UNIVERSIDAD DE COSTA RICA

SISTEMA DE ESTUDIOS DE POSGRADO

PROPUESTA DE UNA HERRAMIENTA APLICATIVA PARA LA AUDITORÍA DE LA SEGURIDAD EN SISTEMAS Y REDES DE COMUNICACIÓN DEL GRUPO BEKAERT COSTA RICA BASADO EN COBIT®5 PARA SEGURIDAD DE LA INFORMACIÓN

Trabajo Final de Investigación Aplicada sometido a la consideración de la Comisión del Programa de Estudios de Posgrado en Administración y Dirección de Empresas para optar por el grado y título de Maestría Profesional en Auditoría de Tecnologías de la Información

Harold Alberto Hernández Castro

Carné 971646

Ciudad Universitaria Rodrigo Facio, Costa Rica

Junio 2015

DEDICATORIA

A Dios por darme vida, salud y sabiduría para afrontar obstáculos, reconocer errores y tener sapiencia en que el adquirir conocimiento es la base del ser humano.

A mis padres por formarme y creer firmemente con convicción en mis anhelos para el desarrollo de mi plan de mi vida, y por estar a mi lado en cada logro.

A mi esposa Gaby, por demostrarme día con día el significado de la valentía y el esfuerzo de luchar con una consigna de conquistar tu propósito de vida con amor y gallardía.

AGRADECIMIENTOS

En primera instancia agradezco profundamente a los profesores Dr. Sergio Espinoza Guido y el Lic. Gino Ramirez Solís por el apoyo en el desarrollo del presente trabajo de práctica aplicativa, por la orientación brindada y el seguimiento al logro de los objetivos planteados mediante sus recomendaciones.

Igualmente, correspondo mi gratitud al Lic. Sergio Briceño, al Ing. Ivan Echeverría y al Ing. Simón Pineda por permitirme desarrollar esta práctica profesional en la empresa Bekaert C.R., por facilitar la información requerida, el desarrollo de la aplicación de la herramienta y a la vez por los comentarios emitidos en la lectura del trabajo.

Prov.2:2-3. "Que tu oído se abra a la sabiduría, que tu corazón se doblegue a la verdad, apela a la inteligencia y déjate guiar por la razón".

Este trabajo final de investigación aplicada fue aceptado por la Comisión del Programa de Estudios de Posgrado en Administración y Dirección de Empresas de la Universidad de Costa Rica, como requisito parcial para optar al grado y título de Maestría Profesional en Auditoría de Tecnologías de Información.

_____

Dr. Sergio Espinoza Guido

Profesor guía

_____

Lic. Gino Ramirez Solís

Lector (Profesor de Posgrado)

_____

Msc. Sergio Briceño Hernández

Lector de Empresa

_____

Dr. Aníbal Barquero Chacón

Director Programa de Posgrado en Administración y Dirección de Empresas

_____

Lic. Harold Alberto Hernández Castro

Sustentante

Tabla de Contenidos

RESUMEN

El desarrollo del presente trabajo está basado en la conformación de una herramienta aplicativa para la auditoría de la seguridad en sistemas y redes de comunicación del grupo Bekaert Costa Rica fundamentado en COBIT 5, por medio de la cual se pueda medir los niveles de cumplimento de los marcos de referencia sobre las buenas prácticas de la gestión de los sistemas de información.

Como objetivo general se ha planteado el desarrollo de una herramienta para determinar el grado de cumplimiento del marco normativo y de mejores prácticas que le resulta aplicable a al Grupo Bekaert Costa Rica en materia de seguridad de las tecnologías de información, tanto física como lógica, esto con el fin de posibilitar la elaboración del diagnóstico de la situación actual de la empresa a nivel local examinando la eficacia de los controles de seguridad de las TIC y que a su vez funcione para procesos de auditoría futuros. Dicha empresa pertenece a un grupo global belga del sector construcción, siendo uno de los mayores productores de alambre de acero a nivel mundial y que recientemente se ha instalado en el país iniciando operaciones desde hace un año.

Inicialmente en el primer apartado se establecen los objetivos y alcances, así como la metodología a desarrollar, se enumeran los marcos de referencia en los que se basará la guía de auditoría que se desarrollará en este trabajo y donde además se enumeran los lineamientos generales sobre la seguridad de las TIC. A su vez, en este capítulo se describe el entorno organizacional de la empresa tanto a nivel global corporativo como a nivel de la región y localmente.

