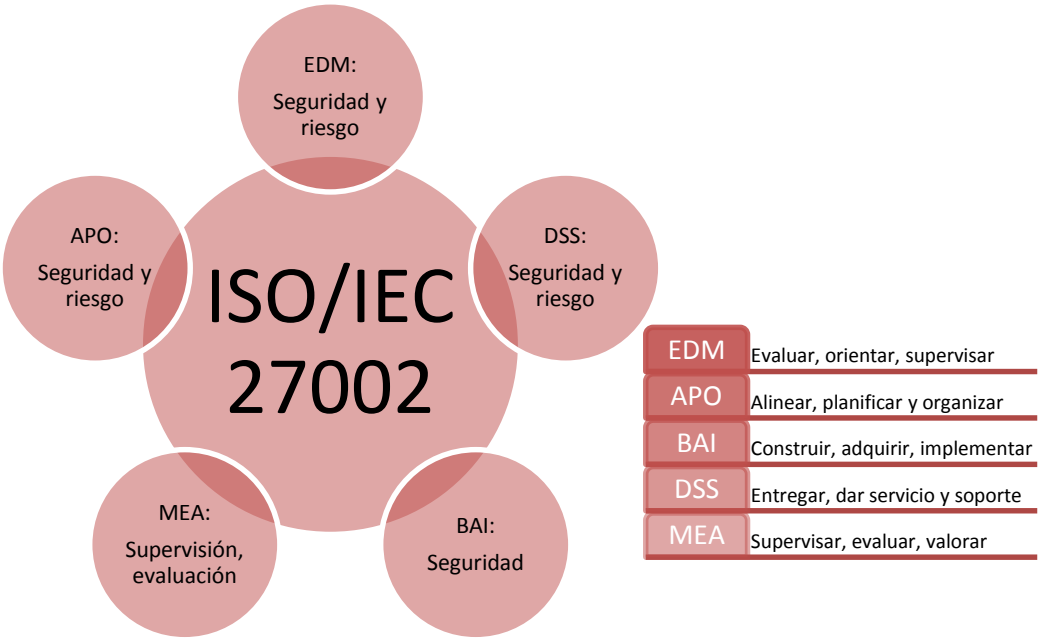

Figura 20 Relación de ISO/IEC 27002 y COBIT 5

La Figura 21 destaca como otros estándares y marcos, como ISO/IEC 27002, se integran con los materiales existente y nuevos de ISACA, formando la base de conocimiento principal; la cual, complementada con la definición de los catalizadores, es filtrada para generar el "Marco COBIT 5" y las "Guías profesionales COBIT 5". Estas últimas tratan aspectos específicos del marco principal expandiendo sus definiciones y brindando guías más prácticas apoyadas por información extendida de los mismos estándares u otros complementarios.

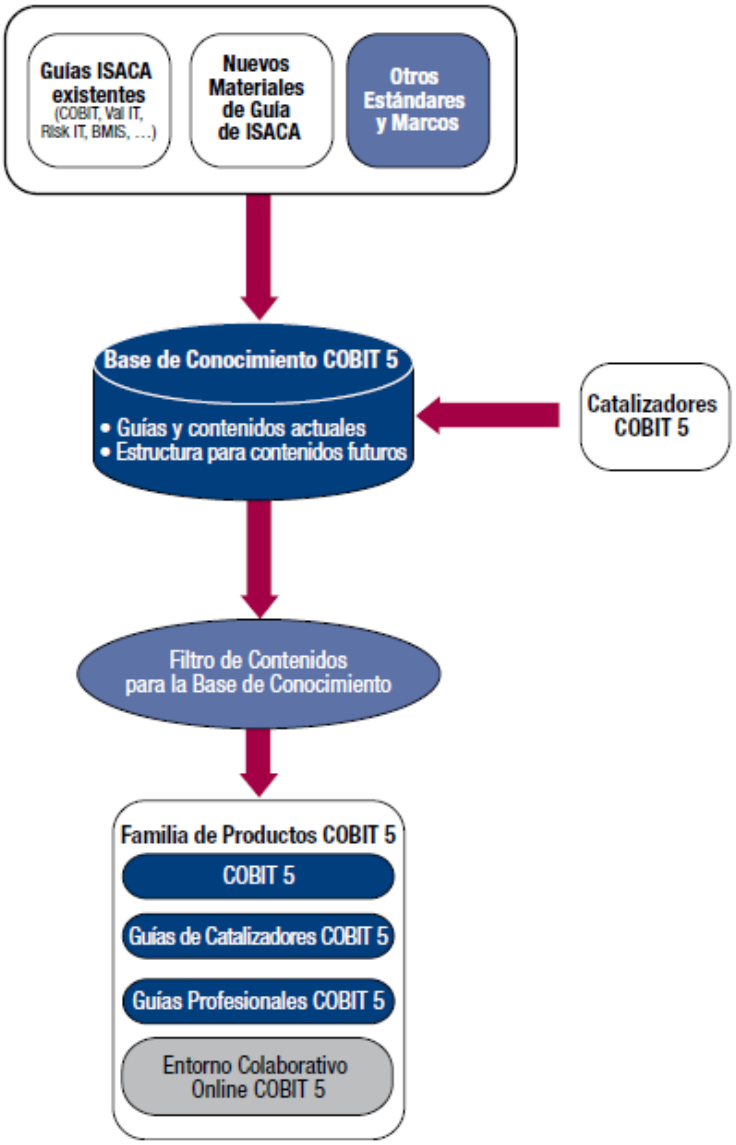

Figura 21 COBIT como marco integrador único (ISACA, 2012)

2.8.2 *Procedimiento práctico para alinear COBIT 5 e ISO27002*

A continuación se detalla un procedimiento genérico que nos permitirá alinear COBIT 5 e ISO 27002 en beneficio de la empresa. Las fases detalladas no son definitivas, y al igual que los estándares deberán ser analizadas y mejoradas según corresponda.

2.8.2.1 Elaboración

En esta fase se establece un contexto de análisis y se define las necesidades que se tratarán de solucionar. El principal reto de esta fase es definir un alcance adecuado que considere las consecuencias de los cambios organizativos y operativos que la adopción de un estándar implica. Los principales temas que podrán ser tratados mediante la utilización de COBIT 5 son:

- Gobernabilidad
- Política de gestión y Control
- Alineación de objetivos de TI con los objetivos corporativos
- Establecimiento de requisitos de auditoría
- Identificación de procesos y responsables
- Procesos de control y mejora continua

2.8.2.2 Priorización

Esta fase tiene como objeto optimizar la implementación de estándares, evitando crear un marco de referencia desenfocado y que carece de apoyo o comprensión por parte de los niveles directivos de la empresa.

Las principales actividades de esta fase son:

- Aseguramiento del compromiso de cambio por parte de los niveles ejecutivos
- Selección de procesos relevantes del marco de referencia principal, en función de las necesidades corporativas.
- Establecer los controles e indicadores claves que serán comunicados a la alta gerencia.

Se debe aclarar que una herramienta útil para la selección de los procesos relevantes es el análisis de riesgo, el cual complementa las necesidades corporativas y permite tomar decisiones consistentes bajo un esquema de aseguramiento.

2.8.2.3 Planificación

Una vez establecido el rumbo y con el apoyo de la alta gerencia, se establece un plan de implementación que sea conducido en las mismas condiciones de un proyecto. Se debe entender que la implementación deberá ser paulatina y se deberá medir continuamente el resultado de los esfuerzos realizados. Un enfoque más completo, basado en la "Guía de implementación COBIT 5" será detallado como parte de la presente investigación en el capítulo 4.

2.8.2.4 Alineamiento de las mejores prácticas

Considerando que COBIT 5 es el marco gobernante e integrador, las actividades que se deben realizar en esta fase deben estar orientadas a complementar las áreas discretas y procesos que el marco principal ha definido como estratégicos y prioritarios. Por tanto, ISO/IEC 27002 podrá ser utilizada para definir los siguientes aspectos:

- Objetivos de control y controles para los procesos de COBIT.
- Enfoque de la S-I bajo un criterio de gestión de riesgos.
- Verificación de cumplimiento de buenas prácticas
- Definición de niveles de servicio y métodos de control para los mismos.
- Políticas específicas

3 Capítulo III El estado del arte de la Seguridad de la Información de EP PETROECUADOR

3.1 La Empresa Pública de Hidrocarburos del Ecuador

La Empresa Pública de Hidrocarburos del Ecuador fue creada mediante la expedición del Decreto Ejecutivo No. 315, el 6 de abril de 2010.

"El objeto principal de EP PETROECUADOR, es la gestión del sector estratégico de los recursos naturales no renovables, para su aprovechamiento sustentable, conforme a la Ley Orgánica de Empresas Públicas y la Ley de Hidrocarburos, para lo cual intervendrá en todas las fases de la actividad hidrocarburífera, bajo condiciones de preservación ambiental y de respeto de los derechos de los pueblos" (Decreto Ejecutivo No. 315, 2010).

El día 2 de enero de 2013 se publicó en el Registro Oficial Número 860, el Decreto Ejecutivo N.- 1351-A, mediante el cual se reforma el Decreto Ejecutivo No. 315, disponiendo que PETROAMAZONAS EP asuma las fases de exploración y explotación de la actividad hidrocarburífera; como consecuencia EP PETROECUADOR interviene en todas las fases de la actividad hidrocarburífera, a excepción de las fases de exploración y producción.

3.1.1 *Misión*

“Generar riqueza y desarrollo sostenible para el Ecuador, con talento humano comprometido, gestionando rentable y eficientemente los procesos de transporte, refinación, almacenamiento y comercialización nacional e internacional de hidrocarburos, garantizando el abastecimiento interno de productos con calidad, cantidad, oportunidad, responsabilidad social y ambiental".

3.1.2 *Visión*

"Ser la empresa reconocida nacional e internacionalmente por su rentabilidad, eficiente gestión, productos y servicios con elevados estándares de calidad, excelencia en su talento humano, buscando siempre el equilibrio con la naturaleza, la sociedad y el hombre"

3.1.3 *Valores Institucionales*

Los valores empresariales de EP PETROECUADOR son los siguientes:

- Integridad
- Respeto
- Responsabilidad
- Excelencia
- Trabajo en Equipo

3.1.4 *Indicadores financieros*

Algunos indicadores financieros, presentados por el directorio de EP PETROECUADOR, para los años 2011 y 2012 son los siguientes:

Tabla 5 Indicadores financieros EP PETROECUADOR

Concepto	dic-11		dic-12	
Rentabilidad sobre ventas				
Utilidad	6260328	42,40%	5864482	37,60%
Ventas	14781524		15616497	
Rentabilidad sobre patrimonio				
Utilidad	6260328	153,80%	5864482	120,40%
Patrimonio	4069749		4871941	
Rentabilidad sobre total de activos				
Utilidad	6260328	79,80%	5864482	68%
Activos	7849475		8619941	

3.1.5 *Cadena de Valor*

En la Figura 22 se muestra esquematizada la cadena de valor de EP PETROECUADOR, en donde se distingue el macro proceso gobernante relacionado a

la Gestión del sector hidrocarburífero, los macro procesos agregadores de valor y los macro procesos habilitantes, dentro de los cuales se encuentra las Tecnologías de la Información y Comunicaciones.

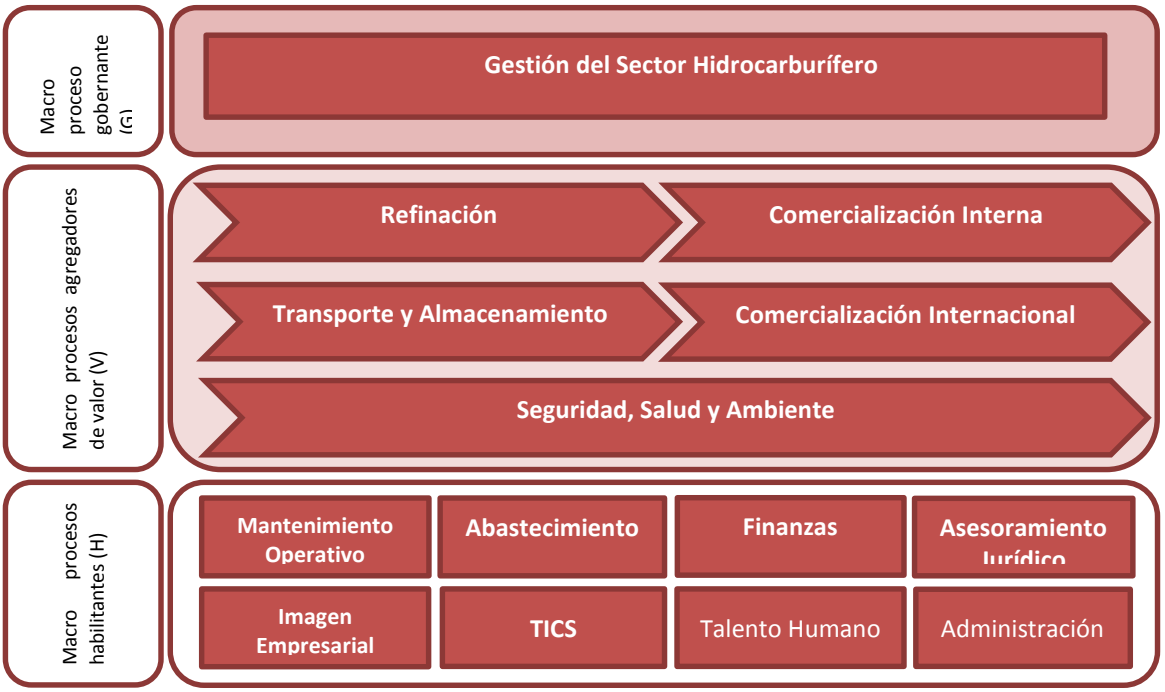

Figura 22 Cadena de valor de EP PETROECUADOR

3.1.5.1 Transporte y almacenamiento

Se ocupa del transportar los petróleos crudos y derivados por sistemas de oleoductos y poliductos, garantizando la entrega oportuna de hidrocarburos para exportación y refinación.

Forman parte de este proceso las siguientes instalaciones:

- Sistema de Oleoducto Transecuatoriano (SOTE) que transporta en promedio 360000 barriles diarios de crudo desde la Amazonía hasta el terminal marítimo Balao en Esmeraldas.
- Red de poliductos con una extensión de 1597 kilómetros

- Almacenamiento de crudo con una capacidad 5200000 barriles distribuidos en las cabeceras del Balao y Lago Agrio del SOTE.
- Almacenamiento de derivados con una capacidad operativa de 2662617 barriles.

3.1.5.2 Refinación

Se encarga de la industrialización del petróleo extraído de los campos petroleros del país en 3 refinerías ubicadas estratégicamente:

- Refinería Esmeraldas: se encuentra en proceso de rehabilitación para recuperar su capacidad de procesamiento de 110000 barriles diarios, siendo la más grande del país. Produce gasolinas súper y extra, diésel, gas licuado de petróleo, jet fuel, fuel oil, asfaltos, diésel premiun y combustibles para pesca artesanal.
- Refinería Shushufindi: Posee 2 unidades de destilación atmosférica con una capacidad de procesamiento total de 20000 barriles por día y una planta de gas con que produce 500 toneladas métricas de gas licuado de petróleo.
- Refinería la Libertad: Con más de 70 años de operación es la más antigua del país y la segunda en capacidad de procesamiento con 45000 barriles diarios. Produce Gas licuado de petróleo, gasolina base, diésel, turbo fuel, solvente de caucho, solvente de pinturas, spray oil y fuel oil.

3.1.5.3 Comercialización interna

Comercializa los derivados del petróleo para satisfacer la demanda nacional; lidera y administra la red de gasolineras más grande del país, que incluye 245 gasolineras de las cuales 45 son de propiedad del Estado. Actualmente se suman 20 estaciones de servicio, en las fronteras con Perú y Colombia, en las cuales realiza controles para

evitar el uso indebido de los combustibles subsidiados. Las ventas promedio diarias de la comercializadora hacienden a los $15’810.113 USD para el mes de octubre de 2013.

3.1.5.4 Comercialización internacional

Desarrolla estrategias de comercialización para la compraventa de hidrocarburos, de preferencia con los consumidores finales, ya sean países o empresas estatales y/o privadas. Esta división tiene a su cargo la importación de derivados en los que el país es deficitario, como el gas licuado de petróleo, naftas y diésel premiun, entre otros.

3.1.5.5 Seguridad, Salud y Ambiente

Mantiene la responsabilidad de preservar el ambiente en todas las fases de la operación hidrocarburífera en el ámbito nacional, en cumplimiento de la política empresarial y de las normas internacionales ISO 9001, 14001, 17025.

Las iniciativas que se manejan son:

- Mitigación y remediación
- Gestión Socio ambiental
- Seguridad y Salud ocupacional
- Seguridad Física

3.1.6 *Distribución Geográfica*

EP Petroecuador tiene presencia en todas regiones y provincias del Ecuador; la mayoría de sus instalaciones industriales se encuentran en las provincias de Esmeraldas, Santa Elena y Sucumbíos, mientras que las redes de transporte, almacenamiento y sobre todo las estaciones de servicios se encuentran en cada provincia del país, como se puede verificar en el mapa de la Figura 23.

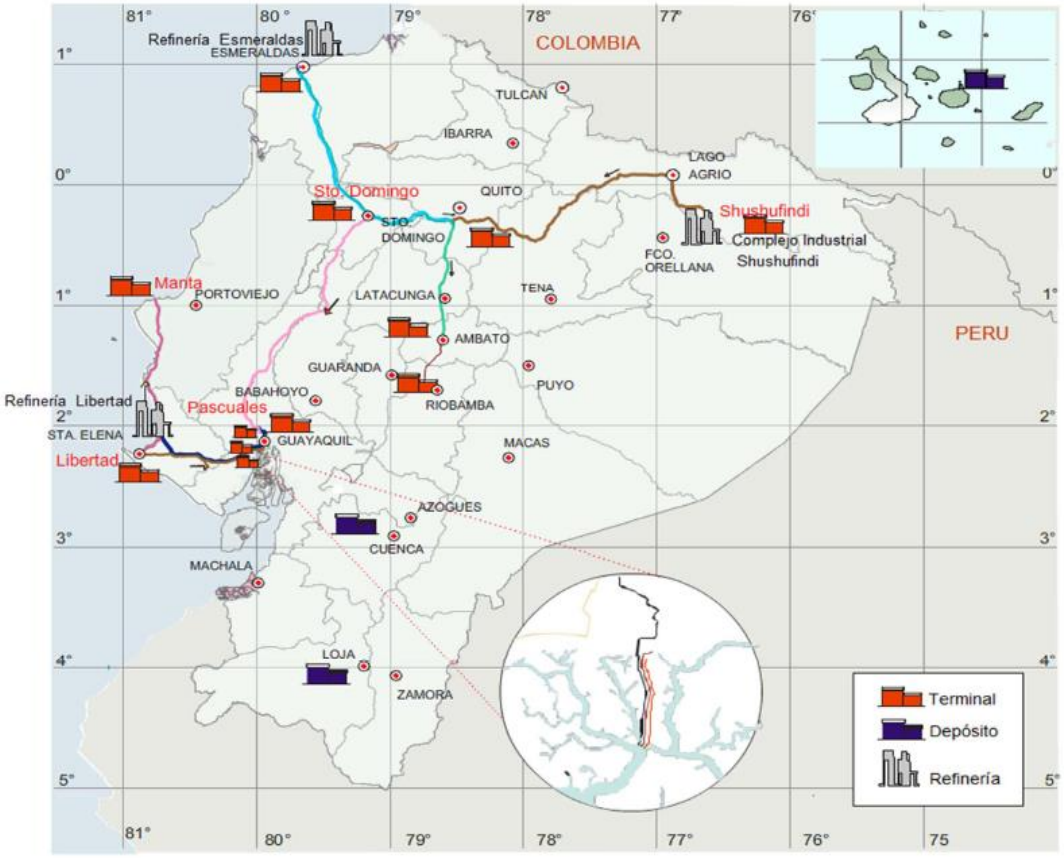

Figura 23 Mapa de localización de terminales, depósitos y refinerías de EP PETROECUADOR

3.1.7 *Estructura organizacional de EP Petroecuador*

EP PETROECUADOR, como se detalla en la Figura 24, está constituida por una Gerencia General, unidades asesoras o de apoyo, y unidades de negocio o gerencias sobre las cuales recae las responsabilidades de ejecución de los macro procesos habilitantes y agregadores de valor.

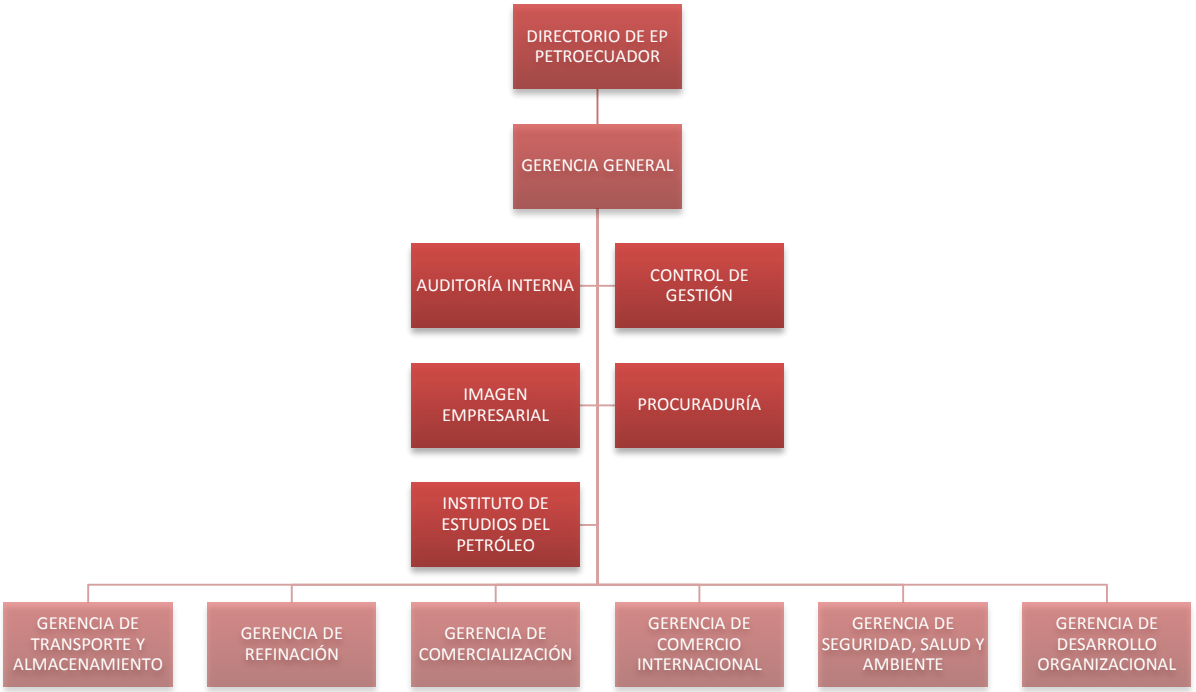

Figura 24 Estructura Organizacional de EP PETROECUADOR

3.1.7.1 La Subgerencia de Tecnologías de la información y comunicación

La subgerencia de Tecnologías de la Información y Comunicación pertenece a la Gerencia de Desarrollo Organizacional, y de acuerdo con la Figura 25, cuenta con cuatro áreas principales: Aplicaciones, Infraestructura y Comunicaciones, Datos y Soporte a Usuarios.

Figura 25 Subgerencia de Tecnologías de la Información y Comunicación

La STIC[41] de EP PETROECUADOR es la responsable de la ejecución del macro proceso "TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES (TIC)" de acuerdo a los siguientes objetivos:

- Alinear su gestión a los objetivos empresariales
- Garantizar la continuidad de los servicios de TIC
- Proporcionar servicios de calidad
- Administrar en forma óptima los recursos de TIC
- Gestionar los riesgos asociados a los servicios de TIC

El alcance de las actividades de esta subgerencia está orientado a proporcionar productos y servicios relacionados con los SI y las comunicaciones, incluyendo desde las fases de diagnóstico y de planificación hasta la implantación, supervisión y mejora de los mismos (EP Petroecuador, 2011).

La STIC y sus áreas dependientes están siendo restructuradas bajo los lineamientos de la consultora Deloitte, incluyendo el objetivo de implementar el plan de mejora de la S-I en la empresa. El Directorio de EP PETROECUADOR, como máxima autoridad y responsable, aprobó la estructura organizacional detallada en la Figura 26 para el área de TIC de la empresa; en donde se distingue el cambio de jerarquía de subgerencia a gerencia de TIC, la fusión de las áreas de datos e infraestructura y la inclusión del área de arquitectura bajo la cual se distingue el área de seguridad.

[41] STIC: Subgerencia de Tecnologías de la Información y Comunicación

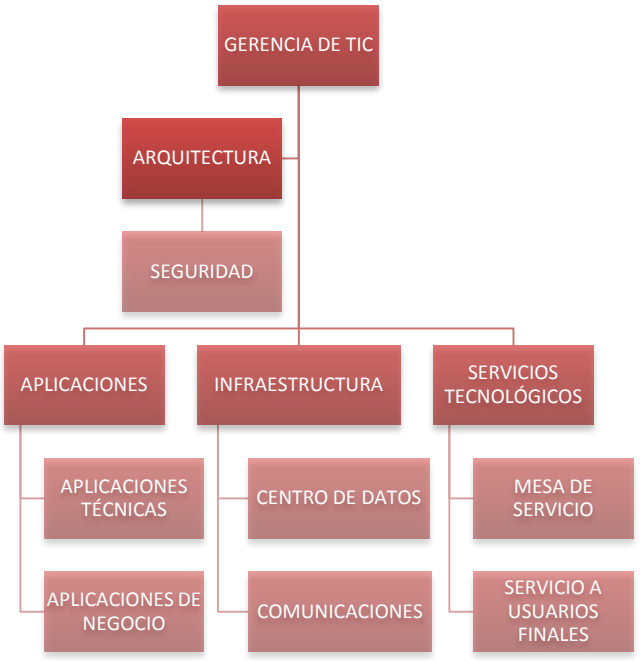

Figura 26 Estructura organizacional aprobada por el directorio de EP PETROECUADOR

La estructura organizacional aprobada, fue un primer paso por parte de la alta dirección de EP PETROECUADOR en reconocer la necesidad de incluir un área especializada en S-I, sin embargo no contempla de forma clara los lineamientos de la consultora Deloitte que explícitamente indican la necesidad de crear el área de S-I fuera de las áreas de TIC. Se debe tomar en cuenta que, EP PETROECUADOR no cuenta actualmente con un modelo completo relacionado a la S-I, por tanto esta definición poco acertada puede responder a una falta de madurez en este tema.

3.1.8 *La Normativa de procesos de la Subgerencia de Tecnologías de la Información y Comunicación de EP PETROECUADOR.*

La normativa de procesos de la STIC, está diseñada de acuerdo al marco de referencia COBIT 4.1; por lo 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)

Los subprocesos, de nivel 2 en adelante, se rigen a la Normativa de Procesos de EP PETROECUADOR. Para el caso de la STIC se cuenta con 26 subprocesos identificados y documentados, los cuales a su vez han sido relacionados con el modelo de procesos de COBIT 4.1. En la Tabla 6 se resume los procesos y subprocesos de la normativa vigente, marcando con un asterisco (*) los roles que no existen actualmente en EP PETROECUADOR, pero que han sido asumidos por comisiones delegadas por las autoridades de la empresa o incluidos de manera informal dentro de otros roles.

Tabla 6 Resumen Normativa de Procesos de EP PETROECUADOR para STIC (EP Petroecuador, 2011)

NOMBRE SUBPROCESO	FECHA PUBLICACIÓN	RESPONSABLES/ROL	ACTIVIDAD/PROCEDIMIENTO	APROBACIÓN
H04.01 Planear y Organizar TIC (PO)				
H04.01.01 Definir un Plan Estratégico de TIC (PO1)	11/01/2011	Coordinador de Área Usuaria	Analizar el portafolio de programas, propuestos por TIC	
		Administrador de Proyecto de TIC	Construir los planes tácticos para TIC	
		Coordinador Sénior de Aplicaciones	Administrar el portafolio de servicios y proyectos	
		Subgerente de TIC	Identificar el desempeño actual de TIC y construir el plan estratégico	Aprobar los planes tácticos y portafolio de proyectos
		Gerente de Desarrollo Organizacional	Relacionar las metas de la empresa con las metas de TIC	Aprobar el plan estratégico
H04.01.02 Definir la Arquitectura de la Información (PO2)	11/01/2011	Control de Gestión de TIC	Establecer y mantener esquema de clasificación de datos	
		Oficial de Seguridad*	Establecer y mantener esquema de clasificación de datos	
		Arquitecto En Jefe*	Crear y mantener un modelo de información corporativo	Aprobar el diccionario de datos, y el esquema de clasificación de datos
H04.01.03 Determinar la Dirección Tecnológica (PO3)	11/01/2011	Arquitecto En Jefe*	Crear y mantener el plan de infraestructura tecnológica y estándares tecnológicos. Monitorear la evolución tecnológica y definir su uso. Definir el uso futuro de las nuevas tecnologías.	Autorizar el plan de infraestructura tecnológica y los estándares

Continúa →

NOMBRE SUBPROCESO	FECHA PUBLICACIÓN	RESPONSABLES/ROL	ACTIVIDAD/PROCEDIMIENTO	APROBACIÓN
H04.01.04 Administrar la Inversión en TIC (PO5)	11/01/2011	Apoyo Gestión TIC*	Establecer y mantener procedimiento presupuestal de TIC e identificar, comunicar y monitorear la inversión, costo y valor de TIC para la empresa	
		Subgerente de TIC	Gestionar el portafolio de programas de inversión	
		Subgerente de Gestión Financiera		Aprobar la certificación presupuestaria
		Gerente de Desarrollo Organizacional		Aprobar las solicitud de certificación presupuestaria
H04.01.05 Administrar la Calidad de TIC (PO8)	11/01/2011	Subgerente de TIC	Definir, establecer, mantener y comunicar el sistema de administración de calidad de TIC	
H04.01.06 Evaluar y Administrar los Riesgos de TIC (PO9)	11/01/2011	Coordinadores de Área Usuaria	Identificar los riesgos relacionados con TIC	
		Apoyo Gestión TIC	Evaluar y medir los riesgos ocasionados	
		Control de Gestión TIC	Mantener y monitorear un plan de acción de riesgos	
		Arquitecto en Jefe*	Planear las acciones correctivas a los riesgos	
		Supervisor de Operaciones*	Implantar los planes de acción relacionados con las operaciones	

Continúa →

NOMBRE SUBPROCESO	FECHA PUBLICACIÓN	RESPONSABLES/ROL	ACTIVIDAD/PROCEDIMIENTO	APROBACIÓN
		Coordinador Sénior de Aplicaciones	Implantar los planes de acción relacionados con las aplicaciones	
		Subgerente de TIC	Aprobar los planes de acciones correctivas respecto a los riesgos	Aprobar los planes de acciones correctivas respecto a los riesgos
		Gerente de Desarrollo Organizacional	Crear el marco de trabajo y estándares para la evaluación de riesgos	Aprobar y garantizar el financiamiento de los planes de acción de riesgos
H04.01.07 Administrar Proyectos de TIC (PO10)	11/01/2011	Administrador de Proyecto de TIC	Establecer y mantener un marco de trabajo para la administración de proyectos de TIC	
		Subgerente de TIC		Autorizar el marco de trabajo, políticas y métodos de aseguramiento y revisión de proyectos
H04.02 Adquirir e Implantar TIC (AI)				
H04.02.01 Identificar Soluciones Automatizadas (AI1)	11/01/2011	Arquitecto en Jefe*	Liderar el grupo de trabajo para los requerimientos generados por las áreas usuarias	
		Administrador de Proyectos de TIC	Conducir un estudio de pre-factibilidad y analizar sus riesgos	
		Coordinador Del Área Usuaria	Definir los requerimientos funcionales	
		Coordinador Sénior de Aplicaciones	Definir los requerimientos técnicos	

Continúa →

NOMBRE SUBPROCESO	FECHA PUBLICACIÓN	RESPONSABLES/ROL	ACTIVIDAD/PROCEDIMIENTO	APROBACIÓN
		Subgerente de TIC	Evaluar los beneficios operativos de TIC	
		Gerente de Desarrollo Organizacional		Aprobar autorizar las soluciones automatizadas propuestas
H04.02.02 Adquirir y Mantener Software Aplicativo (AI2)	11/01/2011	Oficial de Seguridad*	Definir las políticas de acceso y modificación de la información	
		Administrador de Proyectos de TIC	Verificar que el software cumpla con los requerimientos realizados por el área usuaria	
		Coordinador Sénior de Aplicaciones	Dar seguimiento y administrar los requerimientos de la aplicación	Aprobar los planes de adquisición y mantenimiento
H04.02.03 Adquirir y Mantener Infraestructura Tecnológica (AI3)	11/01/2011	Analista de TI (Aplicaciones)	Aplicar el procedimiento de generación requerimiento, previo a la adquisición de bienes y/o contratación de servicios	
		Técnico Líder de Infraestructura Y Comunicaciones	Aplicar el procedimiento de generación requerimiento, previo a la adquisición de bienes y/o contratación de servicios	
		Supervisor de Infraestructura Y Comunicaciones	Aplicar el procedimiento de generación requerimiento, previo a la adquisición de bienes y/o contratación de servicios	
		Arquitecto En Jefe*	Definir estrategia y planear la instalación y el mantenimiento de infraestructura	

Continúa →

NOMBRE SUBPROCESO	FECHA PUBLICACIÓN	RESPONSABLES/ROL	ACTIVIDAD/PROCEDIMIENTO	APROBACIÓN
		Coordinador Sénior de Aplicaciones	Definir estrategia y planear la instalación y el mantenimiento de infraestructura/ configurar componentes de la infraestructura	
H04.02.04 Facilitar la Operación y el Uso (AI4)	11/01/2011	Coordinador de Área Usuaria	Verificar y aprobar los manuales de usuario	
		Gestión Documental y Entrenamiento*	Generar el manual de usuario	
		Supervisor de Operaciones	Revisar los manuales de operación y administración	Aprobar los manuales de operación y administración
		Coordinador Sénior de Aplicaciones	Revisar los manuales de usuario en coordinación con el área usuaria	Aprobar los manuales de usuarios
H04.02.05 Administrar Cambios (AI6)	11/01/2011	Coordinador de Área Usuaria	Crear la necesidad del cambio	
		Administrador de Proyectos de TIC*	Evaluar el impacto del cambio	
		Arquitecto en Jefe*	Evaluar el impacto del cambio	
		Supervisor de Operaciones*	Evaluar el impacto del cambio	Priorizar y autorizar el cambio
		Coordinador Sénior de Aplicaciones	Evaluar el impacto del cambio y dar la prioridad	Priorizar y autorizar el cambio
H04.02.06 Instalar y Acreditar Soluciones y Cambios (AI7)	11/01/2011	Coordinadores de Áreas de TIC	Ejecutar las modificaciones del sistema y las pruebas de integración en el ambiente de prueba	
		Supervisor de Operaciones*	Recomendar la liberación a producción	
		Coordinador Sénior de Aplicaciones	Recomendar la liberación a producción	Aprobar la liberación a producción

Continúa →

NOMBRE SUBPROCESO	FECHA PUBLICACIÓN	RESPONSABLES/ROL	ACTIVIDAD/PROCEDIMIENTO	APROBACIÓN
H04.03 Entregar y Dar Soporte de TIC (DS)				
H04.03.01 Definir y Administrar los Niveles de Servicio (DS1)	11/01/2011	Apoyo de Gestión de TIC*	Elaborar los SLA[42] y catálogos de servicio	
		Supervisor de Operaciones	Acordar los OLA[43]	Aprobar los OLA
		Coordinador Sénior de Aplicaciones	Acordar los OLA	
		Coordinador Sénior de Soporte a Usuarios	Acordar los olas con los clientes	Aprobar los SLA
H04.03.02 Administrar los Servicios de Terceros (DS2)	11/01/2011	Apoyo de Gestión de TIC	Seguimiento y definición de los procedimientos para los contratos con terceros	
		Supervisor de Operaciones	Gestionar los riesgos del contrato y elaborar un plan de contingencia	
		Coordinador Sénior de Aplicaciones	Monitorear la prestación del servicio del proveedor respecto a las aplicaciones	
		Subgerente de TIC	Evaluar las metas de largo plazo para la relación del servicio para todos los interesados	Actualizar los planes de contratación sobre los servicios y posibles modificaciones a las contrataciones actuales

Continúa →

[42] SLA: Acuerdos de Nivel de Servicio

[43] OLA: Acuerdos de Nivel de Operación

NOMBRE SUBPROCESO	FECHA PUBLICACIÓN	RESPONSABLES/ROL	ACTIVIDAD/PROCEDIMIENTO	APROBACIÓN
H04.03.03 Administrar el Desempeño y la Capacidad (DS3)	11/01/2011	Supervisor de Operaciones	Establecer la planificación, el monitoreo y el diseño futuro de los desempeños de los recursos de TIC	Establecer y aprobar los umbrales para los KPI[44] y KGI[45]
		Coordinador Sénior de Aplicaciones	Realizar análisis de brechas para identificar incompatibilidad de los recursos de TIC	Aprobar el plan para disminuir la brechas
H04.03.04 Garantizar la Continuidad del Servicio (DS4)	11/01/2011	Apoyo Gestión de TIC	Definir y ejecutar los procedimientos de control de cambios, capacitación y mantener los planes de continuidad	
		Administrador de Proyectos de TIC*	Asegurar que el plan de continuidad este vigente	
		Supervisor de Operaciones*	Definir procedimientos para la continuidad de TIC	
		Coordinador Sénior de Aplicaciones	Definir los procedimientos para la continuidad de TIC	
H04.03.05 Garantizar la	18/07/2012	Control de Gestión TIC	Definir y mantener un plan de seguridad de ti. Evaluar vulnerabilidades y derechos de accesos	

Continúa →

[44] KPI: Indicadores Clave de Desempeño

[45] KGI: Indicadores Clave de Éxito

NOMBRE SUBPROCESO	FECHA PUBLICACIÓN	RESPONSABLES/ROL	ACTIVIDAD/PROCEDIMIENTO	APROBACIÓN
Seguridad de los Sistemas (DS5)		Arquitecto en Jefe*	Definir, establecer y operar un proceso de administración de identidad (cuentas)	
		Coordinador Sénior de Aplicaciones	Implementar y mantener controles técnicos y de procedimiento para proteger el flujo de información a través de las redes	
		Supervisor de Operaciones*	Registrar incidentes de seguridad reales y potenciales. Establecer procedimientos para salvaguardar llaves criptográficas	Aprobar procedimientos respecto a la seguridad de los servicios brindados por TIC.
H04.03.06 Identificar y Asignar Costos (DS6)	11/01/2011	Apoyo Gestión de TIC	Mapear la infraestructura, identificar todos los costos, establecer y mantener proceso de control con los servicios de TIC	
H04.03.07 Administrar la Mesa de Servicio y los Incidentes (DS8)	11/01/2011	Analista de Soporte A Usuario	Registrar, atender, solucionar y reportar incidentes	
		Arquitecto En Jefe*	Liderar el diseño de los procedimientos de la mesa de servicios	
		Supervisor de Operaciones	Resolver, recuperar y cerrar incidentes que han sido escalados	
		Coordinador Sénior de Aplicaciones	Resolver, recuperar y cerrar incidentes que han sido escalados. Elaborar procedimientos para atender requerimientos sobre las aplicaciones, administrar la gestión de incidentes	
		Coordinador Sénior de Soporte A Usuarios	Resolver, recuperar, cerrar incidentes y diagnosticar consultas	Administrar la gestión de incidentes
	11/01/2011	Apoyo Gestión de TIC*	Actualizar el repositorio de configuración	

Continúa →

NOMBRE SUBPROCESO	FECHA PUBLICACIÓN	RESPONSABLES/ROL	ACTIVIDAD/PROCEDIMIENTO	APROBACIÓN
H04.03.08 Administrar la Configuración (DS9)		Arquitecto En Jefe*	Actualizar el repositorio de configuración	
		Supervisor de Operaciones*	Actualizar el repositorio de configuración	
		Supervisor de Configuraciones*	Desarrollar procedimientos de planeación de administración de la configuración. Recopilar, verificar y auditar la información de configuraciones	Aprobar y actualizar los procedimientos y repositorio de configuraciones
H04.03.09 Administrar los Problemas de TIC (DS10)	11/01/2011	Apoyo Gestión de TIC*	Identificar, clasificar, revisar el estado de problemas y analizar la causa raíz	
		Administrador de Proyectos de TIC*	Resolver problemas	
		Arquitecto en Jefe*	Resolver problemas	
		Coordinador Sénior de Aplicaciones	Resolver problemas	
		Supervisor de Operaciones*	Revisar el estado del problema	Clasificar las soluciones conocidas
H04.03.10 Administrar los Datos de TIC (DS11)	11/01/2011	Arquitecto en Jefe*	Traducir los requerimientos de almacenamiento y conservación a procedimientos	
		Supervisor de Operaciones*	Definir, mantener e implementar procedimientos para: administración de librerías de medios, restauración de datos y descartar de forma segura medios y equipos	Autorizar la ejecución de los procedimientos establecidos
H04.03.11 Administrar las Operaciones de TIC (DS13)	11/01/2011	Supervisor de Operaciones*	Crear, modificar, administrar, resolver, programar, asegurar la continuidad de los servicios de TIC	Autorizar los planes de operación, mantenimiento y escalamiento de la infraestructura de TIC

Continúa →

NOMBRE SUBPROCESO	FECHA PUBLICACIÓN	RESPONSABLES/ROL	ACTIVIDAD/PROCEDIMIENTO	APROBACIÓN
H04.04 Monitorear y Evaluar TIC (ME)				
H04.04.01 Monitorear y Evaluar el Desempeño de TIC (ME1)	11/01/2011	Coordinador de Área Usuaria	Identificar y validar los objetivos medibles	
		Coordinador Sénior de Aplicaciones	Crear los scorecards[46]	
		Supervisor de Operaciones*	Crear los scorecards	
		Subgerente de TIC	Establecer el enfoque de monitoreo	Aprobar los scorecards
H04.04.02 Garantizar el Cumplimiento Regulatorio (ME3)	11/01/2011	Coordinador de Área Usuaria	Evaluar cumplimiento de actividades de ti con políticas, estándares y procedimientos de TIC	
		Apoyo Gestión de TIC*	Evaluar cumplimiento de actividades de ti con políticas, estándares y procedimientos de TIC	
		Administrador de Proyectos de TIC	Garantizar el cumplimiento regulatorio	
		Arquitecto En Jefe*	Evaluar cumplimiento de actividades de TIC con políticas, estándares y procedimientos de TIC	
		Supervisor de Operaciones	Evaluar cumplimiento de actividades de TIC con políticas, estándares y procedimientos de TIC	

Continúa →

[46] SCORECARDS: Se refiere a la identificación de las medidas financieras y no financieras con sus metas asociadas; bajo el esquema del Cuadro de Mando Integral o BSC, por sus siglas en inglés.

NOMBRE SUBPROCESO	FECHA PUBLICACIÓN	RESPONSABLES/ROL	ACTIVIDAD/PROCEDIMIENTO	APROBACIÓN
		Coordinador Sénior de Aplicaciones	Evaluar e integrar los reportes del cumplimiento de actividades de TIC con políticas, estándares y procedimientos de TIC	Aprobar procesos, procedimientos y políticas respecto de los cumplimientos regulatorios
		Gerente de Desarrollo Organizacional	Definir y ejecutar un proceso para identificar los requerimientos legales, contractuales, políticas y regulatorios	Informar a los entes de control

3.2 Análisis de los servicios y productos ofrecidos por la Subgerencia de Tecnologías de la Información y Comunicación de EP PETROECUADOR

Los servicios y productos ofrecidos por la STIC, se encuentran identificados en el Catálogo de Servicios de TIC de EP PETROECUADOR de la Tabla 7. En donde se ha tratado de resumir y agrupar los servicios afines o con características similares; esto se debe a que el catálogo original detalla servicios de acuerdo a los aplicativos existentes, que en muchos casos son soluciones de legado, aisladas y con tecnologías distintas como resultado de las varias modificaciones organizativas y estructurales que ha sufrido la empresa, hasta la creación de la actual Empresa Estatal.

Tabla 7 Catálogo de Servicios de la STIC

SERVICIO	DESCRIPCIÓN DEL SERVICIO	ÁREA RESPONSABLE	OBSERVACIONES
FAMILIA DE SERVICIOS CORPORATIVOS			
Equipos de cómputo de oficina	Mantenimiento de equipos de escritorio, portátiles, escáneres, impresoras, proyectores, entre otros.	Coordinación Sénior de Soporte a Usuario	
Aplicaciones de escritorio	Instalación, actualización y configuración de los programas y utilitarios empresariales.	Coordinación Sénior de Soporte a Usuario	Incluye: antivirus, clientes de correo, terminales para aplicaciones AS/400, aplicaciones ofimáticas, entre otras.
Impresión	Impresión de boletines de noticias relacionados a EP PETROECUADOR	Coordinación Sénior de Soporte a Usuario	
Correo electrónico	Sistema para intercambio de información por vía electrónica, a través de las aplicaciones cliente o el portal web.	Coordinación Sénior de Datos	Se considera dentro de este servicio, la emisión de comunicados corporativos y boletines electrónicos
Alojamiento WEB	Brinda almacenamiento, y pone a disposición de los usuarios material multimedia, aplicaciones, archivos, entre otros.	Coordinación Sénior de Datos Coordinación Sénior de Aplicaciones	Este servicio está disponible para todos los servicios y aplicaciones, propias de EP PETROECUADOR, desplegadas en intranet e internet.
Radio fijo-móvil	Servicio de comunicaciones VHF[47] half-duplex móviles.	Coordinación Sénior de Infraestructura y comunicaciones	

Continúa →

[47] VHF: Rango de frecuencia comprendido entre los 30 y los 300 MHz, Very High Frecuency por sus siglas en inglés

SERVICIO	DESCRIPCIÓN DEL SERVICIO	ÁREA RESPONSABLE	OBSERVACIONES
Servicios de internet	Es el conjunto de redes interconectadas, internas y externas, que da soporte a protocolos para transmisión e intercambio de imágenes, archivos, telefonía, correo electrónico etc.	Coordinación Sénior de Infraestructura y comunicaciones	
Telefonía	Es el servicio telefónico como tal	Coordinación Sénior de Infraestructura y comunicaciones	Incluye los servicios tradicionales y la telefonía IP.
Video conferencia	Comunicación multimedia en tiempo real, para la realización de reuniones desde múltiples sitios remotos de forma simultánea.	Coordinación Sénior de Infraestructura y comunicaciones	
Servicios para plataforma AS/400	Mantenimiento y a actualización de las aplicaciones y servidores AS/400. Monitoreo, soporte y gestión de usuarios.	Coordinación Sénior de Datos	Está relacionado a varios sistemas corporativos para: Recursos Humanos, Contratos, Costos, Finanzas-Contabilidad, Abastecimientos, Gestión de mantenimiento, Gestión de Activos.
		Coordinación Sénior de Aplicaciones	Se identifica como un servicio especializado debido a que varias de las aplicaciones de los sistemas AS/400 ya no cuentan con soporte oficial del fabricante, o han sufrido varias personalizaciones para que se adapten a las necesidades de la empresa.
Data Warehouse / data	Mantenimiento de los repositorios de información y los programas de inteligencia de negocios.	Coordinación Sénior de Datos	
		Coordinación Sénior de Aplicaciones	

Continúa →

SERVICIO	DESCRIPCIÓN DEL SERVICIO	ÁREA RESPONSABLE	OBSERVACIONES
Gestión documental	Gestión de contenido y flujos de trabajo	Coordinación Sénior de Aplicaciones	
Aplicaciones complementarias	Desarrollo, soporte, mantenimiento de múltiples aplicaciones que complementan los sistemas corporativos o atienden necesidades puntuales de las áreas usuarias de la empresa.	Coordinación Sénior de Aplicaciones	Incluye los siguientes aplicativos: Agenda, control de asistencia, control de bodega, control de gastos médicos, control de pólizas y seguros, empresa por resultados, registro de proveedores, seguimiento de resoluciones, auditoría y control, órdenes de pago, sistema para acceso a documentos públicos (Lexis), viáticos, seguimiento de juicios y coactivas.
FAMILIA DE SERVICIOS DE LA GERENCIA DE COMERCIALIZACIÓN			
Sistemas de Comercialización	Desarrollo, soporte, mantenimiento y operación de aplicaciones e infraestructura de TIC especializada.	Coordinación Sénior de Aplicaciones	Sistemas relacionados con los procesos de comercialización de hidrocarburos, movimiento de productos, despacho transporte y almacenamiento, autorizaciones electrónicas para compra de combustibles
FAMILIA DE SERVICIOS DE LA GERENCIA DE COMERCIO INTERNACIONAL			
Sistemas de Comercio Exterior	Desarrollo, soporte, mantenimiento y operación de aplicaciones e infraestructura de TIC especializada.		Comercio exterior, viajes para transporte marítimo, registro y generación de invitaciones.
FAMILIA DE SERVICIOS DE LA GERENCIA DE REFINACIÓN			
Sistemas de Refinación	Soporte, mantenimiento y operación de aplicaciones e infraestructura de TIC especializada.	Coordinación Sénior de Aplicaciones	Control de plantas, control de operaciones, control y adquisición de datos, interfaces humano-máquina, simulación de plantas, balanceó másico, información geográfica.