En el segundo capítulo se diseña y establece la herramienta de auditoría para elaborar el examen sobre el Sistema de Gestión de Seguridad de Información, establecida en la guía profesional de COBIT®5 *para Seguridad de la Información*, donde fueron obtenidos los

procesos y actividades para ser aplicados como base de medición de las actividades que deben realizarse con el fin de mantener una gestión de la seguridad bajo control y en regulación de las buenas prácticas globales.

En el tercer apartado del trabajo se detallan las secciones que contienen la aplicación del examen, las cuales definen el objetivo del proyecto, el alcance, la planificación preliminar y detallada, así como la preparación de los papeles de trabajo. Se han establecido los criterios de control para la gestión de las TI, donde se analizan las actividades y las métricas requeridas para cumplirlas. También se describe el proceso de verificación o aplicación de la guía de auditoría y finalmente la comunicación de los resultados que consta de los hallazgos determinados en la evaluación realizada presentada bajo el formato del informe de auditoría de tecnologías de información.

Finalmente se enumeran las conclusiones determinadas luego de ejecutar las pruebas específicas de la guía y reportadas en el informe de auditoría como resultados de la examinación de la gestión de las TIC. A su vez, se emiten las recomendaciones específicas originadas en las oportunidades de mejora identificadas en el análisis de las evaluaciones desarrolladas.

En resumen, se puede indicar que la empresa cuenta con un nivel de madurez primario, con características de administrar la gestión bajo los procedimientos corporativos, pero que a su vez se dispersan con las actividades a nivel local conllevando a dejar grietas en el cumplimiento. Los niveles de receptividad de los hallazgos, criterios y validación de las métricas fueron elocuentes para el gobierno corporativo de la empresa, teniendo aceptación y emitiendo planes de acción para subsanar las debilidades de control evidenciadas. La organización debe enfocarse en lograr los planteamientos de mejora y buscar mantener un control de riesgos robusto para la administración de los sistemas de información.

ÍNDICE DE FIGURAS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE ABREVIATURAS

COBIT	Objetivos de Control para la Información y las Tecnologías relacionadas (Por su nombre en inglés Control Objective for Information and Related Technologies)
ISO/IEC	Organización Internacional de Normalización (Por su nombre en inglés International Organization for Standardization e International Electrotechnical Commission
ISACA	Asociación de Auditoría y Control de Sistemas de Información (por su nombre en inglés Information Systems Audit and Control Association
ERP	Sistemas de Planificación de Recursos empresariales (por sus siglas en inglés, Enterprise Resource Planning)
NT	Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)
PIB	Producto Interno Bruto
SGSI	Sistema de Gestión de Seguridad de Información
SI	Sistemas de Información
SAP	Sistemas, Aplicaciones y Productos para Procesamiento de Datos
SAP CC	SAP Competence Center – Centro de consultores regionales corporativos en
TI	Tecnologías de Información, conjunto de tecnologías dedicadas al manejo de información organizacional. Término genérico que incluye los recursos de: información, software, infraestructura y personas relacionadas
TIC	Tecnologías de Información y Comunicación

CAPÍTULO I: TEMA DE LA PRÁCTICA PROFESIONAL

1.1 Título

Propuesta de una herramienta aplicativa para la auditoría de la seguridad en sistemas y redes de comunicación del grupo Bekaert Costa Rica basado en* COBIT®5 *para Seguridad de la Información.

La idea central es conjuntar en una herramienta aplicativa la ejecución de la auditoría de seguridad en los sistemas de TIC en la empresa asignada para el desarrollo de la misma y elaborar las recomendaciones correspondientes a raíz de la evaluación de la guía aplicada basada el COBIT®5 *para Seguridad de la Información*.

1.2 Organización

La herramienta de auditoría será aplicada en las empresas Bekaert Costa Rica S.A. y BIA Alambres Costa Rica S.A., que conforman el Grupo Bekaert C.R., las cuales pertenecen a la transnacional Bekaert Corp., empresa de capital europeo, fundada desde 1880. Bekaert es un líder en el mercado de la aplicación de tecnología mundial para la transformación de alambre de acero y recubrimientos. Bekaert es una compañía global con sede en Bélgica, que emplean a 27 000 personas en todo el mundo, sirviendo a clientes en 120 países. Tiene sedes en Europa, Medio Oriente, Asia Pacifico, Norteamérica y Suramérica.

Bekaert consolida su aprovisionamiento de servicios de TI en línea con la expansión global del grupo con un número limitado de socios globales. Esta práctica de *outsourcing* de TI se aplica para servicios de aplicaciones, infraestructura y comunicación. Tal enfoque de asociación mundial fomenta mejor en conocimientos técnicos de mercado, las oportunidades de la normalización y de la gestión de costos de TI.

Bekaert asume la responsabilidad de su arquitectura empresarial de TI y la organización de las operaciones del Grupo de TI, así como la Gestión de Infraestructura y Comunicación. El *IT Group* asume la responsabilidad de la infraestructura y valida sus planes de acción con los administradores de TI de cada Unidad de Negocio. En cuanto a la gestión de aplicaciones, las unidades de negocios son responsables de identificar los requisitos de aplicación y el inicio del proyecto / coordinación; el *Grupo SAP Competence Center* dirige

la prestación de servicios y fomenta soluciones de aplicación alineados. El área de las tecnologías de Información para Costa Rica es administrada por el grupo de consultores en IT desde la Unidad de Negocio de SAP CC con sede en Ecuador. La persona que fungirá como supervisor laboral es el Lic. Sergio Briceño Hernández, MBA, Director Administrativo Financiero del grupo local. Además, el Ing. Iván Echeverría quien es Gerente Regional de TI para Latinoamérica (ubicado en Ecuador), y el Ing. David Castro quien es el Coordinador Local de TI, estos dos últimos dando apoyo profesional sobre el conocimiento de la gestión de TI en la empresa.

1.3 Objetivos

1.3.1 Objetivo General

Desarrollar una herramienta para determinar el grado de cumplimiento del marco normativo y de mejores prácticas que le resulta aplicable a las empresas del Grupo Bekaert Costa Rica en materia de seguridad de las tecnologías de información. La cual sea funcional para elaborar el diagnostico actual y aplicable en futuras ocasiones.

1.3.2 Objetivos específicos

I. Objetivo específico No. 1

Describir el contexto, conceptos y terminología relativos al ámbito de la seguridad, tanto física como lógica, de las redes y sistemas de comunicación de manera que se pueda lograr un mejor entendimiento sobre el tema de auditoría de seguridad de las TIC.

II. Objetivo específico No. 2

Diseñar una herramienta, a ser aplicada en la Empresa, que permita medir el cumplimiento de estándares y mejores prácticas en materia de seguridad de Sistemas de Información.

III. Objetivo específico No. 3

Diagnosticar la situación de la empresa Bekaert C.R. en cuanto a su nivel de seguridad y cumplimiento con la ejecución de la herramienta en el entorno y los procesos operativos de las redes de comunicación y los sistemas informáticos actuales, para poder obtener pruebas que sustenten el informe a la administración.

IV. Objetivo específico No. 4

Proponer las recomendaciones pertinentes, con referencia a las conclusiones obtenidas posterior al diagnóstico desarrollado, en pro de coadyuvar a la administración a fortalecer su sistema de control en cuanto a seguridad de las TIC.

1.4 Introducción

1.4.1 Justificación

Durante los últimos años las compañías se han enfrentado a cambios vertiginosos de la tecnología, según los servicios que brindan o productos que elaboren, por ejemplo las empresas transnacionales ubicadas en el mercado costarricense del sector industrial. Las organizaciones se han tenido que acoplar rápidamente a la tecnología global siguiendo la carrera de la innovación tecnológica, condicionadas muchas veces por los contratos de servicios locales y por la calidad recibida por parte del proveedor de servicio de redes e interconexiones.

La atracción de nuevas inversiones por parte del Gobierno de la República con el fin de reducir la tasa de desempleo y mejorar los índices económicos, como es el PIB per cápita, promoviendo la capacidad tecnológica del país y el nivel académico de la población, hacen que inversionistas vean con buenos ojos colocar sus inversiones en nuestro país, lo que deriva en beneficios a los objetivos e intereses del gobierno en atracción de empresas multinacionales.