Continúa →

SERVICIO	DESCRIPCIÓN DEL SERVICIO	ÁREA RESPONSABLE	OBSERVACIONES
Comunicación VHF marina	Comunicación de voz half duplex a través de radios VHF para operaciones en el Terminal Marítimo.	Coordinación Sénior de Infraestructura y comunicaciones	
Telefonía de operación	Sistema de comunicación multiconferencia encriptado para coordinación de las operaciones del poliducto.	Coordinación Sénior de Infraestructura y comunicaciones	

3.3 Análisis de la Seguridad de la Información de EP Petroecuador

3.3.1 *Análisis de los informes de Hacking Ético de EP Petroecuador*

EP PETROECUADOR, como parte de las iniciativas de modernización tecnológica que está ejecutando, contrató en el año 2012 los servicios de consultoría para la realización de pruebas de Hacking Ético[48] en la infraestructura tecnológica, de la empresa. Los objetivos principales de la consultoría fueron los siguientes:

- Identificar riesgos potenciales de seguridad informática y oportunidades de mejora.
- Identificar potenciales problemas de seguridad, fraudes o fugas de información que puedan encontrarse en el personal o elementos tecnológicos.
- Priorizar un plan de acción de acuerdo al nivel de impacto de los riesgos identificados.
- Establecer recomendaciones, de acuerdo a las buenas prácticas de seguridad, para mitigar los riesgos identificados.

[48] HACKING ÉTICO: Actividad realizada por un experto que conoce y entiende las vulnerabilidades de los sistemas informáticos, que tiene como objetivo realizar pruebas de penetración con herramientas y técnicas similares a las usadas por intrusos o crackers

3.3.1.1 Metodología de las pruebas de Hacking Ético

Las pruebas realizadas en la infraestructura tecnológica de EP PETROECUADOR, fueron alineadas de acuerdo a las metodologías, internacionalmente reconocidas, OSSTMM[49] y OWASP[50].

La metodología aplicada puede resumirse, en pasos ordenados, de la siguiente manera:

1. Recolección de información enfocándose en pruebas blackbox[51], y en algunos casos utilizando información proporcionada por EP PETROECUADOR para acelerar los procedimientos a ser ejecutados.
2. Análisis y clasificación de vulnerabilidades utilizando herramientas automatizadas, escaneo de puertos, documentación, manuales y análisis de tráfico.
3. Ejecución del ataque sobre un grupo determinado de vulnerabilidades detectadas, con el objetivo de diferenciar las teóricas y las reales.

[49] OSSTMM: Manual de metodología abierta para pruebas de seguridad. Open Source Security Testing Methodology Manual, por sus siglas en inglés.

[50] OWASP: Proyecto abierto de seguridad de aplicaciones web. Open Web Application Security Project, por sus siglas en inglés.

[51] PRUEBAS BLACKBOX: En el ámbito del Hacking Ético, son pruebas realizadas sobre una infraestructura tecnológica de la cual se ha proporcionado poca o ninguna información por parte del cliente, con el objetivo de simular un ambiente más similar al que se enfrentaría un atacante real.

4. Análisis final y documentación, en donde se detalla las vulnerabilidades reales, se descarta los falsos positivos[52], y se define el plan de acción o recomendaciones específicas.

Las actividades de la empresa consultora fueron divididas, en relación a la infraestructura tecnológica, en pruebas: externas e internas. Esta diferenciación consideró características específicas para cada grupo de pruebas, con el objetivo de formar un escenario para la simulación de ataques externos desde internet y otro para ataques internos desde intranet.

3.3.1.2 Equipos utilizados para las pruebas de Hacking Ético

Los equipos utilizados para las pruebas de Hacking Ético comprenden computadores portátiles con software de virtualización para la ejecución de distribuciones Linux[53]. Las distribuciones de Linux son sistemas operativos a los cuales se les ha instalado y configurado, un conjunto de herramientas de software que han sido desarrolladas y seleccionadas por profesionales en seguridad, y comunidades a fines. Las herramientas que normalmente son incluidas en estas distribuciones Linux se clasifican, según su funcionalidad, en los siguientes grupos:

- Recolección de Información
- Evaluación de vulnerabilidades
- Herramientas de explotación

---

[52] FALSO POSITIVO: Se considera aquella vulnerabilidad que durante la ejecución de las pruebas se presentó y fue reportada, pero al corroborarlo y analizarlo en detalle no se materializa como riesgo, bien sea por las condiciones técnicas del servidor o porque simplemente no aplica.

[53] DISTRIBUCIÓN LINUX: Sistema operativo basado en el núcleo Linux, el cual es acompañado de un grupo de paquetes de software específico, de acuerdo a las necesidades de los usuarios finales o corporativos.

- Escalamiento de privilegios
- Mantenimiento o persistencia de acceso
- Ingeniería inversa
- Pruebas de estrés
- Informática forense

3.3.1.3 Resultados de las pruebas externas de Hacking Ético de EP PETROECUADOR

Las pruebas externas fueron realizadas sobre los siguientes dominios públicos:

Tabla 8 Dominios para pruebas de Hacking Ético Externo

DOMINIO	GERENCIA/UBICACIÓN
eppetroecuador.ec	Matriz, Gerencia General
tra.eppetroecuador.ec	Transporte y almacenamiento
com.eppetroecuador.ec	Comercialización
ind.eppetroecuador.ec, petroindustrial.com.ec	Industrialización
sig.eppetroecuador.ec	Seguridad, salud y ambiente

El número de equipos analizados, dentro de los dominios antes detallados, fue de 23, de los cuales el 39% se encuentra afectado por vulnerabilidades, como se detalla en la Figura 27.

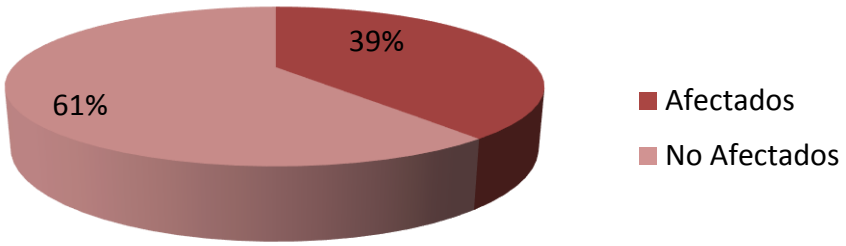

Figura 27 Equipos externos afectados por vulnerabilidades

Las vulnerabilidades detectadas en la infraestructura externa de EP PETROECUADOR se resumen en la siguiente tabla:

Tabla 9 Vulnerabilidades EP Petroecuador para pruebas externas

Vulnerabilidad	Equipos afectados	CVE[54]	Descripción de la vulnerabilidad
Inyección SQL Blind	1	OWASP-DV-005	Permite realizar consultas sobre el servidor de base de datos utilizando la interfaz de la aplicación, de esta manera un atacante puede obtener información de retorno de los objetos y tablas existentes.
Stored Cross Site Scripting (XSS)	1	OWASP-DV-002	Ocurre cuando una aplicación web solicita información y la almacena para un uso posterior, si esta información no es filtrada, un atacante puede ingresar código malicioso que luego puede ser ejecutado como parte de la aplicación web.
Servicio FTP con usuario anonymous habilitado	2	1999-0497	Permite ingresar al servidor ftp sin utilizar credenciales de autentificación, exponiendo la información empresarial que se encuentre en este servidor, o permitiendo la carga de exploits[55].
Usuarios y contraseñas débiles	2	N/A	Las contraseñas o claves utilizadas para la validación en las consolas de administración de las aplicaciones utilizan palabras comunes y pueden ser susceptibles a ataques por diccionario.

Continúa →

[54] CVE: Vulnerabilidades y Exposiciones Comunes, Common Vulnerabilities and Exposures por su siglas en inglés, es un diccionario de nombres comunes para las vulnerabilidades de seguridad de información de conocimiento público. (MITRE, 2013)

[55] EXPLOIT: Es un fragmento de código o conjunto de comandos que se utiliza para aprovechar una vulnerabilidad de seguridad de un sistema de información, logrando que este se comporte una manera determinada.

Vulnerabilidad	Equipos afectados	CVE[54]	Descripción de la vulnerabilidad
Acceso a configuración del servidor mediante componente instalado en el mismo	1	N/A	Las aplicaciones web exponen componentes que pueden ejecutar código de configuración. Estos componentes normalmente no están disponibles en un ambiente de producción.
Servicio SMTP relay habilitado	2	CVE-1999-0512 CVE-2002-1278 CVE-2003-0285	Los servidores SMTP[56] permiten el envío de correos mediante línea de comandos, de esta manera un atacante puede suplantar la identidad del remitente para obtener información, trasmitir información falsa, generar eventos inmorales, entre otros.
Consolas de acceso permiten acceder a información privada o confidencial	1	OWASP-CM-007	Las aplicaciones web exponen sus consolas de administración sin filtrado de direcciones IP o con autentificación débil.
Divulgación de información a través de archivos no referenciados	1	OWASP-CM-006	Algunas aplicaciones web permiten la indexación de directorios, de esta manera se puede obtener gran cantidad de archivos y los metadatos asociados. Son fuente de información para ataques más elaborados.
Directorio con publicación de scripts y código fuente PHP	1	OWASP-CM-004	Las aplicaciones exponen directorios con código fuente y archivos de configuración de las aplicaciones, lo cual permite obtener información de otros equipos de la red interna.

Continúa →

[56] SMTP: Protocolo simple para transferencia de correo, Simple Mail Transfer Protocol por sus siglas en inglés.

Vulnerabilidad	Equipos afectados	CVE[54]	Descripción de la vulnerabilidad
Archivo Robots.txt se encuentra habilitado en el sitio web	1	N/A	Los sitios web tienen habilitado el archivo robots.text, que se utiliza para la indexación de páginas a través de buscadores. Puede proveer a un atacante, la ruta de los directorios que contiene el sitio, facilitando la búsqueda de archivos que brinden información sobre configuración.
Puntos de acceso/login web podrían permitir la intercepción de información en texto claro	1	N/A	Las páginas de login o autentificación no utilizan un protocolo seguro que cifre la comunicación entre el cliente y el servidor. La información de usuario y contraseña viajan por la red en texto plano y podrían ser recuperados por un atacante que se encuentre analizando el tráfico de red.
Métodos tipo TRACE habilitados en el servidor	1	CVE-2003-1567 CVE-2004-2320 CVE-2010-0386	Los servidores tienen habilitados los métodos de tipo HTTP TRACE, mediante la cual un atacante podría extraer información sensible respecto a la configuración del servidor o información relacionada con las sesiones de los usuarios conectados.

3.3.1.4 Resultados de las pruebas internas de Hacking Ético de EP PETROECUADOR

Las pruebas internas fueron realizadas sobre los siguientes objetivos de análisis:

Tabla 10 Objetivos de análisis para pruebas internas de Hacking Ético

Tipo	Características	Tipo de pruebas
Segmentos de Red	Edificio Alpallana (Quito)	Escaneo de puerto, explotación de vulnerabilidades, suplantación y captura de tráfico Wireless, monitoreo de tráfico, envenenamiento ARP.
	Edificio Plaza Lavi (Quito)	
	Edificio El Rocío (Quito)	
	Edificio la Previsora (Guayaquil)	

Continúa →

Tipo	Características	Tipo de pruebas
Servidores	Servidores distribuidos en 3 VLAN[57]	Inyección sql y malformación de parámetros, cross site scripting, escaneo de puertos, análisis de código fuente generado (HTML, Javascript), manipulación de controles, data fuzzing[58].
Dominios	3 controladores de dominio	Envenenamiento ARP, ataques de hombre en el medio, explotación de vulnerabilidades.
Computadores personales	Varios equipos seleccionados al azar	Ataques de fuerza bruta, ataque de hombre en el medio, pruebas de obtención de huellas.

Las vulnerabilidades detectadas en la infraestructura interna de EP PETROECUADOR se resumen en la siguiente tabla:

Tabla 11 Vulnerabilidades EP Petroecuador para pruebas internas

Vulnerabilidad	Equipos afectados	CVE	Descripción de la vulnerabilidad
Enumeración de servicios y versiones	376	N/A	Los equipos probados entregan fácilmente información que permite identificar, sistema operativo, versiones, servicios. Esta información permite planificar un ataque más elaborado
Protocolo de cifrado débil SSL	49	N/A	La versión de SSL usada en algunos servidores es antigua y se considera obsoleta, debido a varias vulnerabilidades que pueden ser aprovechadas por los atacantes.
Escritorio Remoto podrían permitir la ejecución de código remoto	122	CVE-2012-0002 CVE-2012-0152	Se refiere a una vulnerabilidad del protocolo RDP[59] utilizado por Windows, en donde es posible la captura de la sesión para la ejecución de un exploit de negación de servicio.

Continúa →

[57] VLAN: Red de área local virtual, Virtual Local Area Network, por sus siglas en inglés.

[58] DATA FUZZING: Técnica que consiste en proporcionar a los sistemas y aplicaciones información incorrecta, incompleta o aleatoria con el objeto de detectar vulnerabilidades o fallas de pérdida de memoria.

[59] RDP: Protocolo de escritorio remoto, Remote Desktop Protocol por sus siglas en inglés.

Vulnerabilidad	Equipos afectados	CVE	Descripción de la vulnerabilidad
DNS[60] Cache snooping	14	N/A	Permite conocer que direcciones resuelve el servidor DNS, de esta manera se podría elaborar un ataque de secuestro de sesión o derivados, de acuerdo a los hábitos de navegación de los usuarios.
Escritorio remoto susceptible a ataques de hombre en el medio	168	CVE-2005-1794	Esta vulnerabilidad podría permitir que un atacante tome el control del equipo afectado, debido a un manejo inadecuado del manejo de sesiones
Múltiples Vulnerabilidades en HP Data Protector < 06.20	34	CVE-2011-0923 CVE-2011-728 CVE-20111729 CVE-2011-1730 CVE-2011-1731 CVE-2011-1732 CVE-2011-1733 CVE-2011-1734 CVE-2011-1735 CVE-2011-1736 CVE-2011-2399	Las vulnerabilidades detectadas podrían permitir ejecutar código remoto, elevación de privilegios tomando control total del equipo y su información.
Múltiples vulnerabilidades en HP System Managment	22	CVE-2008-1468 CVE-2008-4226 CVE-2008-5557 CVE-2008-5814 CVE-2009-1377 CVE-2009-1378 CVE-2009-1379 CVE-2009-1386 CVE-2009-1387 CVE-2009-4185 CVE-2010-1034 CVE-2010-1917 CVE-2010-2531 CVE-2010-2939 CVE-2010-2950 CVE-2010-3709 CVE-2010-4008 CVE-2010-4156 CVE-2011-1540 CVE-2011-1541	Las vulnerabilidades detalladas permiten evadir los controles de acceso permitiendo acceso a las consolas administrativas del servidor.
HP Data Protector permite ejecución de comandos	32	CVE-2011-0923	Esta vulnerabilidad permite en el caso de sistemas operativos Windows, la ejecución de comandos sin parámetros, y en sistemas Linux/Unix es posible tener acceso al usuario root comprometiendo totalmente el servidor.

Continúa →

[60] DNS: Servicio de nombre de dominio, Domain Name Service por sus siglas en inglés.

Vulnerabilidad	Equipos afectados	CVE	Descripción de la vulnerabilidad
Sesiones nulas activas (Windows SMB NULL)	115	CVE-1999-0519 CVE-1999-0520 CVE-2002-1117	Permite utilizar credenciales nulas para autenticarse con el servidor, de esta manera se puede enumerar servicios y conocer algunas configuraciones del equipo.
Microsoft SQL Server ejecución de código remoto	13	CVE-2008-5416	Vulnerabilidad relacionada con la ejecución de código en el procedimiento almacenado extendido "sp_replwritetovarbin", en donde los parámetros no están bien filtrados.
Múltiple escalado de privilegios en Microsoft SQL Server	9	CVE-2008-0085 CVE-2008-0086 CVE-2008-0106 CVE-2008-0107	Vulnerabilidad que le permite a un usuario autentificado, escalar sus privilegios y tomar control de objetos y esquemas de la base de datos a los cuales no fue autorizado.
Credenciales por defecto en Microsoft SQL Server	5	CVE-1999-0508	La cuenta "sa", que forma parte de la instalación por defecto de Microsoft SQL Server, está configurada con la contraseña por defecto permitiendo que cualquier usuario ingrese con privilegios elevados a la base de datos.
Credenciales por defecto en PostgreSQL Server	1	CVE-1999-0508	La cuenta "postgres", no tiene configurada la contraseña permitiendo que cualquier usuario ingrese con privilegios elevados a la base de datos.
Credenciales por defecto en MySQL Server	1	CVE-2002-1809 CVE-2004-1532	La cuenta "anonymous", no tiene configurada la contraseña permitiendo que cualquier usuario ingrese con privilegios elevados a la base de datos.
Múltiples vulnerabilidades en MySQL	1	CVE-2004-0835 CVE-2004-0627 CVE-2004-8371	Existe un bug en las versiones MySQL anteriores a 4.021 y 3.23.49, en las cuales los derechos de CREATE/INSERT no son validados de forma correcta.
Credenciales por defecto db2admin en Windows	36	CVE-2001-0051	La instalación de DB2 crea por defecto la cuenta db2admin, la cual puede ser usada para comprometer los servicios, bases de datos, credenciales de otros usuarios, e información almacenada.
Múltiples vulnerabilidades en Windows permiten la ejecución de código remoto	27	ms08-067 ms05-039 ms06-040 ms04-022 ms10-054 ms05-043 ms04-011	Permite ejecución de código remoto, debido a la falta de instalación de parches de seguridad, o a fallas en los servicios Plug and Play

Continúa →

Vulnerabilidad	Equipos afectados	CVE	Descripción de la vulnerabilidad
Sistema operativo obsoleto	8	N/A	La versión de Windows 2000 server se considera obsoleta, debido a que su soporte oficial extendido finalizó el 13 de julio de 2010, y existen vulnerabilidades que ya no serán corregidas.
Múltiples vulnerabilidades en Apache	5	CVE-2007-6750 CVE-2009-3555 CVE-2010-0408 CVE-2010-0425 CVE-2010-0434 CVE-2009-2699	Varias vulnerabilidades que permiten: evadir controles de acceso, denegación de servicio, ataques de hombre en el medio por falla en la renegociación de sesiones, elevación de privilegios, etc.
Múltiples vulnerabilidades en Apache Tomcat	2	CVE-2011-1184 CVE-2011-2204 CVE-2011-2526 CVE-2011-2729 CVE-2011-3190 CVE-2011-5062 CVE-2011-5063 CVE-2011-5064 CVE-2010-4172 CVE-2008-5515	Versiones de Tomcat, anteriores a la 2.2.34, son susceptibles a vulnerabilidades de ejecución de código remoto y cross site scripting y denegación de servicio.
Credenciales por defecto en Tomcat	2	CVE-2009-3099 CVE-2009-3548 CVE-2010-0557 CVE-2010-4094	La contraseña de la consola administrativa está configurada con los valores por defecto, permitiendo el despliegue de cualquier aplicación que ejecute comandos a nivel de sistema operativo.
Múltiples Vulnerabilidades en PHP < 5.3.11	2	CVE-2011-4566 CVE-2011-4885 CVE-2012-0057 CVE-2012-0781 CVE-2012-0788 CVE-2012-0789 CVE-2012-0831 CVE-2012-1172	Varias vulnerabilidades que permiten ejecución de código remoto y denegación de servicio.
Actualización crítica de parches de Oracle	1	CVE-2009-2001 CVE-2012-0510 CVE-2012-0511 CVE-2012-0512 CVE-2012-0519 CVE-2012-0520 CVE-2012-0525	Existen varias vulnerabilidades relacionadas con actualizaciones críticas, las cuales afectan a varios módulos internos y externos del servidor Oracle.
Credenciales por defecto en dispositivo Cisco	2	CVE-2001-0051	Las claves por defecto permiten el acceso total a la configuración del equipo, y por tanto puede poner en riesgo la infraestructura de comunicaciones.
Múltiples Vulnerabilidades en Cisco IOS Software	17	CVE-2012-0385 CVE-2012-0382 CVE-2011-3271 CVE-2012-0384 CVE-2011-0946	Vulnerabilidades que permiten denegación de servicio por reinicio del equipo mediante la manipulación de paquetes.

Continúa →

Vulnerabilidad	Equipos afectados	CVE	Descripción de la vulnerabilidad
Credenciales por defecto en db2 ISERIES	1	CVE-2001-0051	El equipo ISeries tiene la contraseña por defecto del usuario QSECOFR permitiendo el control total del equipo.
Múltiples vulnerabilidades en IBM websphere	10	CVE-2010-0778 CVE-2010-0779 CVE-2010-0781 CVE-2010-3186	Las vulnerabilidades encontradas permiten evadir los controles de acceso y la ejecución de ataques de cross site scripting.
Credenciales por defecto en unix/linux	6	CVE-1999-0502 CVE-2006-5288 CVE-2012-4577	La contraseña por defecto del usuario root compromete por completo el servidor.
Overflow remoto sobre Compaq WBEM	3	CVE-2005-4823	Vulnerabilidad que permite al atacante ejecutar código remoto mediante el desborde de registros, y en algunos casos podría provocar una denegación de servicio.
DoS[61] por renegociación en protocolos TLS/SSL[62]	89	CVE-2011-1473	El protocolo TLS/SSL, requiere gran capacidad computacional para renegociar la sesiones de los usuarios, por tanto sino se controla la renegociación y el número de sesiones simultáneas, es fácilmente lograr una negación de servicio.
Acceso anónimo a FTP	14	N/A	Cualquier usuario puede conectarse al servidor ftp sin necesidad de proporcionar una contraseña, comprometiendo la información cargada en estos equipos.
Nombres por defecto en las comunidades SNMP[63]	43	CVE-1999-0186 CVE-1999-0254 CVE-1999-0472 CVE-1999-0516 CVE-1999-0517 CVE-1999-0792	Esta vulnerabilidad permite realizar cambios en las configuraciones de los sistemas utilizando los nombres de las comunidades por defecto.

[61] DoS: Denegación de servicio, Deny of service por sus siglas en inglés

[62] TSL/SSL: Transport Socket layer/Secure Socket, por sus siglas en inglés son protocolos que permiten encriptar comunicaciones a través de redes.

[63] SNMP: Protocolo simple de administración de redes, Simple Network Management Protocol por sus siglas en inglés

3.3.1.5 Resultados de las pruebas de ingeniería social

Las pruebas de ingeniería social se limitaron a recolectar información de forma pasiva de algunas instalaciones a las que se les permitió acceso a los consultores; es decir que no se utilizaron técnicas de manipulación directa sobre el personal de EP PETROECUADOR. La información que los consultores pudieron recolectar fue la siguiente:

Tabla 12 Información recolectada en pruebas de ingeniería social

Información	Condición
Usuarios y contraseñas de equipos	Notas adhesivas colocadas sobre los propios equipos
Diagramas de red explícitos	Colocados en paredes y divisiones modulares de las oficinas
Documentos con información oficial de la empresa	Arrojados en los basureros sin ser destruidos de forma adecuada
Tablas de direccionamiento IP	Abandonados sobre escritorios o mesas de trabajo

De la misma manera los consultores verificaron que los centros de datos permanecen abiertos y sin control a determinadas horas, en las cuales incluso se verificó que varios equipos son dejados encendidos sin bloquear sus respectivas sesiones.

3.3.1.6 Recomendaciones y planes de remediación para los resultados de las pruebas de Hacking Ético

Los resultados de las pruebas de Hacking ético, dieron como resultado una gran cantidad de vulnerabilidades en un número equivalente de equipos; con algunas excepciones en donde se determinó que un equipo puede estar afectado por más de una vulnerabilidad, y de la misma manera requiere un plan de remediación que contemple esta característica. Cada vulnerabilidad detectada fue valorada, utilizando criterios aceptados internacionalmente, de acuerdo a 3 parámetros: impacto, probabilidad de ocurrencia y riesgo, con el objetivo de priorizar los planes de remediación.

Las recomendaciones realizadas por la empresa consultora fueron clasificadas en 3 grupos principales: aplicación o software, infraestructura y gestión. Esta clasificación obedece al ámbito en donde el plan de remediación se enfocará, el alcance que este tendrá y los responsables o involucrados. Tomando en cuenta esta diferenciación, en la Tabla 13 se detalla las recomendaciones realizadas por la empresa consultora.

Tabla 13 Recomendaciones Hacking Ético

Ámbito	Recomendación	Responsables
Aplicación / Software	Instalar parches y actualizaciones de los sistemas operativos.	Coordinaciones de aplicaciones, datos y soporte usuarios
	Renovar software obsoleto.	
	Desactivar los servicios no utilizados	
	Instalar y actualizar software anti virus	
	Cambiar contraseñas y parámetros por defecto	
	Utilizar una política de contraseñas fuertes	
	Utilizar técnicas de programación segura	
	Eliminar o desactivar cuentas y usuarios por defecto	
	Utilizar del criterio de menor privilegio en la asignación de permisos	
	Depurar el contenido de los servidores web, publicar el contenido estrictamente necesario para servicios de intranet e internet.	
	Utilizar protocolos de comunicación segura donde sea posible	
	Personalizar las instalaciones de software, o no utilizar las instalaciones por defecto.	
	Activar opciones de seguridad opcionales	

Continúa →

Ámbito	Recomendación	Responsables
Infraestructura	Instalar sistemas de prevención de intrusos	Coordinación de infraestructura y telecomunicaciones
	Actualizar el firmware de los dispositivos de red	
	Configurar equipos de seguridad perimetral utilizando el criterio de menor privilegio	
	Cambiar usuarios y contraseñas por defecto	
	Controlar el acceso a los puntos de red	
	Restringir el acceso físico a los centros de datos y equipos de red	
Gestión	Elaborar políticas y procedimientos de seguridad de la información	STIC, procesos, coordinaciones de aplicaciones, datos, soporte usuarios, e infraestructura y comunicaciones
	Definir políticas y estándares para el desarrollo y publicación de aplicaciones	
	Establecer pruebas periódicas de seguridad de aplicaciones e infraestructura	
	Establecer métodos de control y cumplimiento de las políticas y procedimientos de seguridad	
	Establecer políticas para el uso de contraseñas	
	Capacitar al personal y socializar las iniciativas de seguridad	

3.3.2 *Análisis del plan de mejoras planteado por Deloitte para la seguridad de la información de EP Petroecuador.*

La consultora Deloitte, como parte de su diagnóstico y recomendaciones realizadas a EP PETROECUADOR, planteó un plan de mejoras para cada unidad de negocio o unidad funcional de la empresa. En el caso de la STIC, las iniciativas de

mejora identificadas fueron 14, de las cuales 2 se encuentran directamente relacionadas con la estructura funcional, políticas, procesos y los procedimientos de la S-I.

3.3.2.1 Plan para definir las políticas y procedimientos faltantes relacionados con la seguridad de la información

El objetivo principal de este plan de mejora es establecer un marco de trabajo que permita administrar la seguridad de los activos de TI, en el que se definan las políticas, objetivos, procesos y procedimientos relacionados con la S-I con el fin de manejar el riesgo, mejorar la seguridad y entregar resultados alineados a los objetivos de la organización. El plan propuesto de esta iniciativa se detalla en la Figura 28.

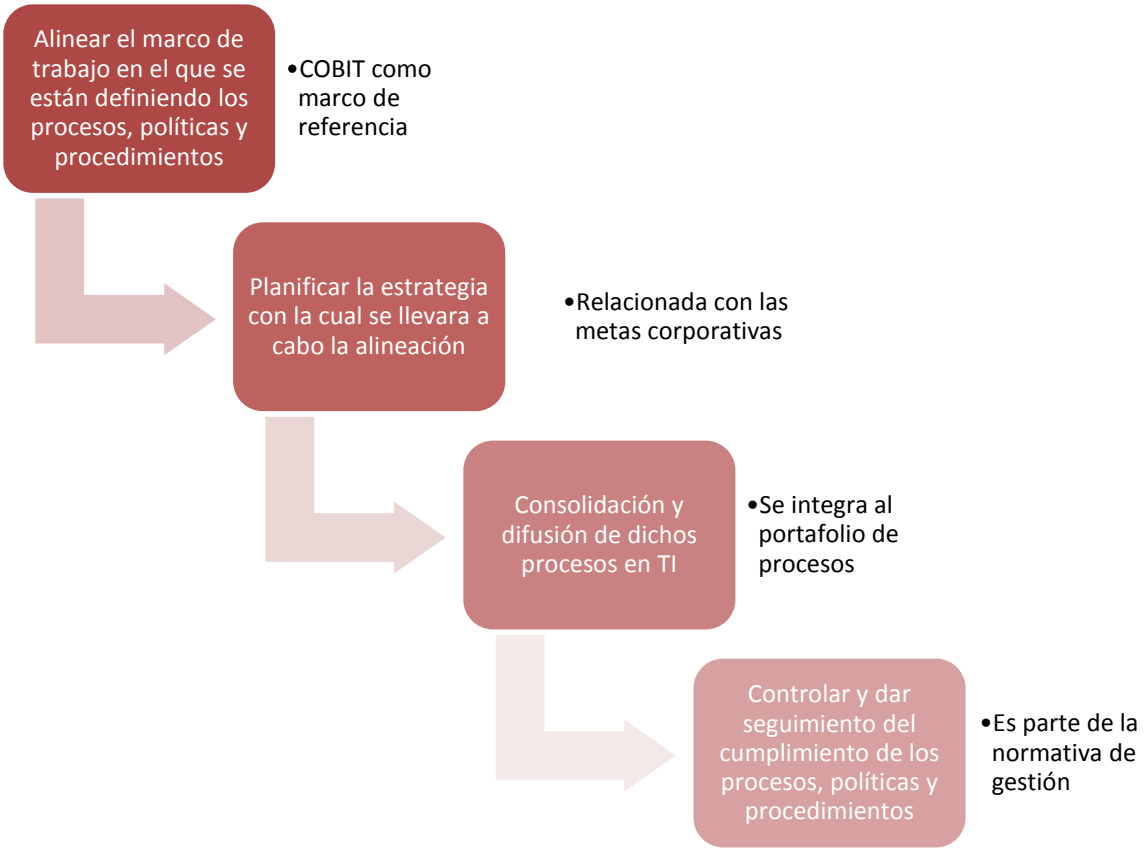

Figura 28 Plan para definir las políticas y procedimientos de S-I

3.3.2.2 Plan para implementar Áreas de Seguridad de la Información y PMO fuera de la estructura de TI

Los objetivos principales de esta iniciativa relacionados con el área de S-I son los siguientes:

- Definir los roles y funciones del personal del área de Seguridad de la información.
- Establecer su ubicación en la estructura organizacional fuera del área de TI

En la Figura 29 se define el plan de mejora para la creación del área de S-I de acuerdo a un esquema que resalta las principales fases de implementación; desde una definición en la cual participa el gobierno corporativo y la alta gerencia, hasta la definición de roles y actividades, de esta manera se pretende generar un área que responda a las necesidades empresariales de S-I y tenga el soporte y aceptación de todas las partes interesadas.

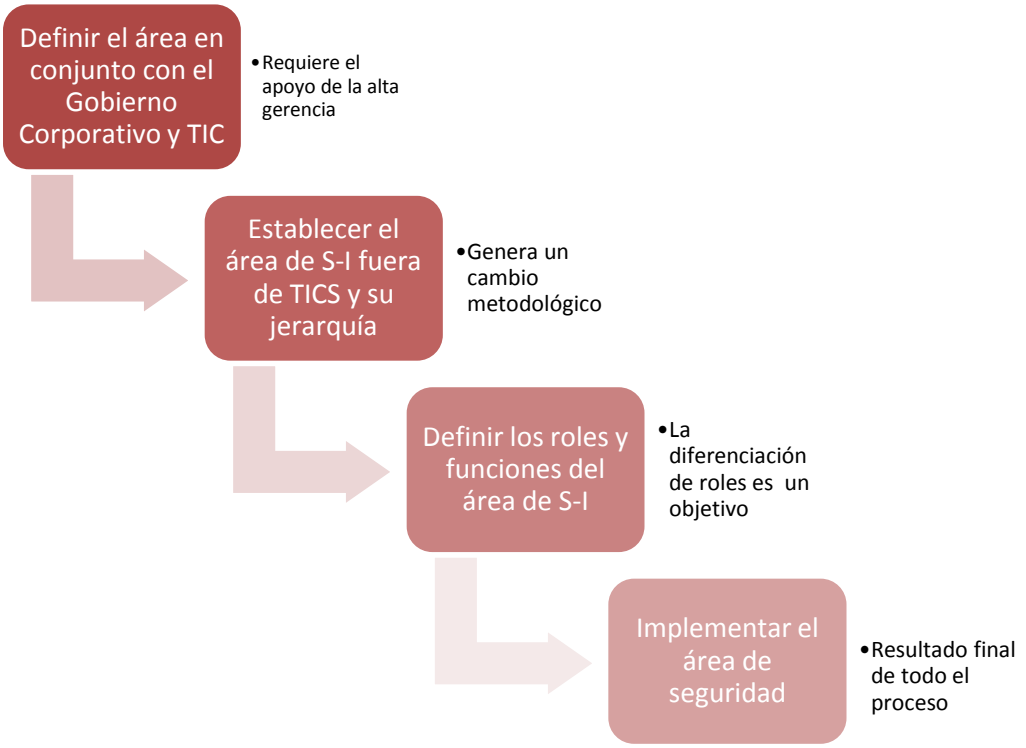

Figura 29 Plan para la creación del área de S-I

3.4 Análisis de riesgos del sistema ERP de EP PETROECUADOR

Para el análisis de riesgos del sistema ERP de EP PETROECUADOR, se utilizó la metodología MAGERIT, enfocada en un modelo cualitativo. Es claro que este tipo de modelo carece de la precisión intrínseca de un modelo cuantitativo; sin embargo, son herramientas de gran utilidad que permiten identificar la importancia relativa de los diferentes activos sometidos a varias amenazas, en sistemas cuya información no puede ser considerada definitiva o estable, como es el caso del sistema ERP de EP por encontrarse en una fase de transición hacia la puesta en producción.

Cabe aclarar que el alcance del análisis presentado en esta investigación, no comprende un modelo integral de gestión de riesgos, ya que solo representa la delimitación de un contexto de análisis y la valoración de los riesgos definida por su identificación y evaluación.

Los pasos metodológicos, que se llevaron a cabo para el análisis fueron los siguientes:

1. Identificación de los activos relevantes: información, servicios, equipos, personas, entre otros.
2. Identificación de las amenazas de los activos
3. Estimación del impacto potencial
4. Determinación de salvaguardas
5. Estimación del riesgo

De acuerdo a las técnicas aconsejadas en la metodología citada, la información básica para el análisis de riesgo fue recabada en reuniones de trabajo, en las cuales se identificó información crítica de cada módulo del sistema ERP y se definió las políticas de auditoría que serían configuradas en la herramienta Audit Vault[64] como complemento del ERP E-Business Suite.

El análisis realizado hace uso de escalas cualitativas que facilitan modelar los componentes del riesgo, de esta manera los resultados obtenidos pueden ser interpretados bajo un contexto común de niveles de valoración cualitativa.

Tabla 14 Escalas cualitativas

Valor	Impacto	Probabilidad	Riesgo
MA: muy alto	MA: muy alto	MA: prácticamente seguro	MA: crítico
A: alto	A: alto	A: probable	A: importante
M: medio	M: medio	M: posible	M: apreciable
B: bajo	B: bajo	B: poco probable	B: bajo
MB: muy bajo	MB: muy bajo	MB: muy raro	MB: despreciable

[64] Audit Vault: Software propietario de Oracle Corporation, que permite consolidar y gestionar, bajo un solo esquema integrado, pistas y políticas de auditoría de carácter corporativo para motores de bases de datos y sistemas operativos.

Para la determinación de las amenazas se consultó el catálogo proporcionado por MAGERIT en su segundo libro, y para estimar su impacto se utilizó una tabla de doble entrada que utiliza las escalas cualitativas, en donde el valor asignado a un activo es una representación relativa en comparación a los otros activos y su degradación se mide en las mismas unidades pero representada como un porcentaje de su propio valor. La Tabla 15 presenta el modelamiento del impacto con las consideraciones antes detalladas.

Tabla 15. Estimación del impacto

Impacto		Degradación		
		Mínima (1%)	Parcial (10%)	Total (100%)
Valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

De manera similar el modelamiento del impacto, probabilidad y riesgo se realizó utilizando una tabla de doble entrada para la probabilidad y el impacto, las cuales se detallan en la siguiente tabla.

Tabla 16 Estimación del riesgo

Riesgo		Probabilidad				
		MB	B	M	A	MA
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

3.4.1 *Identificación de Información crítica*

La información crítica identificada corresponde a los procesos de manufactura, abastecimientos y finanzas que se están implementando en el sistema ERP; el criterio

para definir esta información está relacionado a la experiencia del personal seleccionado para participar en el proyecto de implementación, complementada con las recomendaciones de procesos de auditoría que han sido llevados a cabo durante años anteriores en los sistemas de legado.

En la Tabla 17 se detalla los procesos y los módulos del ERP E-Business Suite, de acuerdo a su nombre comercial, utilizados para gestionar la información empresarial. Técnicamente las transacciones representan la creación, acceso, modificación o eliminación de cualquier tipo de información, realizada por los usuarios del sistema, utilizando la interfaz web o los formularios de los módulos del sistema ERP. Desde el punto de vista del usuario, estas transacciones pueden traducirse, en aprobaciones, negaciones, configuraciones, cálculos, parametrizaciones, cierres, promedios, entre otros; todo depende del contexto y el flujo de trabajo asociado.

Tabla 17 Información crítica del sistema ERP de EP PETROECUADOR

PROCESO/AMBITO	MODULO EBS	TRANSACCIÓN	INFORMACIÓN RELACIONADA
Compras	ICX-iProcurement	Solicitudes y aprobaciones de compra	Responsable, fecha, valor calculado, cantidad, precio unitario, dirección IP de la transacción, aprobador
Comercio Exterior	COMEX[65]	Liquidación de importaciones	Liquidador, fecha, campos personalizados.
Contratos	OKC-Contracts Core	Términos del contrato	Responsable del cambio, fechas, estado, artículos y clausulas.
Negociaciones	PON-Sourcing	Administración del plan de compras	Fecha de publicación, apertura y cierre, monto, cantidad, responsable
		Recepción de ofertas	Fecha de publicación y oferta, valor calculado
Inventarios	INV-Inventory	Cambio de fecha de emisión o vencimiento	Fecha, responsable, cantidad contada, cantidad ajustada, aprobador.
		Conversiones	Valor de la conversión, responsable, fecha

Continúa →

[65] COMEX: Es una personalización del E-Business Suite para EP PETROECUADOR, y no forma parte de los módulos estándar.

PROCESO/AMBITO	MODULO EBS	TRANSACCIÓN	INFORMACIÓN RELACIONADA
Compras	PO-Purchasing	Configuración del módulo	Fecha, responsable, jerarquía de puestos, aprobadores, opciones de compra, opciones de recepción, opciones financieras
Planeación	OPM-Oracle Process Manufacturing	Configuración del módulo	Calendarios, fecha, responsable, eventos de creación, modificación, eliminación
		Modificación de formulas	Artículo, cantidad, unidad de medida, tipo de escala, participación, costo
		Asignación de recursos de en operación	Tipo de plan, unidad de medida, código de análisis, costo, uso.
		Modificación de costos	Tipo de ajuste, cantidad, unidad de medida, costo
Cuentas por cobrar	AR-Receivables	Emisión de documentos (facturas, notas de crédito, reversiones)	Fechas de emisión y vencimiento, divisa, estado, descripciones de artículos, cantidad, precio.
Activos fijos	FA-Fixed assets	Actualización de información del activo	Fecha, responsable, categoría del activo, clave del activo, ubicación del activo.
		Actualización de fechas de cierre	Fecha, responsable
		Actualización de póliza de seguro	Tipo de póliza, tasa, vigencia, responsable

Continúa →

PROCESO/AMBITO	MODULO EBS	TRANSACCIÓN	INFORMACIÓN RELACIONADA
Contabilidad	GL-General Ledger	Configuraciones del módulo	Fecha, responsable, tipo de regla de seguridad, reglas de validación cruzada
		Asientos contables	Fecha, responsable, periodo, combinación contable, débito entrado, crédito entrado, valor débito, crédito contabilizado, débito contabilizado.
		Inactivación de cuentas	Fecha, responsable
		Inactivación de combinaciones contables	Fecha, responsable
Presupuesto	GL-General Ledger	Configuración de módulo	Fecha, responsable
		Adición de valores en los rangos de presupuesto	Parámetros, fecha, responsable, combinación contable
Cuentas por pagar	AP-Payables	Configuraciones del módulo	Fecha, responsable, opciones, parámetros financieros
		Modificación de lotes de pago	Fecha, responsable, valor a pagar, valor pagado, número de la factura
Administración de efectivo	CE-Cash Management	Configuración de cuentas bancarias	Fecha, responsable, cuenta bancaria, cuenta contable
Administración de proyectos	PA-Project	Creación de activos capitalizables	Fecha, responsable

3.4.2 *Identificación de Activos*

Para la identificación de activos se dividió o categorizó cada uno de ellos en capas interrelacionadas, las cuales facilitan reconocer la importancia de cada uno de ellos dentro de la organización, considerando que en las capas superiores se encuentran los activos que representan la razón del negocio, y a medida que se desciende en las mismas se pueden hallar los activos habilitantes o de soporte. Una ventaja adicional que se obtiene al categorizar los activos de manera jerárquica, es la identificación de dependencia entre estos; lo cual, bajo el análisis realizado, permite identificar el riesgo acumulado que afecta a un activo de capa superior en función de los riesgos de los activos de las capas inferiores. Este enfoque se representa gráficamente en la Figura 30, de acuerdo a la información de dependencia de activos de la Tabla 18, en donde las flechas representan las dependencias directas desde las capas superiores a las inferiores.

Tabla 18 Identificación de activos

Activos				Dimensiones de análisis				
Categoría	**Subcategoría**	**Nombre**	**Dependencia**	**Disponibilidad**	**Integridad**	**Confidencialidad**	**Autenticidad**	**Trazabilidad**
Capa de negocio [N]	Información	1. Finanzas	4, 12	X	X	X	X	X
		2. Abastecimientos	4, 12	X	X	X	X	X
		3. Manufactura	4, 12	X	X	X	X	X
	Servicio	4. Instancias EBS	5,6	X	X	X		X
Equipamiento [E]	Software	5. E-Business Suite	7,8	X	X	X		
		6. Oracle 11g	7,8	X	X	X		
	Hardware	7. Host Server AP	9,11,13,14	X	X	X		
		8. Host Server BD	9,11, 13, 14	X	X	X		
	Comunicaciones	9. Red LAN Quito	10, 15	X	X	X		
Servicios Subcontratados [S]	Comunicaciones	10. Enlaces de datos CNT		X	X	X		
Instalaciones [I]	Recinto	11. Centro de Datos		x				
Personal [P]	Usuarios	12. Usuarios módulos		x		x		
	Base de Datos	13. DBA		x		x		
	Aplicación	14. SYSADMIN		x		x		
	Redes y telecomunicaciones	15.Administrador de redes y comunicaciones		x		x		

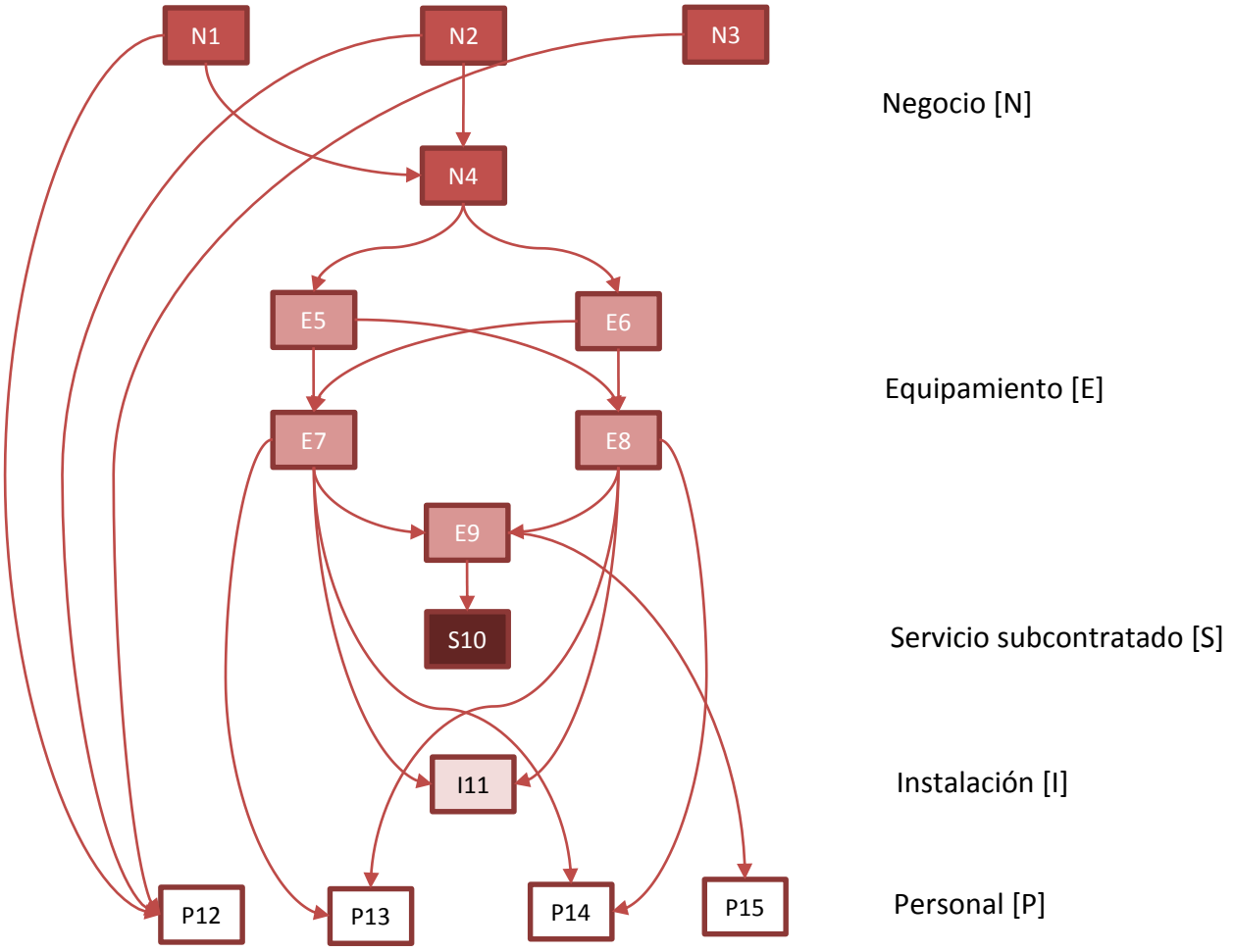

Figura 30 Dependencia de activos

3.4.3 *Identificación de Amenazas*

Para la elaboración de la Tabla 19, se utilizó el catálogo de MAGERIT, el cual brinda una definición de las amenazas más comunes de acuerdo a cada subcategoría de activos y de la misma manera proporciona información que permite definir la dimensión o dimensiones más apropiadas a ser consideradas en la valoración. Las dimensiones básicas definidas para el análisis son: disponibilidad, integridad, y confidencialidad; añadiéndose las dimensiones de autenticidad y trazabilidad, derivadas de las dimensiones básicas, utilizadas para un acercamiento a la percepción de los usuarios sobre un SI. Por ejemplo, la amenaza "Denegación de Servicio" se analiza únicamente en la dimensión de Disponibilidad debido a que guarda completa relación; mientras que las dimensiones de confidencialidad y autenticidad no se ven afectadas por una falta o no disponibilidad de la información.