La ubicación de este tipo de empresas en el mercado costarricense obliga a la provisión de servicios de interconexión robustos, que soporten la capacidad en conectividad y estabilidad a las organizaciones. A su vez, los niveles de seguridad se tornan en un aspecto muy relevante a examinar para las administraciones de las empresas, lo que conduce a mantener evaluación constante del cumplimiento de la normativa y buenas prácticas en la materia.

La empresa Bekaert Corp., es un claro ejemplo de lo descrito. Una compañía trasnacional atraída por los beneficios gubernamentales, por los índices macroeconómicos y por el nivel de desarrollo local ante la región para establecer negocios en el país. Estas compañías requieren infraestructura de redes y sistemas de comunicación para el desarrollo de las actividades y la gestión de los negocios día con día. Estas actividades conllevan atracción a riesgos propios que van contra la seguridad de la información; para la mitigación de los mismos es recomendado la aplicación de la observancia a las regulaciones y bases de control en la sección de seguridad de las TIC implementadas para contrarrestar estos riesgos.

Las buenas prácticas deben ser aplicadas para todas las empresas u organizaciones sin importar el tamaño y magnitud del gobierno corporativo, el seguimiento a los estándares globales son de gran importancia para la administración del negocio, se debe lograr el desarrollo del plan de gobierno de la seguridad y poder respaldar en este aspecto su continuidad, manteniendo el control de la seguridad como un elemento primordial para la gestión.

1.4.2 Finalidad

Este trabajo tiene como fin desarrollar la guía de auditoría y gestionar la aplicación de esta guía como una herramienta de control sobre la seguridad de los sistemas de información y comunicaciones de la empresa Bekaert Corp., que les permita a la administración de la entidad, de una forma rutinaria o programada, ejecutar pruebas de cumplimiento sobre la gestión de la seguridad en el uso de las tecnologías de información en el entorno local y su interacción a nivel global.

1.4.3 Intereses profesionales

La elaboración de este trabajo final de graduación, con una metodología de práctica profesional dirigida, nos estimula en el desarrollo como profesionales propiamente en el campo de la auditoría de TI y especialmente en materia de seguridad de la información. El cual conlleva un gran valor agregado para el caso de los profesionales en auditoría que no cuentan con la asignación de tareas específicas relacionas con el cumplimiento de la normativa o mejores prácticas en el área de seguridad de las TIC con cierta regularidad.

La importancia de este tema radica principalmente en la capacidad de aplicar conocimientos relacionados con la seguridad física y lógica de las TIC, la cual constituye un foco de control vital para el desempeño de las empresas en todo el orbe mundial.

En lo personal, este desarrollo del proyecto de posgrado me generaría apertura dentro del área de Sistemas de Información y por ende me crear un valor adicional a mis conocimientos prácticos del tema y sobre todo a mis funciones de control interno dentro de la organización.

1.5 Alcance

El proyecto a realizar en Bekaert busca apoyar la gestión para la toma de decisiones con respecto a la seguridad de los sistemas de información y comunicaciones mediante la herramienta de evaluación confeccionada. En colaboración para lograr el acometido anterior, se contará con el respaldo de la Dirección General y los Consultores regionales para Latinoamérica, así como de miembros claves de su organización.

La administración de la empresa busca obtener con este proyecto una herramienta para evaluar el cumplimiento del control de la seguridad de los sistemas de información y tecnologías de comunicaciones, que les permita identificar desviaciones a la norma o tener una pauta para determinar riesgos de control.

La investigación se limita a diseñar una herramienta de evaluación de los controles de seguridad física y lógica de las TIC, se basó en la guía práctica de COBIT 5 para la

Seguridad de la Información por medio de la cual se elaboraron las pruebas de control en el Grupo Bekaert Costa Rica. Seguidamente se hace entrega a la organización para la implementación continua y la ejecución rutinaria la cual estará a cargo de la administración local.

A su vez, se producirá un informe de auditoría basado en la determinación de hallazgos basados en el examen realizado para las instalaciones en Costa Rica seguidamente se enlistaran las conclusiones y recomendaciones con relación al trabajo de examen de auditoría ejecutado. La administración será la responsable de ejecutar las recomendaciones definidas en la aplicación de la evaluación mediante la herramienta a diseñada así como darle el seguimiento y monitorio de las actividades requeridas para mitigar los riesgos.