Para la definición del impacto acumulado se utiliza el mayor valor de las dimensiones analizadas, y en caso de contar con dos o más dimensiones en un nivel medio se acumulan para asumir un impacto acumulado alto. Al tratarse de un análisis cualitativo se puede asumir las siguientes condiciones de contorno para la función de cálculo de impacto:

Siendo V el valor del activo y D degradación porcentual sufrida

Impacto(0,0%) = 0

Impacto(V,0%) = 0

Impacto(V,100%) = V

Tabla 19 Identificación y valoración de amenazas

Activos			Amenazas	Dimensiones de valoración										Impacto acumulado
				Disponibilidad		Integridad		Confidencialidad		Autenticidad		Trazabilidad		
Categoría	Subcategoría	Nombre		V	D	V	D	V	D	V	D	V	D	
Negocio	Información	1. Finanzas	1. Modificación deliberada de información			MA	TOT.							MA
			2. Errores de los usuarios	A	PAR.	MA	PAR.	M	PAR.					A
			3. Suplantación de la identidad	A	PAR.	MA	MIN.	M	TOT.					A
		2. Abastecimientos	4. Modificación deliberada de información			MA	TOT.							MA
			5. Errores de los usuarios	A	PAR.	MA	PAR.	M	PAR.	A	PAR.			A
			6. Suplantación de la identidad	A	PAR.	MA	MIN.	M	TOT.					A

Continúa →

Activos			Amenazas	Dimensiones de valoración										Impacto acumulado
				Disponibilidad		Integridad		Confidencialidad		Autenticidad		Trazabilidad		
Categoría	Subcategoría	Nombre		V	D	V	D	V	D	V	D	V	D	
		3. Manufactura	7. Modificación deliberada de información			MA	TOT.							MA
			8. Errores de los usuarios	A	PAR.	MA	PAR.	M	PAR.					A
			9. Suplantación de la identidad	A	PAR.	MA	MIN.	M	TOT.					A
	Servicio	4. Instancias EBS	10. Repudio			A	PAR.					A	PAR.	A
			11. Denegación de servicio	MA	PAR.									A
			12. Errores del administrador	MA	PAR.	A	PAR.	M	PAR.					A
Equipamiento	Software	5. E-Bussines Suite	13. Abuso de privilegios de acceso	A	PAR.	M	PAR.	A	MIN.					M

Continúa →

Activos			Amenazas	Dimensiones de valoración										Impacto acumulado
				Disponibilidad		Integridad		Confidencialidad		Autenticidad		Trazabilidad		
Categoría	Subcategoría	Nombre		V	D	V	D	V	D	V	D	V	D	
			14. Errores de mantenimiento / actualización	A	PAR.	M	PAR.							M
			15. Vulnerabilidades de los programas	A	PAR.	M	PAR.	A	PAR.					A
		6. Oracle 11g	16. Abuso de privilegios de acceso	A	PAR.	M	PAR.	A	MIN.					M
			17. Errores de mantenimiento / actualización	A	PAR.	M	PAR.							M
			18. Vulnerabilidades de los programas	A	PAR.	M	PAR.	A	PAR.					A
	Hardware	7. Host Server AP	19. Avería de origen físico o lógico	A	TOT.									A
			20. Condiciones inadecuadas de temperatura o humedad	A	PAR.									M

Continúa →

Activos			Amenazas	Dimensiones de valoración										Impacto acumulado
				Disponibilidad		Integridad		Confidencialidad		Autenticidad		Trazabilidad		
Categoría	Subcategoría	Nombre		V	D	V	D	V	D	V	D	V	D	
			21. Errores del administrador	A	PAR.	A	PAR.	A	PAR.					A
			22. Corte de suministro eléctrico	A	MIN.									B
		8. Host Server BD	23. Avería de origen físico o lógico	A	TOT.									A
			24. Condiciones inadecuadas de temperatura o humedad	A	PAR.									A
			25 Errores del administrador	A	PAR.	M	TOT.	A	PAR.					A
			26. Corte de suministro eléctrico	A	MIN.									B
	Comunicaciones	9. Red LAN Quito	27. Errores de encaminamiento					M	PAR.					B
			Continúa →											

Activos			Amenazas	Dimensiones de valoración										Impacto acumulado
				Disponibilidad		Integridad		Confidencialidad		Autenticidad		Trazabilidad		
Categoría	Subcategoría	Nombre		V	D	V	D	V	D	V	D	V	D	
			28. Errores del administrador	A	PAR.	A	MIN.	A	PAR.					A
			29. Acceso no autorizado			M	PAR.	A	PAR.					M
			30. Denegación de servicio	A	PAR.									M
Servicios contratados	Servicio subcontratado	10. Enlaces de datos CNT	31. Caída del servicio	A	TOT.									A
			32. Fuga de información					A	PAR.					M
Instalaciones	Recinto	11. Centro de Datos	33. Desastres naturales: inundaciones, sismos, contaminación	MA	TOT.									MA
			34. Acceso no autorizado			MA	MIN.	MA	PAR.					A

Continúa →

Activos			Amenazas	Dimensiones de valoración										Impacto acumulado
				Disponibilidad		Integridad		Confidencialidad		Autenticidad		Trazabilidad		
Categoría	Subcategoría	Nombre		V	D	V	D	V	D	V	D	V	D	
Personal	Usuarios	12. Usuarios de los módulos ERP	35. Indisponibilidad	M	PAR.									B
			36. Ingeniería social	M	PAR.	M	PAR.	M	TOT.					M
			37. Extorsión	M	PAR.	M	PAR.	M	PAR.					M
	Base de Datos	13. DBA	38. Indisponibilidad	M	PAR.									B
			39. Ingeniería social	M	PAR.	M	PAR.	M	TOT.					M
	Aplicación	14. SYSADMIN	40. Indisponibilidad	M	PAR.									B
			41. Ingeniería social	M	PAR.	M	PAR.	M	TOT.					M
	Redes y telecomunicaciones	15. Técnico líder	42. Indisponibilidad	M	PAR.									B
			43. Ingeniería social	M	PAR.	M	PAR.	M	TOT.					M

3.4.4 *Estimación del Riesgo*

La estimación del riesgo utiliza como entrada el impacto acumulado de la Tabla 19, y estima una probabilidad de ocurrencia de acuerdo a varias fuentes de información, como la caracterización de las CVE por parte de OWASP, los estudios realizados por el MITRE[66], la base de datos nacional de vulnerabilidades mantenida por el NIST[67]; pero sobre todo la base de conocimientos propia de cada empresa correspondiente a los registros de incidentes ocurridos.

Tabla 20 Riesgo según impacto y probabilidad

No.	**Activo**	**Amenazas**	**Impacto acumulado**	**Probabilidad**	**Riesgo**
1	1. Finanzas	Modificación deliberada de información	MA	MB	A
2		Errores de los usuarios	A	B	A
3		Suplantación de la identidad	A	MB	M
4	2. Abastecimientos	Modificación deliberada de información	MA	MB	A
5		Errores de los usuarios	A	B	A
6		Suplantación de la identidad	A	MB	M
7	3. Manufactura	Modificación deliberada de información	MA	MB	A
8		Errores de los usuarios	A	B	A

Continúa →

[66] MITRE: Organización sin fines de lucro que opera centros de desarrollo e investigación auspiciadas por el Gobierno Federal de EEUU.

[67] NIST: National Institute of Standards and Technologies

No.	**Activo**	**Amenazas**	**Impacto acumulado**	**Probabilidad**	**Riesgo**
9		Suplantación de la identidad	A	MB	M
10	4. Instancias EBS	Repudio	A	MB	M
11		Denegación de servicio	A	MB	M
12		Errores del administrador	A	MB	M
13	5. E-Bussines Suite	Abuso de privilegios de acceso	M	B	M
14		Errores de mantenimiento / actualización	M	MB	B
15		Vulnerabilidades de los programas	A	MB	M
16	6. Oracle 11g	Abuso de privilegios de acceso	M	M	M
17		Errores de mantenimiento / actualización	M	MB	B
18		Vulnerabilidades de los programas	A	MB	M
19	7. Host Server AP	Avería de origen físico o lógico	A	MB	M
20		Condiciones inadecuadas de temperatura o humedad	M	MB	B
21		Errores del administrador	A	MB	M
22		Corte de suministro eléctrico	B	B	M
23	8. Host Server BD	Avería de origen físico o lógico	A	MB	M

Continúa →

No.	**Activo**	**Amenazas**	**Impacto acumulado**	**Probabilidad**	**Riesgo**
24		Condiciones inadecuadas de temperatura o humedad	A	MB	M
25		Errores del administrador	A	MB	M
26		Corte de suministro eléctrico	B	B	B
27	9. Red LAN Quito	Errores de encaminamiento	B	M	B
28		Errores del administrador	A	MB	M
29		Acceso no autorizado	M	MB	B
30		Denegación de servicio	M	MB	B
31	10. Enlaces de datos CNT	Caída del servicio	A	B	A
32		Fuga de información	M	MB	B
33	11. Centro de Datos	Desastres naturales: inundaciones, sismos, contaminación	MA	B	MA
34		Acceso no autorizado	A	MB	M
35	12. Usuarios de los módulos ERP	Indisponibilidad	B	M	B
36		Ingeniería social	M	M	M
37		Extorsión	M	MB	B
38	13. DBA	Indisponibilidad	B	M	B
39		Ingeniería social	M	M	M
40	14. SYSADMIN	Indisponibilidad	B	M	B
41		Ingeniería social	M	M	M
42	15. Técnico líder	Indisponibilidad	B	M	B
43		Ingeniería social	M	M	M

3.4.4.1 Tendencia del riesgo

La Figura 31 utiliza los resultados cualitativos de la Tabla 20 para representar gráficamente cada uno de los riesgos identificados en función de probabilidad e impacto. Para la elaboración de este gráfico se asignó valores numéricos a cada nivel cualitativo, siendo muy bajo equivalente a 1 y muy alto a 5. Esta equivalencia no representa valoraciones cuantitativas de riesgo y no debe considerarse como tal, su única utilidad es la asignación de una escala numérica discreta, útil para trasladar cualquier conjunto de niveles cualitativos en un plano cartesiano bidimensional con entradas numéricas como se muestra en la Tabla 21.

Tabla 21 Tabla de equivalencias para niveles cualitativos

Riesgo		Probabilidad				
		MB 1	B 2	M 3	A 4	MA 5
Impacto	MA 5	A (1,5)	MA (2,5)	MA (3,5)	MA (4,5)	MA (5,5)
	A 4	M (1,4)	A (2,4)	A (3,4)	MA (4,4)	MA (5,4)
	M 3	B (1,3)	M (2,3)	M (3,3)	A (4,3)	A (5,3)
	B 2	MB (1,2)	B (2,2)	B (3,2)	M (4,2)	M (5,2)
	MB 1	MB (1,1)	MB (2,1)	MB (3,1)	B (4,1)	B (5,1)

Este gráfico también puede ser de utilidad para encontrar una tendencia característica de los riesgos, es decir que podríamos determinar de manera general que tan probable es un riesgo en función de su impacto; o viceversa, podríamos determinar el impacto de un riesgo en un función de su probabilidad.

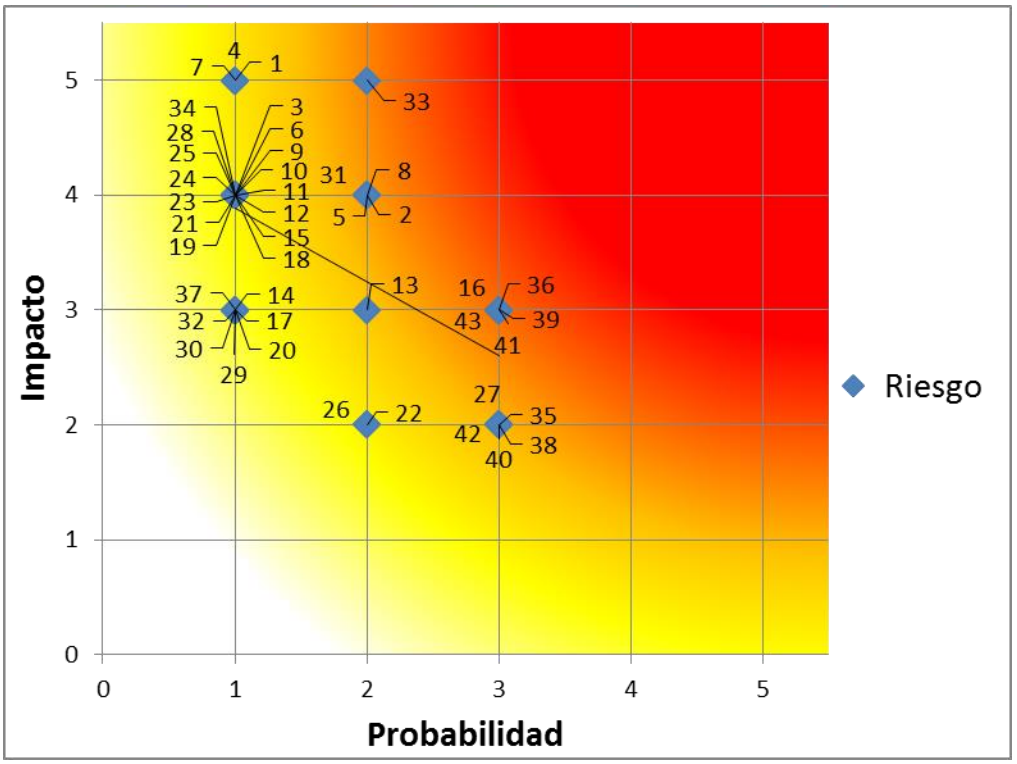

Figura 31 Tendencia del riesgo según impacto y probabilidad

3.4.5 *Identificación de salvaguardas*

Para la identificación de las salvaguardas se recurrió nuevamente a los catálogos de MAGERIT, adaptándolos de acuerdo a los activos a proteger y a las características de las amenazas identificadas para el sistema ERP de EP PETROECUADOR. Los objetivos de las salvaguardas son: reducir la probabilidad de una amenaza y limitar la posible degradación que un activo puede sufrir. Para conseguir estos objetivos las salvaguardas pueden afectar aspectos administrativos, operacionales y organizacionales, por tanto la información de la Tabla 22 solamente considera aquellas salvaguardas que técnicamente son aplicables y justificables de acuerdo a las características de los activos a proteger.

Tabla 22 Salvaguardas para el sistema ERP de EP PETROECUADOR

Activo	Amenazas	Salvaguardas
1. Finanzas	Modificación deliberada de información	Copias de seguridad, cifrado de la información, uso de firmas electrónicas, aseguramiento de la integridad, gestión de incidencias.
	Errores de los usuarios	
	Suplantación de la identidad	
2. Abastecimientos	Modificación deliberada de información	
	Errores de los usuarios	
	Suplantación de la identidad	
3. Manufactura	Modificación deliberada de información	
	Errores de los usuarios	
	Suplantación de la identidad	
4. Instancias EBS	Repudio	Aseguramiento de la disponibilidad, gestión de cambios, aplicación de perfiles de seguridad
	Denegación de servicio	
	Errores del administrador	
5. E-Bussines Suite	Abuso de privilegios de acceso	Segregación de tareas, análisis de vulnerabilidades, sistemas de prevención de intrusos
	Errores de mantenimiento / actualización	
	Vulnerabilidades de los programas	
6. Oracle 11g	Abuso de privilegios de acceso	
	Errores de mantenimiento / actualización	
	Vulnerabilidades de los programas	
7. Host Server AP	Avería de origen físico o lógico	Perfiles de seguridad, aseguramiento de la disponibilidad, operación, protección de equipos.
	Condiciones inadecuadas de temperatura o humedad	
	Errores del administrador	
	Corte de suministro eléctrico	
8. Host Server BD	Avería de origen físico o lógico	
	Condiciones inadecuadas de temperatura o humedad	
	Errores del administrador	
	Corte de suministro eléctrico	

Continúa →

Activo	Amenazas	Salvaguardas
9. Red LAN Quito	Errores de encaminamiento	Perfiles de seguridad, autenticación y cifrado de canal, , aseguramiento de redes inalámbricas, segregación de redes y dominios
	Errores del administrador	
	Acceso no autorizado	
	Denegación de servicio	
10. Enlaces de datos CNT	Caída del servicio	Establecer y hacer cumplir los SLA
	Fuga de información	
11. Centro de Datos	Desastres naturales: inundaciones, sismos, contaminación	Control de accesos físicos, aseguramiento de la disponibilidad, plan integral de desastres
	Acceso no autorizado	
12. Usuarios de los módulos ERP	Indisponibilidad	Formación, capacitación, gestión del personal, concientización.
	Ingeniería social	
	Extorsión	
13. DBA	Indisponibilidad	Formación, capacitación, gestión del personal, aseguramiento de la disponibilidad
	Ingeniería social	
14. SYSADMIN	Indisponibilidad	
	Ingeniería social	
15. Técnico líder	Indisponibilidad	
	Ingeniería social	

4 Capítulo IV Propuesta del Modelo de Gestión de Seguridad de la información del sistema ERP de EP PETROECUADOR

4.1 Introducción

La presente propuesta se basa en los conceptos de la guía profesional "COBIT 5 para la seguridad de la información", la misma que proporciona un conjunto de información filtrada y actualizada que refuerza los conceptos de S-I del marco principal, haciendo uso de otros estándares como la norma ISO/IEC 27002.

Los conceptos presentados en COBIT 5 para la seguridad de la información, al igual que otros marcos de referencia o estándares, no pretenden ser una guía prescriptiva para las necesidades de todas las empresas (ISACA, 2012); por lo tanto, el modelo que se presenta a continuación corresponde a una adaptación resultado del análisis de las necesidades y priorización de las partes interesadas en la S-I del sistema ERP de EP PETROECUADOR, considerando los 5 principios y las 7 categorías de catalizadores de COBIT 5 detalladas en el capítulo 2.

Es importante resaltar que las 7 categorías de catalizadores fueron alineadas bajo los conceptos de la cascada de metas, para dar soporte al Modelo de Gestión de Seguridad de la Información del Sistema ERP de EP PETROECUADOR, sintetizándolas bajo 4 dimensiones comunes: las partes interesadas, metas, ciclo de vida y las buenas prácticas; complementándose con la gestión del rendimiento para la definición de métricas de control y supervisión como se detalla en la Figura 32.

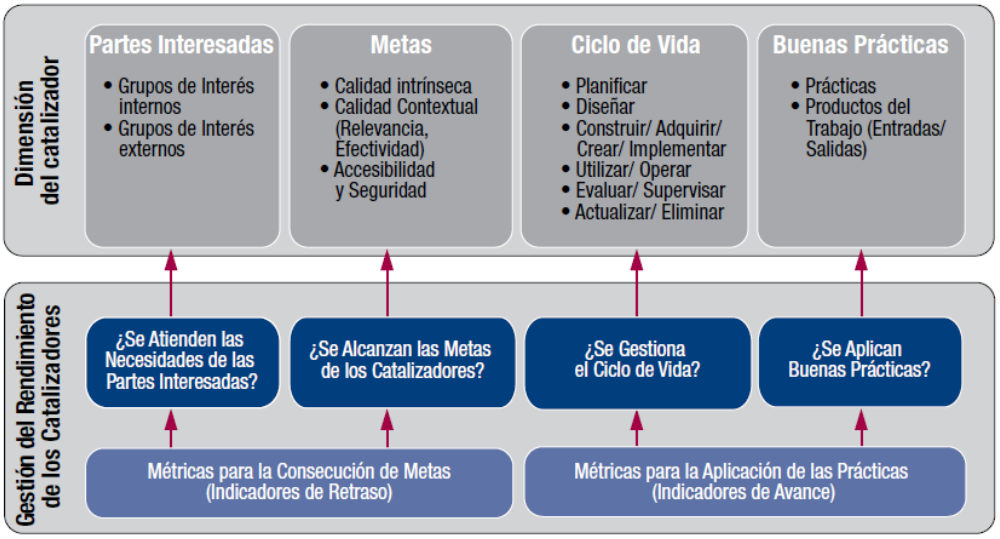

Figura 32 Dimensiones Genéricas de los catalizadores COBIT 5 (ISACA, 2012)

4.1.1 ***Cascada de Metas***

La cascada propuesta pretende aclarar el origen de las metas de las 7 categorías de catalizadores, que serán desarrolladas en las siguientes secciones del documento según corresponda.

4.1.1.1 Metas corporativas a Metas de TI

Las metas corporativas que EP PETROECUADOR se ha planteado con la implementación del sistema ERP son las siguientes:

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

Estas metas definidas, para EP PETROECUADOR, equivalen a priorizar 3 metas corporativas genéricas que según COBIT 5 y su numeración estándar son:

9. Toma estratégica de Decisiones basada en Información

11. Optimización de la funcionalidad de los procesos de negocio

15. Cumplimiento con las políticas internas

Para establecer las relaciones entre las metas corporativas y las metas de TI se utilizó el apéndice B del marco COBIT 5 denominado “Mapeo detallado de metas de Empresa y las metas relacionadas con las TI”. Estas relaciones entre metas, reducidas para el caso del sistema ERP de EP PETROECUADOR, se detallan en Tabla 23, utilizando 2 escalas:

- La escala ‘P’ para principal, cuando exista una importante relación, es decir, las metas relacionadas con TI son el pilar imprescindible para conseguir los objetivos de la empresa.
- La escala ‘S’ para secundario, cuando todavía existe un vínculo fuerte, pero menos importante, es decir, las metas relacionadas con TI son un soporte secundario para los objetivos de la empresa.

Para el presente modelo solo se utiliza las relaciones principales definidas en COBIT 5 y serán usadas como insumos o entradas para los siguientes niveles de la cascada de metas; las relaciones secundarias pueden ser parte de un proceso de revisión del modelo planteado y su inclusión a futuro depende de la priorización que EP PETROECUADOR asigne a sus metas de acuerdo a las necesidades de las partes interesadas.

Tabla 23 Relación entre metas Corporativas y metas de TI

			Metas corporativa de COBIT 5														
			Valor para las partes interesadas de las Inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activos)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basada en Información	Optimización de costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Metas relacionadas con las TI			Financiera					Cliente					Interna				
Financiera	1	Alineamiento de TI y estrategia de negocio									P		P				
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas															P
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI															
	4	Riesgos de negocio relacionados con las TI gestionados															
	5	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI															
	6	Transparencia de los costes, beneficios y riesgos de las TI															
Cliente	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio											P				
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas											P				
Interna	9	Agilidad de las TI											P				
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones															P
	11	Optimización de activos, recursos y capacidades de las TI															
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio											P				
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad															
	14	Disponibilidad de información útil y fiable para la toma de decisiones									P						
	15	Cumplimiento de las políticas internas por parte de las TI Aprendizaje y Crecimiento															P
Aprendizaje y Crecimiento	16	Personal del negocio y de las TI competente y motivado															
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio															

4.2 Política de Seguridad de la información del Sistema ERP de EP PETROECUADOR.

4.2.1 *Términos y definiciones*

Para la presente política se consideran las siguientes definiciones:

4.2.1.1 La seguridad de la Información

Se define, en un ambiente empresarial, como la protección de la información contra la divulgación a personal no autorizado, modificación inadecuada y el no acceso cuando es requerida; de acuerdo al principio CIA[68] ampliamente aceptado.

La S-I es un catalizador para la continuidad del negocio, minimización del riesgo comercial, la maximización el retorno de las inversiones y la ampliación de las oportunidades comerciales.

4.2.1.2 Riesgo

Se define como una desviación positiva o negativa de un resultado esperado, debido a la falta total o parcial de información relacionada con la comprensión o conocimiento de un evento, su probabilidad de ocurrencia y consecuencias.

4.2.1.3 Gestión de Riesgos

Es un proceso sistemático que comprende la identificación, análisis y evaluación de riesgos; para determinar si estos deben ser modificados satisfaciendo los criterios de cada organización.

4.2.2 ***Alcance***

La presente política constituye el conjunto de reglas establecidas para brindar soporte a los objetivos de gobierno y los valores empresariales, mediante el aseguramiento de la información del sistema ERP de EP PETROECUADOR, sin

[68] CIA: Confidencialidad, Integridad y disponibilidad, o CIA por sus siglas en inglés

importar la forma que esta tome incluyéndose los medios escritos, gráficos, electrónicos o multimedia.

4.2.3 *Objetivos*

Los objetivos de la presente política son:

- Brindar soporte a las actividades empresariales
- Defender el giro de negocio
- Promover comportamientos responsables con la S-I

4.2.4 *Principios*

EP PETROECUADOR gestiona el sector hidrocarburífero mediante la refinación, transporte, almacenamiento y comercialización de hidrocarburos de forma rentable y eficiente, aprovechando TI de punta, para automatizar sus procesos. Es por esto que EP PETROECUADOR considera a la S-I como un elemento clave en el logro de sus objetivos, permitiéndole obtener el máximo beneficio de su plataforma tecnológica mientras mantiene controlados los riesgos asociados. Consecuente con la importancia reconocida, EP PETROECUADOR define los principios que regirán esta política a continuación:

- Incluir, como un elemento clave, los principios y criterios técnicos de la S-I en las actividades empresariales.
- Disponer de los recursos económicos y personal técnico especializado, que garanticen la implementación de programas de aseguramiento.
- Controlar que las TI garanticen la S-I, y el cumplimiento del marco regulatorio de las empresas públicas, normativa interna y procedimientos establecidos.
- Promover la cultura de S-I en todos los niveles de la empresa.

- Difundir y comunicar la política, a todo el personal, contratista y clientes de EP PETROECUADOR.
- La estrategia y plan de aseguramiento de la información de EP PETROECUADOR deberán orientarse mediante la gestión de los riesgos asociados a la S-I.

4.2.5 *Sobre el marco de referencia*

- Se utilizará COBIT 5 como marco de referencia principal para el gobierno y gestión de la S-I del sistema ERP, ajustándose a toda la normativa vigente de EP PETROECUADOR, aplicándola según su orden jerárquico y especialidad. En caso de duda se observará la norma de rango superior.
- Los reglamentos, procesos, procedimientos, manuales, guías y documentación que se desarrolle como complemento a COBIT 5, se ajustará a las buenas prácticas definidas en la norma ISO/IEC 27002. El uso de otros estándares o marcos de referencia no está permitido, a excepción de que exista la justificación necesaria para incluirlos y que su contenido no se contraponga con el marco principal de referencia o las buenas prácticas normalmente aceptadas.

4.2.6 *Responsabilidades y obligaciones*

- Las autoridades de cualquier nivel jerárquico de EP PETROECUADOR son responsables de la implementación de la presente política de acuerdo a su ámbito de acción y a las actividades asignadas en el plan de aseguramiento de la empresa.

- Es obligación de todo el personal, contratistas y clientes de EP PETROECUADOR cumplir y hacer cumplir los lineamientos de la presente política.
- El área de Talento Humano, será la responsable de comunicar al personal que ingresa a laborar a EP PETROECUADOR, bajo cualquier modalidad contractual, sobre su obligación de cumplimiento con la Política de S-I y los reglamentos o procedimientos adicionales derivados de esta.
- Los propietarios de la información, entendiéndose como los responsables de su creación y explotación, tienen la obligación de clasificar, definir y documentar los niveles de protección y acceso a la misma.

  Es responsabilidad del área de S-I de EP PETROECUADOR, proponer y comunicar la Estrategia de S-I y el plan de aseguramiento.
- El área de S-I de EP PETROECUADOR será la responsable de revisar y proponer cambios al contenido de esta política, de forma periódica, considerando principalmente los ajustes que faciliten conseguir las metas empresariales, los requerimientos de las entidades de control y la regulación vigente.
- La aprobación, de la presente política y sus modificaciones, será responsabilidad de las autoridades definidas en la normativa interna de EP PETROECUADOR.

4.2.7 *Sanciones por incumplimiento*

El incumplimiento de la política de S-I tendrá como resultado la aplicación de diversas sanciones de acuerdo a las prescripciones de orden, obligaciones,

prohibiciones y faltas disciplinarias establecidas en la normativa interna de EP PETROECUADOR.

4.3 Políticas específicas de S-I de EP PETROECUADOR

Estas políticas, cubren ámbitos específicos de la función de seguridad, y brindan guías más detalladas con respecto a las actividades empresariales. Se establece métricas que faciliten verificar la efectividad de las políticas directamente relacionadas con S-I.

4.3.1 *Política de control de acceso al sistema ERP*

4.3.1.1 Objetivo

Establecer los lineamientos para controlar el acceso a la información, garantizando que sea accedida en cumplimiento de las necesidades del negocio y los niveles de seguridad requeridos por el sistema ERP.

4.3.1.2 Generalidades

- El acceso a la información del sistema ERP, será asignado de acuerdo a los roles y responsabilidades identificados en los procesos de manufactura, abastecimientos y finanzas.
- La asignación de roles a los funcionarios será determinada por los líderes de cada frente funcional, o en su defecto por parte de los coordinadores de cada área involucrada.
- Se utilizará la segregación de funciones, para diferenciar las responsabilidades de cada usuario, de acuerdo a la identificación de los roles de cada proceso.
- Se evitará, bajo todo concepto, que la definición de roles genere conflictos de intereses en el acceso, control y protección de la seguridad de la información.

- Se prohíbe la creación y uso de usuarios genéricos, usuarios con privilegios de administrador o súper usuarios, para las tareas que involucren gestión de la información del sistema ERP.
- Se establecerá el principio de menor privilegio para la asignación de permisos, es decir que cada funcionario contará con los mínimos privilegios que le permitan cumplir con sus funciones.
- En el caso de que un funcionario requiera los permisos de acceso de un rol que no le corresponde, se deberá justificar la necesidad de acceso y en caso de asignar los permisos solicitados, estos deberán ser de carácter temporal.
- La asignación de los roles a los funcionarios es intransferible, y deberá ser actualizada de acuerdo a las necesidades del negocio.
- La definición de roles y responsabilidades con sus respectivos accesos a la información del sistema ERP, deberán ser verificados y actualizados continuamente por parte de los propietarios de la información, las áreas de procesos y S-I de EP PETROECUADOR.

4.3.1.3 Sobre los dispositivos móviles

- El uso de dispositivos móviles[69] para el sistema ERP, deberá ser analizado de forma específica, considerando los riesgos y ventajas relacionadas con este tipo de dispositivos.
- La asignación de privilegios de acceso en dispositivos móviles cumplirá con los mismos principios generales establecidos en la presente política.

[69] Dispositivo móvil: se incluye en esta categoría tabletas, teléfonos inteligentes, agendas electrónicas, laptops, notebooks y estaciones de trabajo portátiles.

- Las medidas de seguridad específicas que se deberán incluir para el uso de dispositivos móviles son:
    - Encriptación de contenido
    - Borrado remoto
    - Respaldos periódicos
    - Restricción de instalación de aplicaciones de terceros
    - Contratación de seguros especializados
    - Capacitación a los usuarios de estas tecnologías
- Las políticas referentes a dispositivos móviles, específicamente tabletas y teléfonos inteligentes, deberán ser revisadas continuamente y validadas a medida que se implementen nuevas funcionalidades en el sistema ERP.
- Se prohíbe el acceso a los módulos del sistema ERP que no hayan sido certificados para plataformas móviles.

4.3.1.4 Métricas

Las métricas con las cuales se puede medir el éxito de la implementación de esta política son:

- Número de violaciones de acceso por privilegios excesivos de los roles definidos.
- interrupción de las actividades debido a privilegios insuficientes.
- Número de observaciones encontradas en auditorias por conflicto de intereses en los privilegios de acceso a la información empresarial.

4.3.2 ***Política de S-I del personal***

4.3.2.1 Objetivos

- Definir planes de relevo y capacitación de acuerdo a información sobre el personal en puestos claves de la empresa, incluyendo el área de S-I.
- Actualización de antecedentes del personal de la empresa.

4.3.2.2 Generalidades sobre el empleo y contratación

- Todo el personal propio o contratado, que tenga acceso a la información del sistema ERP de EP PETROECUADOR, deberá cumplir con las políticas y lineamientos de S-I establecidos.
- Las áreas de Talento Humano serán las encargadas de recolectar y verificar información relevante sobre los antecedentes del personal que ingresa a la empresa, siempre que estas actividades no atenten contra el derecho a la intimidad y otras leyes relacionadas. La información básica a recolectar y verificar debe incluir:
    - Referencias laborales y personales
    - Calificaciones académicas
    - Record policial
- En caso de que el personal que tenga acceso a información confidencial sea proporcionado por una contratista o similar, se debe exigir que los términos del contrato incluyan responsabilidad en la investigación de antecedentes de sus empleados, y cumplimiento con las políticas de S-I de EP PETROECUADOR.
- Se deberá informar a todo candidato, considerado para ingresar a cualquier puesto de EP PETROECUADOR, que la información entregada en sus hojas de vida será verificada y sometida a investigación.

- Todo el personal que ingrese y tenga acceso a información sensible de la empresa, deberá suscribir acuerdos de confidencialidad de acuerdo al tipo de información que gestione. En el anexo 1 se incluye un ejemplo de un acuerdo de confidencialidad.

4.3.2.3 Sobre las responsabilidades de EP PETROECUADOR

EP PETROECUADOR deberá asegurar que sus empleados y contratistas:

- Estén debidamente informado de sus roles y responsabilidades, antes de tener acceso a la información del sistema ERP.
- Conozcan los lineamientos de S-I en las actividades que van a realizar.
- Cumplan con la normativa interna y las políticas de S-I establecidas.

4.3.2.4 Conocimiento, educación y capacitación

- Todo el personal de EP PETROECUADOR, y de ser necesario los contratistas, deberán recibir capacitación y actualización de conocimientos sobre S-I.
- La capacitación de S-I, deberá incluir la inducción para conocimiento y uso de las políticas y normas de la empresa.
- Se debe verificar que el personal asignado a tareas de S-I cumpla con los requisitos de especialización y formación de acuerdo a los roles y responsabilidades asignados, caso contrario deberán incluirse en los planes de capacitación de la empresa.
- EP PETROECUADOR debe impulsar iniciativas de concienciación, por parte de todos los empleados, sobre la importancia de la S-I en todas las actividades empresariales.

4.3.2.5 Sobre la terminación de la relación laboral o cambio de empleo

- Toda terminación de relación laboral deberá considerar los acuerdos de confidencialidad establecidos, y se deberá implementar los métodos de control que garanticen su cumplimiento durante el tiempo posterior a la separación que establezca el acuerdo.
- El área de recursos humanos, encargada de gestionar la terminación de la relación laboral, deberá trabajar en conjunto con el área de seguridad para manejar los aspectos relevantes con la S-I.
- La salida de personal deberá considerar la deshabilitación de los permisos de acceso de manera inmediata o incluso de forma previa a la notificación, verificando los roles y responsabilidades asignados o relación con grupos de acceso. La deshabilitación de los permisos no implica que sean eliminados de registros o históricos ya que esta información puede ser de utilidad en procesos de auditoria o similares.
- Se deberá informar a todo el personal relacionado, sobre la salida o separación de funcionarios para que se evite enviar o compartir información con la persona que se va.
- El cambio de empleo o puesto dentro de EP PETROECUADOR deberá ser considerado de forma similar a la terminación en el sentido de los permisos de acceso a la información, es decir que se deberá deshabilitar todo permiso actualmente asignado y posteriormente se procederá a asignar los nuevos permisos según corresponda, esta también es una consideración válida para los procesos de auditoría.
- Se debe identificar los puestos claves y el personal asignado a dichos puestos, para establecer planes de relevo o reemplazo en caso de ausencia de dicho personal, ya sea por separación definitiva o rotación.

4.3.2.6 Métricas

- Cantidad de perfiles y antecedentes verificados por parte de Talento Humano.
- Cantidad de personal debidamente capacitado de acuerdo a las necesidades identificadas.
- Cantidad puestos clave identificados, cuyo personal asignado no cuenta con reemplazo en caso de ausencia o separación.

4.3.3 *Política de respuesta a incidentes de seguridad*

4.3.3.1 Objetivo

- Proporcionar directrices generales para el manejo de incidentes de seguridad de manera que sean corregidos de forma oportuna.
- Establecer los canales de información de eventos y su posterior registro.

4.3.3.2 Incidente de seguridad

Es la materialización de un riesgo, que afecta la confidencialidad, integridad o disponibilidad de la información.

4.3.3.3 Sobre el reporte de incidentes de S-I

- Es obligación de todo funcionario de EP PETROECUADOR reportar cualquier incidente de seguridad lo más pronto posible, pero se prohíbe que tome acciones correctivas por su cuenta. Se consideran incidentes de seguridad las siguientes eventos:
    - Pérdida del servicio, equipo o medios
    - Mal funcionamiento o sobrecarga del sistema
    - Errores humanos de buena o mala fe
    - Incumplimientos de las políticas o lineamientos
    - Cambios del sistema no controlados o documentados

- Mal funcionamiento del software o hardware
- Violaciones de acceso

- Se establece la mesa de servicios de TIC como el punto de contacto para reportar los incidentes de seguridad.
- Es obligación de la mesa de servicios de TIC solicitar la información relacionada al incidente de acuerdo al formato detallado en el anexo 3.
- Los incidentes de seguridad relacionados con vulnerabilidades en software o hardware, deben ser mantenidos en reserva mientras son tratados por el equipo asignado y se debe advertir al personal que las conozca o que las reportó, que se abstenga de divulgarlas o ponerlas a prueba bajo cualquier circunstancia.

4.3.3.4 Sobre la gestión de incidentes de S-I

- Los incidentes reportados a la mesa de servicios de TIC, serán clasificados de acuerdo a su naturaleza, y deberán ser tratados mediante procedimientos específicos establecidos por el área de S-I.
- Los procedimientos para la gestión de incidentes deberán cubrir de forma obligatoria los siguientes aspectos:
    - Análisis e identificación de la causa del incidente
    - Contención
    - Planeación e implementación de la acción correctiva
    - Escalamiento, en caso de ser necesario
    - Documentación exhaustiva de todas las acciones tomadas
    - Comunicación con las partes afectadas
    - Reporte a la autoridad apropiada o entidad de control de ser el caso

- El área de S-I será la responsable de analizar la información relacionada a los incidentes de seguridad para proponer planes de mejora continua de la S-I, basados en la caracterización de los incidentes.

4.3.3.5 Métricas

- Número de incidentes caracterizados y tratados por parte del área de S-I.
- Tiempo de respuesta a incidentes.

4.4 Políticas dependientes de S-I de EP PETROECUADOR

Las siguientes políticas utilizan como entrada las funciones de seguridad y sus lineamientos, pero abarcan campos más amplios del gobierno y gestión de TIC. En estas políticas no se establecen métricas, ya que su efectividad depende de otros aspectos de gestión que no son considerados para la política de S-I.

4.4.1 *Política de gestión de comunicaciones y operaciones*

4.4.1.1 Objetivo

- Asegurar la operación correcta y segura de los módulos del sistema ERP.

4.4.1.2 Alcance

- Se definirá los lineamientos principales relacionados con la S-I de los procedimientos de operación del sistema ERP de EP Petroecuador.

4.4.1.3 Sobre los procedimientos y responsabilidades operacionales

- Todos los procedimientos de operación y mantenimiento del sistema ERP deben estar documentados, y disponibles para el personal que forma parte del equipo de administración.

- Los procedimientos serán elaborados en conjunto por todas las áreas de TIC, deberán apegarse a las especificaciones técnicas del fabricante de EBS y los estándares de EP PETROECUADOR. En caso de duda se hará uso de los servicios de soporte adquiridos como parte del licenciamiento del sistema, incluyendo la base de conocimientos del portal "My Oracle Support"[70].

4.4.1.4 Sobre la segregación de los deberes

- Los procedimientos establecidos para la administración del sistema ERP deberán identificar claramente los roles y responsabilidades involucradas.
- Las responsabilidades de cada área deberán estar segregadas, con el objetivo de reducir los errores involuntarios o las modificaciones no autorizadas. De la misma manera que se establece la segregación de funciones, se debe establecer el mecanismo de coordinación entre las áreas involucradas para que la segregación sea solo a nivel de actividades y no de objetivos de área o procesos empresariales.

4.4.1.5 Sobre la separación de los medios de desarrollo, prueba y operación.

- EP PETROECUADOR deberá contar con al menos 3 ambientes de EBS desarrollo, prueba y producción.
- Los ambientes de prueba y desarrollo deberán emular lo más posible el ambiente de producción, y deberán cumplir con las matrices de compatibilidad de software/hardware establecidas por el fabricante.

[70] My Oracle Support: Base de conocimiento de los productos Oracle y sitio de descarga de parches y actualizaciones, manuales, guías de diagnóstico, solución de problemas, etc.

- Los ambientes deberán mostrar obligatoriamente indicaciones, en los menús o formularios, que permita identificar y diferenciar claramente cada uno de ellos.
- Las configuraciones de encriptación y protección de información sensible de la base de datos será la misma en todos los ambientes.
- Los ambientes de pruebas y desarrollo deberán estar aislados del ambiente de producción y bajo ninguna circunstancia deberán compartir los mismos recursos de hardware y software, inclusive bajo esquemas de infraestructura virtualizada.

4.4.1.6 Sobre la gestión de la capacidad.

- Es obligación de las áreas de aplicaciones e infraestructura monitorear de manera continua las capacidades de almacenamiento, procesamiento y ancho de banda asignados al ERP.
- Se deben realizar análisis de crecimiento y proyección de las necesidades de recursos del sistema ERP, esta actividad será de mutua responsabilidad entre las áreas funcionales y las áreas de TIC.

4.4.1.7 Sobre los respaldos o backups.

- Las características de copias de respaldo, del sistema ERP, relacionadas a frecuencia y periodo de retención, se ajustarán de acuerdo a las necesidades propias del negocio. Estas deberán ser afinadas de manera continua y serán incluidas como parte de los procedimientos y estándares del área de datos.
- Todos los respaldos considerados especiales, es decir que no se realicen bajo las políticas generales, deberán ser solicitados de manera formal utilizando el formulario del anexo 2.

- Las copias de respaldo deberán ser probadas periódicamente para verificar su funcionalidad.
- Todos los respaldos deben ser almacenados en un medio diferente al de origen y de ser posible apartado de este en un lugar físico diferente.
- Los respaldos deberán tener los mismos niveles de protección física implementados en los ambientes de producción del ERP.

4.4.1.8 Sobre la seguridad de los servicios de red.

- El área de comunicaciones será la responsable de verificar, monitorear y exigir los niveles de servicio con la empresa que brinde los enlaces de datos externos a EP PETROECUADOR.
- Los niveles de servicio deberán estar documentados en acuerdos formales y deberán ser ajustados de acuerdo al monitoreo de la red y la carga efectiva de los enlaces.

4.4.2 *Política de Adquisición, desarrollo y mantenimiento de SI*

4.4.2.1 Objetivo

- Garantizar que la seguridad sea parte integral de los sistemas de información.

4.4.2.2 Sobre las especificaciones de los requerimientos de seguridad

- Todos los sistemas que sean adquiridos de forma complementaria o que deban integrarse con el sistema ERP de EP PETROECUADOR, deberán mantener los estándares de seguridad definidos por la empresa.

- Las validaciones de cumplimiento con las políticas y estándares deberán ser verificados mediante procesos de prueba, antes y durante el periodo de adquisición formal.
- Toda integración o nueva funcionalidad que se agregue al ERP deberá ser valorada en función del riesgo que agregue al sistema y de ser el caso se deberá establecer los controles apropiados para tratar los riesgos.

4.4.2.3 Sobre la gestión de claves criptográficas

- Los archivos de claves criptográficas que forman parte de las configuraciones del ERP deberán ser protegidas contra modificación, pérdida y destrucción, mediante procedimientos de copias de respaldo, registros de auditoría y restricción de acceso.
- Los procedimientos de copias de respaldo de la base de datos deberán también incluir copias de respaldo de las claves criptográficas utilizadas para cifrado, diferenciando de manera obligatoria los medios de almacenamiento y la responsabilidad de custodia de estas claves.
- Las claves comprometidas, por incidentes de seguridad o similares, deberán ser destruidas o modificadas, considerando todos los aspectos de la continuidad del negocio.
- En el caso de claves y certificados públicos se deberá gestionar para que dichos elementos criptográficos sean verificados por una entidad certificadora reconocida, garantizando su autenticidad y el no repudio de la información generada por EP PETROECUADOR.

4.4.2.4 Sobre el control de las vulnerabilidades técnicas

- El área de S-I, con el apoyo de las áreas de TIC, serán las responsables de recolectar información relacionada con el ERP que permita identificar vulnerabilidades técnicas del sistema.
- La identificación de las vulnerabilidades técnicas deberá estar acompañada de una valoración de riesgos asociados y las acciones a tomarse, las cuales podrían incluir el parchado o actualización del sistema.
- La aplicación de parches y actualizaciones deberá ser evaluada en función de los riesgos asociados a su instalación como tal, por tanto se deberá establecer procedimientos que involucren la instalación y verificación previa en el ambiente de pruebas del ERP, antes de ser aplicados en el ambiente de producción.
- Toda instalación de parches o actualizaciones deberá estar fundamentada en la documentación técnica del fabricante, y en caso de duda se deberá utilizar las líneas de soporte oficiales contratadas.
- Si los parches no están disponibles en el momento de la detección de la vulnerabilidad, se deberá establecer procedimientos de monitoreo constante y salvaguardas, que eviten ataques o mitiguen su impacto en el caso de materializarse.