1.6 Metodología

En esta práctica profesional se empleó una metodología basada en la investigación documental en primera instancia, soportada en fuentes de carácter documental, como lo son las leyes, reglamentos, libros y tesis de grado y pos grado. En esta primera etapa se procedió con las actividades de recolección de datos, síntesis, organización y comprensión de la información relacionada principalmente con la normativa de gestión de la seguridad de las TIC, tales como manuales, directrices, reglamentos, circulares y estándares internacionales, los cuales se procesarán y analizarán para establecer los criterios para la guía de la auditoría.

El modelo de esta guía propuesta está diseñada bajo la metodología de los estándares internacionales y mejores prácticas, fundamentalmente en las normas internacionales de Auditoría, COBIT, ISO/IEC 27001 y ISO/IEC 27002, entre algunas otras normas para la gestión de la seguridad de la información.

Es imprescindible lograr un entendimiento claro de la organización y los procesos que se realizan en ella con el fin de diseñar la guía de auditoría, se efectuó la investigación “descriptiva” y “analítica”, de manera que pueda brindarse un bosquejo de la estructura organizativa de la empresa, de los elementos que condicionan su interrelación con el entorno en que se desenvuelve. Para lo cual se procedió con técnicas de entrevista como

instrumento base para la recolección de información, así como la observación y las encuestas, adquiriendo información obtenida de fuente primaria.

Lo anterior permite que el auditor mediante la interacción social consiga datos relevantes con mayor información y mejor estructurada al compararla con la obtención por otros métodos.

Luego de haber obtenido la información recopilada mediante la entrevista se utilizaron los métodos de "análisis", "síntesis" y "deductivo" con la finalidad de identificar cada una de las partes que influyen en la realidad observada y llegar a un criterio comparativo sobre los elementos encontrados y los existentes en un marco de referencia óptimo, con el fin de identificar desviaciones al mismo.

Para culminar con la generación del modelo propuesto la etapa final se hizo del tipo propositiva, mediante la cual se aporta a la empresa una alternativa de guía de auditoría sustentado en un modelo vinculante con la operación y la gestión del negocio para el control de la seguridad de la información.

1.7 Marco Teórico: Ubicación del tema en el contexto

El siguiente apartado hace referencia tácita de las principales definiciones con respecto al tema del proyecto en desarrollo, basadas en los Objetivos de Control para la Información y las Tecnologías relacionadas denominado COBIT (Por su nombre en inglés *Control Objective for Information and Related Technologies*), establecido como un marco de buenas prácticas aceptado internacionalmente para el control de la información en las TI y sus riesgos, y en la serie de normas ISO/IEC 27000 creadas por la Organización Internacional de Normalización ISO/IEC (por su nombre en inglés *International Organization for Standardization y la International Electrotechnical Commission*), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, ya sea grande o pequeña.

1.7.1 Definiciones

Respecto a la seguridad de las tecnologías de información, hay una gran variedad de definiciones, desde seguridad informática, de sistemas de información, seguridad física y lógica, seguridad de redes, seguridad base de datos, entre otras, por lo que a continuación se hace un pequeño extracto de algunas definiciones propuestas por algunos autores.

En relación con una aclaración en general, se define la seguridad de un mecanismo o proceso como aquella que asegura algún buen funcionamiento, precaviendo que éste falle, se frustre o se violente[1].

La información es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje[2]. La información es utilizada cotidianamente, normalmente para las actividades diarias, las operaciones del trabajo, para cumplir con las funciones y responsabilidades; así bien, el uso de la información tiene alto grado de relevancia ya que su uso indebido puede conllevar aspectos negativos para los individuos u organizaciones. La información por sí misma tiene estructura que modificará las sucesivas interacciones del ente que posee dicha información con su entorno.

El estándar Internacional ISO/IEC 27002:2005, define la seguridad de la información como "preservación de confidencialidad, integración y disponibilidad de la información; además también puede involucrar otras propiedades como autenticidad, responsabilidad, no-repudiación y confiabilidad[3].

La ISACA (por su nombre en inglés *Information Systems Audit and Control Association*) define Seguridad de la Información como algo que asegura que dentro de la empresa, la información está protegida contra la divulgación a los usuarios no autorizados (Confidencialidad), la modificación indebida (Integridad) y el no acceso cuando sea necesario (Disponibilidad).