4.5 Estructura Organizacional del área de S-I de EP PETROECUADOR

Para la definición del área de S-I de EP PETROECUADOR se han considerado algunas variables que caracterizan a esta empresa, con el objeto de proponer un esquema que se ajuste a las necesidades de negocio y beneficie los procesos de adopción de un SGSI. Los aspectos tomados en cuenta son los siguientes:

- Cultura organizacional: Con respecto a este punto, EP PETROECUADOR demuestra una cultura organizacional en proceso de consolidación; debido, entre algunas causas, a la fusión de sus empresas filiales las cuales aún mantienen características distintivas.
- Tamaño de la empresa: Se considera como una empresa grande al contar con más de 4500 empleados, 3061 equipos personales y 433 servidores, distribuidos a nivel nacional.
- Grado de madurez de las áreas de seguridad: se considera en un grado de desarrollo inicial, debido a que el área de S-I actual fue aprobada por las autoridades de la empresa pero aún no ha sido ejecutada.

De acuerdo a los antecedentes descritos, la propuesta de la estructura organizacional para el área de seguridad, cambia el nivel de reporte del jefe de seguridad hacia el Gerente de Tecnologías de la Información y Comunicación, y ubica el área de seguridad al mismo nivel que el área de arquitectura, de acuerdo a la Figura 33.

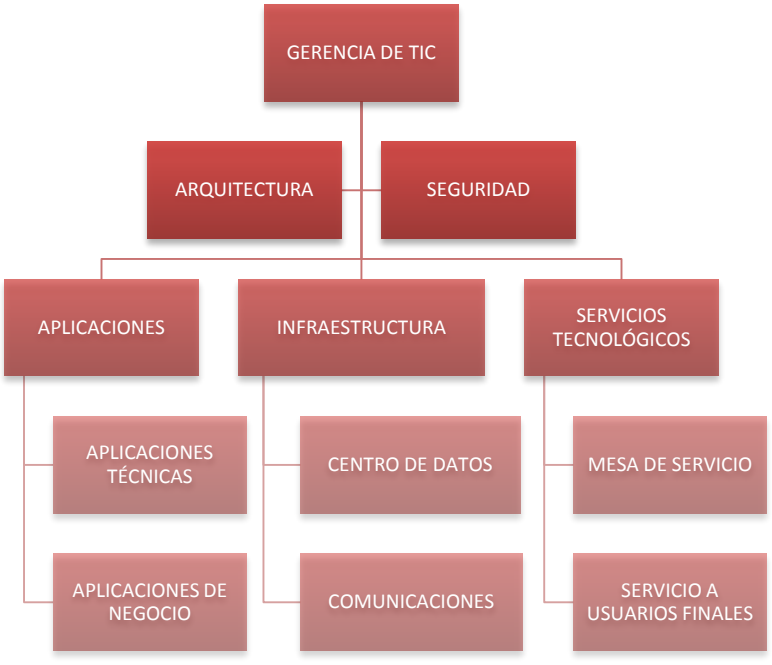

Figura 33 Ubicación del área de seguridad en Estructura Organizacional

La estructura propuesta para la estructura organizacional presenta las siguientes ventajas:

- Se relaciona en mayor medida a la realidad del estado del arte de la S-I de la empresa y el grado de madurez.
- Facilita que la S-I se alinee con todas las iniciativas de TI al estar al mismo nivel que el área de arquitectura.

Por otro lado los inconvenientes que podrían presentarse según algunos factores relacionados con la gestión de TIC son:

- Las iniciativas de TI pueden solapar las de S-I, debido a presiones sobre la Gerencia de TIC por el cumplimiento de tareas puramente técnico/operativas para cubrir los requerimientos de negocio.
- Potencial conflicto de intereses, debido a que las áreas de arquitectura y S-I responden a una misma autoridad; es decir que las actividades de ejecución y control pertenecen a una sola área.
- Las actividades desempeñadas por los profesionales de seguridad pueden ser enfocadas a la seguridad informática y no a la seguridad de la información, es decir que no exista un enfoque suficiente sobre el negocio.

4.5.1 *Madurez del área de seguridad*

El éxito de la estructura propuesta depende de una madurez y evolución mantenida, que permitan pasar el área de S-I desde un nivel técnico, a un gerencial, de negocio y finalmente estratégico. Los inconvenientes descritos en la presente propuesta, pueden ser minimizados controlando los siguientes aspectos:

- Partes interesadas: Se debe verificar que la toma de decisiones, asesoría e influencia que esta área realice, se ajuste a los intereses de las partes interesadas; sean estas otras estructuras, entidades organizativas, clientes o proveedores.
- Metas: el área de seguridad debe ser un catalizador para la consecución de las metas corporativas; para lo cual debe contar con actividades y principios operativos bien definidos.
- Ciclo de vida: la estructura debe ser diseñada, implementada, verificada, mejorada, y de ser el caso eliminada para dar paso a una reestructura completa.
- Buenas prácticas: son esenciales, por tanto deben ser utilizadas para la definición de principios operativos, composición, ámbito de control, niveles de autorización, delegación de autoridad y procedimientos de escalado. En este punto específico es importante recordar la utilización de ISO/IEC 27002 como guía principal de buenas prácticas.

4.5.2 *Roles y responsabilidades del área de seguridad*

El área de seguridad estará conformada por 2 roles principales, el Jefe de seguridad de la Información y el Analista de seguridad de la información agrupado bajo 2 actividades principales, de acuerdo a la Figura 34.

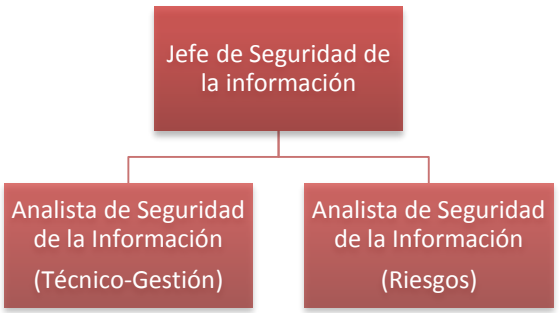

Figura 34 Estructura organizacional del Área de Seguridad

4.5.2.1 Jefe de seguridad de la información (CISO[71])

Misión:

Definir, mantener y controlar políticas, procesos, procedimientos y estándares del sistema de gestión de seguridad de la información para garantizar la integridad, disponibilidad y confidencialidad de la información de EP PETROECUADOR.

Funciones y responsabilidades:

- Definir y comunicar la estrategia de seguridad de la información alineada con la estrategia de negocio
- Planificar, coordinar y mantener el Plan de Seguridad de la Información basado en la gestión de riesgos de seguridad de TIC.
- Controlar el cumplimiento y aplicación de los procedimientos y estándares definidos para la seguridad de la información.
- Formular y mantener el plan de contingencia de seguridad que garantice la disponibilidad, confidencialidad e integridad de la información.

4.5.2.2 Analista de seguridad de la información (ISM[72])

Misión:

Aplicar las políticas, procesos, procedimientos y estándares definidos en el sistema de gestión de seguridad de la información para garantizar la integridad, disponibilidad y confidencialidad de la información de la EP PETROECUADOR

Funciones y Responsabilidades:

- Evaluar los riesgos de seguridad de la información y proponer acciones a incluirse en el Plan de Seguridad de la Información.
- Gestionar los accesos a los servicios tecnológicos empresariales.

---

[71] CISO: Chief Information Security Officer

[72] ISM: Information Security Manager

- Participar en la implementación del plan de seguridad de la información.
- Monitorear e informar acerca del cumplimiento y aplicación de los procedimientos y estándares definidos para la S-I.

4.6 Procesos

Para la selección de los Procesos habilitantes de COBIT 5, es importante conocer cuáles son las relaciones de estos con las metas de TI, facilitando la priorización y selección de nuevos procesos para ser implementados, o en el caso que ya existan en la empresa, para que sean actualizados.

En el caso del sistema ERP de EP PETROECUADOR, se utilizó las metas de TI (1, 2, 7, 8, 9, 10, 12, 14 y 15) identificadas en la Tabla 23 y como guía para definir las relaciones el apéndice C de COBIT 5 denominado "Mapeo Detallado de las Metas Relacionadas con las TI y los procesos Relacionados con las TI". La Tabla 24 muestra las relaciones existentes entre procesos y metas en 2 niveles:

- La escala 'P' para principal, cuando exista una importante relación, es decir, los procesos habilitantes son requisitos fundamentales para cumplir con las metas relacionadas de TI.
- La escala 'S' para secundario, cuando los procesos habilitantes que influyan de una manera indirecta con las metas de TI.

Tabla 24 Relación entre metas de TI y Procesos

			Meta relacionada con TI								
			Alineamiento de TI y estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Disponibilidad de información útil y fiable para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI Aprendizaje y Crecimiento
			1	2	7	8	9	10	12	14	15
Procesos de COBIT 5			Financiera		Cliente				Interna		
Evaluar, Orientar y Supervisar	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	**P**	**S**	**P**		**S**	**S**	**S**	**S**	**S**
	EDM02	Asegurar la Entrega de Beneficios	**P**		**P**	**S**			**S**	**S**	
	EDM03	Asegurar la Optimización del Riesgo	**S**	**S**	**S**	**S**		**P**		**S**	**P**
	EDM04	Asegurar la Optimización de los Recursos	**S**		**S**	**S**	**P**				
	EDM05	Asegurar la Transparencia hacia las partes interesadas	**S**	**S**	**P**					**S**	**S**
Alinear, Planificar y Organizar	APO01	Gestionar el Marco de Gestión de TI	**P**	**P**	**S**		**P**	**S**	**S**	**S**	**P**
	APO02	Gestionar la Estrategia	**P**		**P**	**S**	**S**		**S**	**S**	**S**
	APO03	Gestionar la Arquitectura Empresarial	**P**		**S**	**S**	**P**	**S**	**S**	**S**	
	APO04	Gestionar la Innovación	**S**			**P**	**P**		**S**	**S**	
	APO05	Gestionar el portafolio	**P**		**S**	**S**	**S**				
	APO06	Gestionar el Presupuesto y los Costes	**S**		**S**	**S**					
	APO07	Gestionar los Recursos Humanos	**P**	**S**	**S**		**S**	**S**			**S**
	APO08	Gestionar las Relaciones	**P**		**P**	**S**			**P**		**S**
	APO09	Gestionar los Acuerdos de Servicio	**S**		**P**	**S**	**S**	**S**		**P**	**S**
	APO10	Gestionar los Proveedores		**S**	**P**	**S**	**P**	**S**		**S**	**S**
	APO11	Gestionar la Calidad	**S**	**S**	**P**	**S**	**S**			**S**	**S**
	APO12	Gestionar el Riesgo		**P**	**S**	**S**	**S**	**P**		**S**	**S**
	APO13	Gestionar la Seguridad		**P**	**S**	**S**		**P**		**P**	

Continúa →

			Meta relacionada con TI								
			Alineamiento de TI y estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Disponibilidad de información útil y fiable para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI Aprendizaje y Crecimiento
			1	2	7	8	9	10	12	14	15
Procesos de COBIT 5			Financiera		Cliente				Interna		
Construcción, Adquisición e Implementación	BAI01	Gestionar los Programas y Proyectos	**P**		**S**	**S**					
	BAI02	Gestionar la Definición de Requisitos	**P**	**S**	**P**	**S**	**S**	**S**	**P**	**S**	
	BAI03	Gestionar la Identificación y la Construcción de Soluciones	**S**		**P**	**S**			**S**	**S**	
	BAI04	Gestionar la Disponibilidad y la Capacidad			**P**	**S**	**S**			**P**	
	BAI05	Gestionar la introducción de Cambios Organizativos	**S**		**S**	**P**	**S**		**S**		
	BAI06	Gestionar los Cambios			**P**	**S**	**S**	**P**	**S**	**S**	**S**
	BAI07	Gestionar la Aceptación del Cambio y de la Transición			**S**	**P**	**S**		**P**	**S**	**S**
	BAI08	Gestionar el Conocimiento	**S**		**S**	**S**	**P**	**S**		**S**	
	BAI09	Gestionar los Activos		**S**	**S**		**S**	**S**		**S**	**S**
	BAI10	Gestionar la Configuración		**P**		**S**	**S**	**S**		**P**	**S**
Entregar, dar Servicio y Soporte	DSS01	Gestionar las Operaciones		**S**	**P**	**S**	**S**	**S**		**S**	**S**
	DSS02	Gestionar las Peticiones y los Incidentes del Servicio			**P**	**S**		**S**		**S**	**S**
	DSS03	Gestionar los Problemas		**S**	**P**	**S**	**S**		**S**	**P**	**S**
	DSS04	Gestionar la Continuidad	**S**	**S**	**P**	**S**	**S**	**S**	**S**	**P**	**S**
	DSS05	Gestionar los Servicios de Seguridad	**S**	**P**	**S**	**S**		**P**	**S**	**S**	**S**
	DSS06	Gestionar los Controles de los Procesos del Negocio		**S**	**P**	**S**		**S**	**S**	**S**	**S**
Supervisión, Evaluación y Valoración	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	**S**	**S**	**P**	**S**	**S**	**S**		**S**	**P**
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno		**P**	**S**	**S**		**S**		**S**	**P**
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos		**P**	**S**			**S**			**S**

4.6.1 ***Actividades específicas de seguridad para los procesos de COBIT 5***

En esta sección se complementa la guía genérica "Procesos catalizadores COBIT 5", definiendo actividades de proceso con un enfoque en S-I según ISO 27002, para los procesos cuya relación con las metas de TI sea principal 'P', de acuerdo a la Tabla 24. Adicionalmente, se selecciona las 2 metas principales, como un ejercicio práctico de priorización que sería de utilidad en cualquier otra implementación. Las metas seleccionadas, por ser las mayormente tratadas en esta investigación, son:

- Seguridad de la información, infraestructura de procesamiento y aplicaciones
- Alineamiento de TI y estrategia de negocio

4.6.1.1 EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno.

Actividades:

- Analizar e identificar factores legales, regulatorios y obligaciones contractuales que influencien en el diseño de gobierno de S-I.
- Definir principios que guíen el diseño de catalizadores para S-I y promocione un ambiente adecuado.
- Obtener comprometimiento de los niveles ejecutivos con la S-I y la gestión de riesgos.
- Alinear la estrategia de seguridad con la estrategia de negocio.

4.6.1.2 EDM02 Asegurar la entrega de beneficios

Actividades:

- Identificar y registrar los requerimientos de las partes interesadas para proteger sus intereses a través de la S-I.

- Establecer un método para demostrar el valor de la S-I, incluyendo una colección de información relevante.
- Dar seguimiento a las iniciativas de S-I y verificar la entrega de beneficios

4.6.1.3 EDM03 Asegurar la optimización de riesgos.

Actividades:

- Controlar el nivel de integración de la gestión de riesgos de la información con la gestión de riesgos corporativa.
- Definir niveles de riesgo aceptados, para mantener un equilibrio entre los riesgos y las oportunidades de negocio.

4.6.1.4 APO01 Gestionar el marco de gestión de TI

Actividades:

- Definir las funciones de seguridad, incluyendo roles internos y externos (Jefe de seguridad, Analista de seguridad).
- Determinar los grados de responsabilidad con la S-I de los roles externos y comunicarlos.
- Alinear la organización de la seguridad de la información con los modelos organizacionales empresariales.
- Planificar evaluaciones continuas para determinar cumplimiento con políticas y procedimientos de S-I.

4.6.1.5 APO03 Gestionar la estrategia

Actividades:

- Entender como la S-I soportaría las metas empresariales tomando en cuenta las necesidades de las partes interesadas.

- Desarrollar criterios claros relacionados con la S-I y priorizar la atención de no cumplimientos o brechas.

4.6.1.6 APO07 Gestionar los recursos Humanos

Actividades:

- Asegurarse que los requerimientos de seguridad se apliquen en los procesos de reclutamiento de empleados y contratistas.
- Proporcionar desarrollo profesional con programas de capacitación en S-I
- Establecer criterios de S-I en la evaluación de personal

4.6.1.7 APO08 Gestionar las Relaciones

Actividades:

- Entender el negocio y como la S-I afecta o facilita las actividades de este.
- Establecer un enfoque para influir contactos claves con respecto a la S-I
- Incorporar requerimientos de S-I en los procesos de mejora continua.

4.6.1.8 APO12 Gestionar El riesgo

Actividades:

- Identificar y recolectar información que habilite la identificación de riesgos relacionados con S-I.
- Identificar, analizar y evaluar el riesgo de la información.
- Monitorear continuamente los riesgos de la información
- Aplicar procesos de mitigación de riesgos específicos.

4.6.1.9 APO13 Gestionar la seguridad

Actividades:

- Definir el ámbito y alcance del SGSI, en términos de negocio, organización, localización, activos y tecnología.
- Definir el SGSI en concordancia con las políticas, normativa y marco legal vigente en la empresa.
- Verificar periódicamente la efectividad del SGSI, incluyendo política, objetivos, prácticas, etc.
- Llevar a cabo auditorías internas al SGSI.
- Registrar acciones y eventos que pueden tener un impacto en la efectividad y desempeño del SGSI.

4.6.1.10 BAI01 Gestionar programas y proyectos

Actividades:

- Incorporar S-I en los requerimientos y los estudios de factibilidad para cada proyecto que forme parte de los programas.
- Establecer un proceso para asegurar que toda la información relacionada al proyecto, recolectada o generada, sea segura.
- Desarrollar un plan de S-I que identifique el ambiente y controles a ser implementados para proteger los activos organizacionales.
- Integrar S-I en la gestión de proyectos de TI y de negocio.
- Realizar evaluaciones periódicas para asegurar que los requerimientos de S-I están siendo implementados.

4.6.1.11 BAI02 Gestionar definiciones de requerimientos

Actividades:

- Investigar, definir y documentar requerimientos de S-I, relacionados con confidencialidad, integridad y disponibilidad.

- Analizar los requerimientos de S-I con las partes interesadas y los implementadores técnicos.
- Llevar a cabo una valoración de riesgos para identificar los controles de S-I relevantes para las actividades empresariales.
- Validar los requerimientos de S-I con las partes interesadas y los implementadores técnicos.

4.6.1.12 BAI06 Gestionar cambios

Actividades:

- Asegurar que se lleve a cabo una evaluación de los potenciales impactos en la S-I provocados por los cambios.
- Asegurar que la política de S-I se adapta a las necesidades del negocio.
- Desarrollar prácticas para considerar el impacto en la S-I de las amenazas y tecnologías emergentes.

4.6.1.13 DSS05 Gestionar servicios de seguridad

Actividades:

- Sensibilizar sobre el software malicioso y hacer cumplir los procedimientos de prevención y responsabilidades.
- Instalar herramientas para protección contra software malicioso con opciones de actualización de definiciones activadas.
- Distribuir todo el software de protección centralizado, con opciones de configuración y actualización centralizada.
- Filtrar el tráfico entrante, para protegerse contra información no solicitada.
- Realizar actividades de entrenamiento relacionado con malware y métodos para navegación segura en internet.

- Establecer y mantener una política de seguridad para la conectividad en relación a la valoración de riesgos de la empresa.
- Cifrar la información en tránsito de acuerdo a su clasificación.
- Establecer mecanismos confiables para soportar la transmisión y recepción de información.
- Llevar a cabo pruebas periódicas de la seguridad de los sistemas para determinar idoneidad de las configuraciones realizadas.
- Configurar los sistemas operativos de forma segura.
- Implementar mecanismos de bloqueo automático.
- Cifrar la información en discos y respaldos de acuerdo a la clasificación de la información.
- Gestionar las conexiones remotas y accesos (VPN, oficinas remotas).
- Proteger la integridad de los equipos
- Disponer o desechar quipos terminales de forma segura.
- Mantener accesos a los sistemas de acuerdo a los roles y responsabilidades asignadas.
- Realizar revisiones periódicas de las cuentas y privilegios asignados.
- Asegurarse que todos los usuarios y sus actividades, sean identificadas de forma única.
- Registrar toda la información relacionada con incidentes de S-I, que permitan realizar análisis de causa-efecto.

4.7 Cultura, ética y comportamientos

Este catalizador se enfoca tanto en las partes interesadas internas como en las externas y sus objetivos están relacionados con la ética organizacional, ética individual y los comportamientos individuales.

4.7.1 *Actividades relacionadas con la cultura de S-I*

Los comportamientos de todos los miembros de una empresa forman colectivamente la cultura de dicha empresa. Dicha cultura es caracterizada como un patrón de comportamientos, creencias, asunciones, actitudes y maneras de hacer las cosas. (Roessing, 2010). Bajo este criterio, las actividades para crear, fomentar y mantener un comportamiento deseado que influya en la cultura de EP PETROECUADOR, deben estar orientadas bajo buenas prácticas y deberían incluir las siguientes:

- Comunicación por parte de la empresa de los valores y los comportamientos fundamentales que rigen su funcionamiento.
- Concienciación de la conducta deseada, mediante comportamientos ejemplares por parte de las autoridades y agentes de cambio.
- Utilización de incentivos para promover las actitudes, normas y reglas que se ajusten con las políticas aceptadas por la organización

Debido a que la cultura trasciende las empresas y se extiende a través del tiempo, se debe establecer métodos de evaluación que verifiquen si las actividades llevadas a cabo han influenciado positivamente en la cultura organizacional; algunos ejemplos de las medidas que se pueden llevar a cabo a través del tiempo son:

- Estadísticas de uso de los recursos empresariales tecnológicos para fines no laborales.
- Fortaleza de las claves o contraseña utilizadas
- Número de claves compartidas, genéricas, escritas en lugares accesibles y otros tipos de prácticas no aceptadas.
- Número de malware instalado por los usuarios
- Número de incidentes de S-I repetitivos

4.7.2 *Liderazgo y agentes de cambio*

El liderazgo y los agentes de cambio o campeones, como son referidos en COBIT 5; son participantes claves que facilitan los cambios a través de la empresa, favoreciendo la adopción de buenas prácticas tanto en sus ámbitos de influencia como en las otras áreas de la empresa. Los agentes de cambio no se limitan a los niveles ejecutivos y para el caso del sistema ERP de EP PETROECUADOR podrían ser:

- Dueños de proceso (Manufactura, abastecimientos, finanzas), o líderes de frentes funcionales.
- Jefe de seguridad, Analista de seguridad
- Jefe de recursos humanos
- Gerente General

4.8 Información

La información no solamente es el principal sujeto de la S-I, sino que es un catalizador clave de esta. (ISACA, 2012). Como un catalizador de la S-I, la información puede tomar las siguientes formas:

- Estrategia de seguridad
- Presupuesto de seguridad
- Plan de seguridad
- Políticas
- Requerimientos de seguridad (SLA y OLA)
- Material de prevención y concienciación
- Reportes de revisión de S-I (hallazgos de auditoria, gestión de riesgos, evaluaciones)
- Perfil de riesgo
- Incidentes de seguridad

Para el caso del sistema ERP de EP PETROECUADOR, es de suma importancia que se identifique las partes interesadas para diseñar una distribución adecuada de la información, facilitando el acceso a quienes deben tenerlo y limitando a quienes no. Una definición típica entre los tipos de información y las partes interesadas es la siguiente:

- A: aprobador
- O: originador
- I : informado
- U: usuario

En la Tabla 25 se define los tipos de información y su relación con las partes interesadas que se identificaron para el sistema ERP de EP PETROECUADOR, de esta manera se puede definir un esquema de distribución y control para la información relacionada con el SGSI.

Tabla 25. Tipos de información y partes interesadas

Partes interesadas	Tipo de información									
	Estrategia de S-I	Presupuesto de S-I	Plan de S-I	Políticas	Requerimientos de S-I	Material de prevención y concienciación	Reportes de revisión de S-I	Catálogo de servicios de S-I	Perfil de riesgo de información	Incidentes de seguridad
Internas Corporativas										
Gerente General (CEO)	U			A		U			U	
Gerente Financiero (CFO)		A		U		U	I		U	
Jefe de seguridad de la información (CISO)	O	U	O	O	A	A	A	A	U	U
Dueños de procesos de negocio (Manufactura, abastecimientos, finanzas)				U	O	U		U	U	
Jefe de Recurso Humanos				U		U				
Internas TI										
Gerente de arquitectura (CIO)	U	O	U	U	U	U	I		U	U
Analista de seguridad de la información (ISM)	U	U	U	O	U	O	O	O	O	O
Externas										
Gobierno Nacional	I					I				
Aseguradoras		I				I	I		I	
Entidades de regulación		I				I	I			
Empresas asociadas						I	I			
Proveedores						I				
Auditores externos		I				I	I		I	I

4.9 Servicios, infraestructura, y aplicaciones

De acuerdo a los criterios de COBIT 5, la "Capacidad de los Servicios" es un término utilizado para referirse a la combinación de servicios, infraestructura y aplicaciones; por tanto, sus objetivos deben caracterizarse como tipos y niveles de servicio, propiamente dichos.

A continuación se describen los servicios relacionados con la S-I y las tecnologías de soporte, que se proponen estén disponibles como parte de un catálogo de catalizadores para el sistema ERP:

4.9.1 *Seguridad de arquitectura*

Incluye y mantiene criterios de S-I en la arquitectura del sistema ERP, proporciona gestión de la configuración de la S-I y actualiza o descubre nueva infraestructura relacionada.

4.9.1.1 Tecnologías de Soporte

- Base de Datos de la Gestión de Configuración (CMDB)
- Sistemas de gestión de activos
- Protocolo simple de gestión de red (SNMP)
- Agentes de reporte
- Scanner de vulnerabilidades
- Sistemas de auditoría automatizada

4.9.2 *Concienciación de seguridad*

Proporciona comunicación sobre la S-I, habilitando la concienciación y el entrenamiento.

4.9.2.1 Tecnologías de Soporte

- Cursos de entrenamiento
- Bases de conocimiento
- Herramientas colaborativas

4.9.3 *Desarrollo seguro*

Para el caso del sistema ERP de EP PETROECUADOR, las actividades de desarrollo son contratadas directamente con la empresa ORACLE debido a

obligaciones contractuales; por tanto, este servicio controla la utilización de prácticas de desarrollo seguro por parte de la contratista.

4.9.3.1 Tecnologías de Soporte

- Scanners de código
- Herramientas de análisis estático y binario.

4.9.4 ***Valoración de seguridad***

Ejecuta la valoración de la S-I de en sistemas, procesos, procedimientos, aplicaciones y unidades organizacionales. Proporciona identificación, evaluación, estimación y análisis de las amenazas de los activos, bajo criterios de gestión de riesgos.

4.9.4.1 Tecnologías de soporte

- Escáner de vulnerabilidades
- Sniffers
- Analizadores de protocolos
- Honeypots[73]
- Analizadores de logs
- Agentes Endpoint[74]

---

[73] HONEYPOTS: Herramienta de S-I compuesta por uno o varios equipos de TI que simulan ser vulnerables y permiten atraer a posibles atacantes recolectando información sobre estos y sus técnicas de ataque.

[74] AGENTES ENDPOINT: Paquete de software con capacidad de detección y prevención de ataques, similar a los sistemas IDS/IPS, que se instalan en los computadores de los usuarios finales.

4.9.5 *Sistemas configurados adecuadamente, alineados con los requerimientos de seguridad y la arquitectura de seguridad.*

Proporciona parámetros de configuración relacionados con la S-I, asegurando que todo equipo que pertenezca o esté relacionado con las actividades del ERP, cumpla con un conjunto de requerimientos o diseños de arquitectura.

4.9.5.1 Tecnologías de soporte

- Gestión de actualizaciones o parches
- Gestión de virtualización
- Herramientas de validación de firmas
- Módulos de núcleo o kernel del sistema operativo
- Monitoreo de integridad de archivos

4.10 Gente, habilidades y competencias

Este catalizador pretende definir el conjunto de habilidades y competencias[75] que cada una de las partes interesadas (gente), debe demostrar para asegurar que se toman decisiones correctas y que todas las actividades relacionadas con la S-I son completadas satisfactoriamente. Según COBIT 5, para operar exitosamente la función de S-I dentro de una empresa, es necesario que individuos con apropiados conocimientos y experiencia ejecuten dicha función.

De acuerdo a la propuesta para el área de S-I de la Figura 34, se identifican 2 roles principales que serán responsables de la función de S-I en EP PETROECUADOR,

[75] COMPETENCIAS: "Procesos complejos de desempeño con idoneidad en determinados contextos, integrando diferentes saberes (saber ser, saber hacer, saber conocer y saber convivir), para realizar actividades y/o resolver problemas con sentido de reto, motivación, flexibilidad, creatividad, comprensión y emprendimiento..." (Tobón, 2008)

estos son el Jefe de Seguridad de la Información y el Analista de Seguridad de la Información; por tanto, se definirán algunas características y competencias relacionadas con estos 2 roles según los criterios de COBIT 5.

4.10.1 *Jefe de Seguridad de la Información*

4.10.1.1 Experiencia

Se recomienda 5 años[76] de experiencia en gestión estratégica de S-I, Tecnologías de la Información y negocios; incluyendo actividades como:

- Creación, implementación y medición de políticas, principios, prácticas y actividades de S-I.
- Estrategia y gobierno de S-I.
- Cumplimiento con marcos regulatorios.

4.10.1.2 Formación

Tabla 26 Formación del Jefe de S-I

Requerimiento	**Descripción**
Educación	• Ingenierías en electrónica, computación, software • Ciencias de la computación • Postgrados en Gerencia de TIC o Negocios
Certificaciones	• CISM[77]

[76] De acuerdo a la normativa y manual de perfiles vigente en EP PETROECUADOR.

[77] CISM: Certified Information Security Management, certification soportada por ISACA.

4.10.1.3 Conocimientos, habilidades técnicas y comportamientos

Tabla 27 Conocimientos, habilidades y comportamientos del Jefe de S-I

Requerimiento	Descripción
Conocimientos	• Normativa interna • Cadena de valor • Tendencias de S-I, servicios y disciplinas • Marcos regulatorios y reglamentarios. • Estándares, buenas prácticas y marcos internacionalmente reconocidos y relacionados con el desarrollo de estrategias de S-I.
Habilidades Técnicas	• Amplio entendimiento para la gestión de: acceso, riesgos y vulnerabilidades. • Amplio conocimiento de: arquitectura de TI, protección de datos y comunicaciones.
Comportamientos	• Liderazgo y comunicación • Pensamiento estratégico • Percepción de sistemas y entornos • Innovación y mejora continua

4.10.2 ***Analista de Seguridad de la Información***

4.10.2.1 Experiencia

Se recomienda 3 años[78] de experiencia en S-I, incluyendo actividades adicionales como:

- Trabajo con software y hardware incluyendo sistemas operativos, base de datos, aplicaciones y redes.
- Gestión de redes LAN[79] y WAN[80]
- Implementación de mejores prácticas

[78] De acuerdo a la normativa y manual de perfiles vigente en EP PETROECUADOR.

[79] LAN: red de área local

[80] WAN: red de área amplia

4.10.2.2 Formación

Tabla 28 Formación del Analista de S-I

Requerimiento	Descripción
Educación	• Ingenierías en electrónica, computación, software • Ciencias de la computación
Certificaciones	• CRISC[81], CISSP[82], CCNA Security[83]

4.10.2.3 Conocimientos, habilidades técnicas y comportamientos

Tabla 29 Conocimientos, habilidades y comportamientos del Analista de S-I

Requerimiento	Descripción
Conocimientos	• Arquitectura de software y hardware • Arquitectura de S-I • Métodos para diseño de prácticas para S-I • Análisis de riesgos • Estándares de S-I/Buenas prácticas (familia ISO/IEC 27000, NIST[84]) • Leyes y reglamentos • Procedimientos de valoración de vulnerabilidades y hacking ético. • Auditoría informática
Habilidades Técnicas	• Amplio entendimiento de las TI y tecnologías emergentes. • Diseño e implementación de soluciones de TI. • Operaciones de TI.
Comportamientos	• Supervisión y monitoreo • Pensamiento abstracto y crítico • Percepción de sistemas y entornos

[81] CRISC: Certified in Risk and Information Systems Control, certificación otorgada por ISACA.

[82] CISSP: Certified Information Systems Security Professional, certificación otorgada por la (ISC)2 (International Information Systems Security Certification Consortium, Inc)

[83] CCNA Security: Certificación otorgada por CISCO Systems, enfocada al diseño de infraestructura segura.

[84] NIST: Instituto Nacional de Estándares y Tecnología, NIST por sus siglas en inglés

4.11 Criterios generales para la implementación del modelo de gestión de seguridad de la información

Los criterios que a continuación se detallan, tratan de describir las principales fases para implementar el modelo de gestión de seguridad de la información para el sistema ERP de EP PETROECUADOR en los módulos descritos en el alcance, de acuerdo a las características del GEIT[85] descritas en el marco de referencia COBIT 5 y el modelo planteado como parte de esta investigación.

4.11.1 *Crear el entorno apropiado*

Es de suma importancia que las partes interesadas claves dirijan y soporten las iniciativas de S-I para el ERP, con el objetivo de asegurar que las mejoras son logradas y sostenidas. Bajo este mismo criterio, se debe solicitar desde un inicio, la aprobación de las iniciativas por parte de las partes interesadas relevantes, demostrando que las necesidades de estas están siendo tomadas en cuenta.

Luego de obtener la aprobación, se debe proporcionar los recursos apropiados, definir y asignar roles y responsabilidades, elegir los procesos relevantes, establecer estructuras y finalmente verificar que todos catalizadores se encuentren alineados con las metas corporativas.

4.11.2 *Reconociendo puntos débiles y eventos disparadores*

Los puntos débiles y los eventos disparadores pueden aclarar la necesidad de implementar iniciativas de seguridad, relacionando las posibles mejoras con los problemas diarios. Algunos puntos débiles que podrían ser solucionados con iniciativas de S-I para el sistema ERP son:

---

[85] GEIT: Gobierno corporativo de las TI, o Governance of Enterprise IT por sus siglas en inglés

- Cumplimiento de requerimientos legales exigidos por la autoridad tributaria (SRI), u otro organismo de control.
- Indisponibilidad de la información por falta de recursos o denegación de servicio.

Los eventos disparadores son:

- Adopción de una nueva tecnología (ERP)
- Grandes cambios organizacionales, debidos a la reestructuración de EP PETROECUADOR.

4.11.3 *Habilitando el cambio*

Las iniciativas de S-I, no deben ser consideradas o enfocadas puramente como actividades técnicas; por el contrario, se debe también enfatizar en la gestión del factor humano.

Es importante reconocer agentes de cambio, en cada frente funcional del ERP, que persuadan y brinden el ejemplo utilizando prácticas seguras. De la misma manera, una comunicación directa y amplia que permita concienciar sobre la S-I en todos los niveles de la empresa, es un habilitante que facilitará la adopción de nuevas prácticas y la formación de una cultura organizacional adecuada.

4.11.4 *Un enfoque de ciclo de vida*

El modelo planteado, deberá cumplir un ciclo de vida, similar al de Figura 35, que permita sobrellevar los inconvenientes y la complejidad de implementar un conjunto de buenas prácticas orientadas por un marco integrador. El control y las medidas de efectividad, permitirán ajustar el modelo en función de las necesidades de las partes interesadas y las nuevas tendencias tecnológicas o amenazas a la S-I; de esta manera, se volverá a repetir el ciclo manteniendo un entorno apropiado, reconociendo los puntos débiles y habilitando el cambio de forma sostenida.

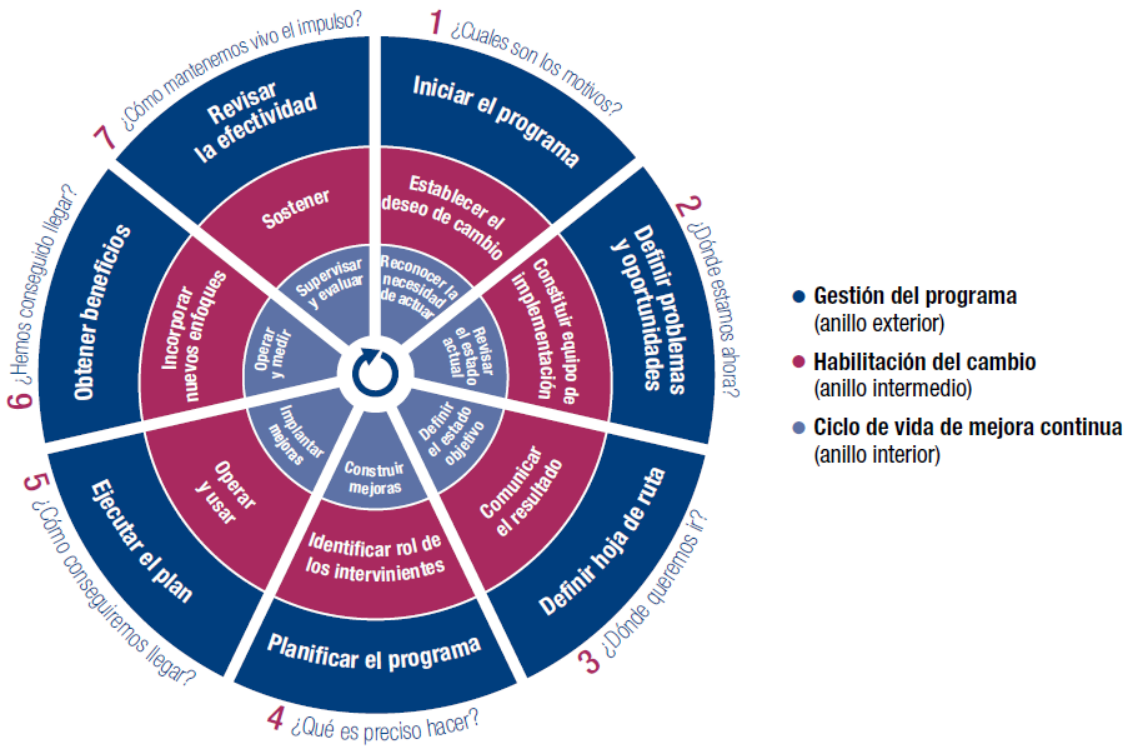

Figura 35 Ciclo de vida de implementación (ISACA, 2012)

5 Conclusiones y Recomendaciones

5.1 Conclusiones

- La información es uno de los activos más importantes de una empresa, y como tal su protección y adecuada gestión puede garantizar la continuidad de negocio.

- La falta de un modelo de gestión de seguridad de la información en EP PETROECUADOR, imposibilita gestionar los riesgos asociados con el uso de las TI, debido al desconocimiento de amenazas o vulnerabilidades y los métodos adecuados para tratarlas.

- El diseño y utilización de un modelo de gestión de S-I en EP PETROECUADOR, permitirá la estandarización de procesos y el cumplimiento con regulaciones como el acuerdo ministerial 166, emitido por la Secretaría Nacional de Administración Pública.

- El costo anual estimado de las actividades cibercrimen a nivel mundial es de 16.000 millones de dólares, y para el caso de EP PETROECUADOR las pérdidas por un minuto de caída de los sistemas de comercialización de combustibles podrían ascender a $11.000 USD., de acuerdo al promedio de ventas de octubre del 2013.

- 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 y que se complemente con mejores prácticas ampliamente aceptadas por la industria de TI.

- La cascada de metas, definida en COBIT 5, es un elemento útil para trasladar las metas corporativas en aspectos tecnológicos u organizacionales, caracterizando un modelo de gestión de S-I basado en: políticas, procesos, estructura organizativa, cultura organizacional, información, servicios-infraestructura y personas con sus habilidades.

- La infraestructura tecnológica de EP PETROECUADOR se encuentra en un nivel de riesgo alto debido a que el 29% y el 28% de los equipos externos e internos, respectivamente, están afectados por vulnerabilidades; y más del 50% de estas son consideradas graves o de alto riesgo de acuerdo al Sistema de Calificación de Vulnerabilidades Comunes (CVSS).

- La normativa interna de EP PETROECUADOR, relacionada con el macroproceso Tecnologías de la información y comunicación, cuenta con 26 procesos aprobados basados en la versión 4.1 de COBIT, pero no evidencia un SGSI completo que incluya políticas, procedimientos, controles, estructura organizacional, y métodos de evaluación de riesgos.

- La estructura organizacional de EP PETROECUADOR, cuenta con un área de seguridad de la información de reciente formación (Octubre de 2013), lo que indica un grado de madurez mínimo, pero un reconocimiento positivo de la importancia de la S-I en la empresa por parte de la alta gerencia.

- El análisis de riesgo cualitativo de S-I para el sistema ERP de EP PETROECUADOR demostró una relación inversa entre la frecuencia de ocurrencia y el impacto de las amenazas, es decir que amenazas con un mayor impacto son menos probables de ocurrir que amenazas con un menor impacto.

- De acuerdo al análisis de riesgo y la información crítica identificada para el sistema ERP, las amenazas con mayor impacto están relacionadas con los desastres naturales y la modificación deliberada de información, siendo esta última identificada como una amenaza interna que involucra a los usuarios del sistema.

- La propuesta del modelo de gestión de Seguridad de la Información para EP PETROECUADOR recoge y concreta las recomendaciones de las consultorías relacionadas con la creación de un área S-I, el diseño de políticas, procesos, y además

propone un enfoque de gobierno corporativo para la gestión de TI basado en la información y las necesidades de las partes interesadas.

- La necesidad de adopción de un modelo de gestión de seguridad de la información en EP PETROECUADOR se basa en tres aspectos principales: el estado de la S-I, el cumplimiento de requisitos legales establecidos por entidades de control y el cambio tecnológico representado por la adopción del sistema ERP como parte de la modernización de la empresa.

- Los Principios, Políticas y Marcos de Referencia son el catalizador o elemento principal sobre el cual se debe diseñar los modelos de gestión, debido a que establecen los lineamientos generales para los otros componentes, considerando los requisitos legales o marco regulatorio de cumplimiento obligatorio.

- El éxito de toda iniciativa de S-I está relacionada con el apoyo de la alta gerencia, quien debe reconocer y entender los beneficios de la S-I en la consecución de las metas corporativas.

- La utilización de metas corporativas como punto de partida para el diseño de modelos de gestión de S-I, es un enfoque que permite simplificar y priorizar los marcos de referencia evitando generar modelos desenfocados o demasiado extensos.

- 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, regulación y acuerdos ministeriales.

    - Reconocimiento y protección de información crítica de los procesos implementados.

    - Facilidad para tareas de auditoría

- Definición de los roles y responsabilidades del Jefe (CISO) y Analista de seguridad de la información.
- Segregación de tareas
- Mantenimiento de la identidad corporativa
- Alineamiento y cumplimiento de las metas de TI con las metas corporativas del ERP: integrar la información administrativa, alcanzar la gestión eficiente y mejorar el control de la empresa.
- Establecimiento de controles e indicadores claves de procesos relacionados con acuerdos de nivel de servicio, desarrollo de aplicaciones, integración de servicios y cumplimiento de políticas.

5.2 Recomendaciones

- Elaborar planes completos de remediación para las vulnerabilidades reportadas en los informes de hacking ético, y establecer revisiones periódicas de la infraestructura tecnológica de EP PETROECUADOR.
- Elaborar una línea base que permita determinar los riesgos, vulnerabilidades, tecnología, ataques, fugas de información, estadísticas y demás aspectos descriptivos de las S-I de EP PETROECUADOR.
- Incluir en el plan anual de capacitación cursos dirigidos a todo el personal de la EP PETROECUADOR, con el objetivo de concienciar sobre la importancia de la S-I en la empresa.
- Elaborar un plan estratégico para actualizar la normativa interna de EP PETROECUADOR utilizando la versión de COBIT 5 y complementar los aspectos faltantes utilizando las mejores prácticas definidas en ISO/IEC 27002.

- Brindar completo apoyo y respaldo por parte de la alta gerencia de EP PETROECUADOR al área de seguridad de la información y las iniciativas o actividades que emprenda.

- Incluir aspectos relacionados con la S-I y el análisis de riesgos de S-I en todos los proyectos que se desarrollen en EP PETROECUADOR.

- Evitar las iniciativas aisladas o puramente reactivas para la compra de soluciones tecnológicas de S-I, en favor de procesos de mejora ordenados, bien documentados y basados en las mejores prácticas que permitan un análisis causa efecto de los problemas detectados.

- Identificar e incluir las necesidades de todas las partes interesadas en las iniciativas de S-I, facilitando los principios de un gobierno corporativo de TI.

- Realizar un nuevo análisis de riesgos de S-I del sistema ERP cuando se implemente nuevas funcionalidades en el sistema, incluyendo interfaces para dispositivos móviles o integraciones con otros sistemas de la empresa.

- Realizar un análisis de factibilidad para la contratación de un proceso de consultoría relacionado con la implementación de un sistema de gestión de seguridad de la información (SGSI) en EP PETROECUADOR.

6 Acrónimos

APPLET: componente de una aplicación que se ejecuta en el contexto de otro programa.

BCG: Matriz de Crecimiento – Participación, o matriz Boston Consulting Group

CERT: Centro de Respuesta a Incidentes Informáticos

CIA: Confidentiality, Integrity and Availability

COBIT: Objetivos de Control para Información y Tecnologías Relacionadas.

CRAAM: CCTA Risk Analysis and Management Method

CVE: Vulnerabilidades y Exposiciones Comunes

DNS: Servicio de nombre de dominio

DoS: Denegación de servicio

EBS: E-Business Suite, por sus siglas en inglés.

ERP: Sistema de Planificación de Recursos Empresariales

EXPLOIT: Fragmento de código o conjunto de comandos que se utiliza para aprovechar una vulnerabilidad de seguridad de un sistema de información.

IDS: Sistema de Detección de Intrusos

IEC: Comisión Electrotécnica Internacional

IPS: Sistema de Prevención de Intrusos

ISACA: Information Systems Audit and Control Association.

ISO: Organización Internacional de Estandarización.

ITIL: Information Technology Infrastructure Library

JEE: Java Enterprise Edition

JRE: Java Runtime Environment

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

OCTAVE: Operationally Critical Threat, Asset, and Vulnerability Evaluation

OLA: Acuerdos de Nivel de Operación

OSSTMM: Open Source Security Testing Methodology Manual

OWASP: Open Web Application Security Project, por sus siglas en inglés.

PDCA: Plan, Do, Check, Act

PMBOK: Project Management Body of Knowledge

RDP: Remote Desktop Protocol

SGSI: Sistema de Gestión de Seguridad de la Información

S-I: Seguridad de la Información

SI: Sistema de información

SLA: Acuerdos de Nivel de Servicio

SMTP: Simple Mail Transfer Protocol

SNMP: Simple Network Management Protocol

SP: Special Publication

STIC: Subgerencia de Tecnologías de la Información y Comunicación

TI: Tecnologías de Información

TIC: Tecnologías de la Información y Comunicación

TSL/SSL: Transport Socket layer/Secure Socket Layer

VHF: Very High Frecuency

7 Referencias bibliográficas

Baldeón, M. J. (2012). Plan maestro de Seguridad Informática para la UTIC de la ESPE con lineamientos de la Norma ISO/IEC 27002. Sangolquí, Pichincha, Ecuador: ESPE.

Banco Central del Ecuador. (24 de 08 de 2013). *Portal del Banco Central del Ecuador*. Obtenido de http://www.bce.fin.ec/documentos/ServiciosBCentral/SistemaPagos/ReingenieriaSNP/AcuerdoConfidencialidadReingenieria.pdf

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/

Data Research DPU. (23 de 05 de 2012). *Portal de data Research DPU.* Obtenido de http://www.dpu.se/boston_e.html

Decreto Ejecutivo No. 315. (6 de ABRIL de 2010). *Créase la empresa pública de hidrocarburos del Ecuador, EP Petroecuador*. Quito, Pichincha, Ecuador.

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

ITGI, OCG. (2008). *Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa.* ITGI, OCG.

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

McAfee Labs. (2013). *McAfee Threats Report: Second Quarter 2013.* Santa Clara, CA: McAfee Labs.

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/

NIST. (2012). *Special Publication 800-30: Guide for Conducting Risk Assessment.* Gaithersburg.

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*. Rolling Meadows, IL: ISACA.

Siemens Enterprise. (08 de 07 de 2013). *How CRAMM works*. Obtenido de http://www.cramm.com/overview/howitworks.htm

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.