---

[1] http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3LEMA=seguridad, recuperado el 09 de diciembre de 2014.
[2] http://es.wikipedia.org/wiki/Informaci%C3%B3n, recuperado el 09 de diciembre de 2014.
[3] International Organization for Standardization. ISO/IEC 27002:2005. Information technology – Security techniques – Code of practice for information security management. USA (Apartado 2.5).

• **Confidencialidad:** significa preservar las restricciones autorizadas en materia de acceso a la información y su divulgación, incluidos los medios para la protección de la privacidad y la propiedad de la información.

• **Integridad:** significa protección contra la incorrecta modificación o destrucción de información, y comprende la garantía de no repudio y autenticidad de la información.

• **Disponibilidad:** significa garantizar el acceso oportuno y confiable, y el uso de información.[4]

Similarmente, Tupia (2010) conceptualiza la información como "el conjunto de ideas que aportan el significado de hechos o conceptos y que pueden manifestarse a través del lenguaje hablado o escrito o por medio del empleo de símbolos y códigos[5]. Así mismo, denota que existen algunas características de la información relacionadas con la seguridad, tales como la integridad, confidencialidad, disponibilidad, autenticidad, no repudio, y la auditabilidad; las cuales las define como a continuación se describe:

Integridad: La información debe estar protegida contra modificaciones no autorizadas. La integridad es la garantía de que los datos sean correctos y de la completitud de la información.

Confidencialidad: Consiste en que la información sea apreciada, manipulada o difundida por aquellas personas que tengan derecho a conocerla. Es garantía de que la información llegue a las personas autorizadas.

Disponibilidad: Esta característica se refiere a que la información se puede utilizar cuando se la necesite. Garantía de que los servicios ofrecidos por el negocio, puedan operar y ser usados cuando sea preciso. Actualmente se está considerando como pate de la disponibilidad, la rapidez con que se pueden ofrecer servicios o realizar transacciones, dado que el costo de oportunidad es fundamental en la teoría de negocios moderna.

Autenticidad y no repudio: Está referido a las operaciones de negocios y los intercambios de información, entre distintas ubicaciones. Se entiende como la garantía de que, quien se hace responsable por una información, transacción o presentación de servicios ante una contraparte, sea quien dice ser. El concepto de no repudio por su parte, es la aceptación de la transacción realizada.

[4] *http://www.isaca.org/Pages/Glossary.aspx?tid=1486&char=I recuperado el 30 de noviembre del 2014.*
[5] Tupia, M. (2010). Administración de la Seguridad de la Información. Lima: GRAFICAR. (pág. 19).

Auditabilidad: Garantía de que en todo momento es posible identificar el origen (autor) de la transacción/operación, la fecha de realización y los medios empleados para la misma[6].

De la misma forma, Tupia (2010) establece la definición de seguridad como "la ausencia de riesgos en determinados entornos, sean éstos humanos o empresariales" y seguridad de la información como "el conjunto de procesos y actividades que permiten mantener libre de peligros y daños por accidentes o ataques a los activos de información que formen parte de una organización"[7].

ISACA nos indica que la Seguridad de la Información es un habilitador de negocios que está estrictamente ligado a la confianza de las partes interesadas, ya sea por el tratamiento del riesgo de negocio o por la creación de valor para la empresa, como ventaja competitiva.

En momentos en que la importancia de la información y las tecnologías relacionadas está aumentando en todos los aspectos de los negocios y la vida pública, la necesidad de mitigar los riesgos de la información, en los cuales se incluye tanto la protección de la información como de los activos de TI relacionados. Las amenazas permanecen en constante cambio, por ende el control de la seguridad de la información debe seguir el mismo camino, estando muy atentos al entorno y al análisis de riesgos que se pueda enfrentar la organización.

El tener presente las actualizaciones en cuanto a normativa y regulación, así como el estudio de las mejoras prácticas de los SGSI dentro del panorama empresarial se suma a la conciencia de la junta directiva de la criticidad de los controles de seguridad de la información que se ameritan tanto para la información y como para los activos relacionados con las TIC.

Por otro lado ISO nos muestra que la información es un recurso que, como el resto de los activos, tiene valor para una organización y por consiguiente debe ser debidamente protegida. La seguridad de la información protege ésta de una amplia gama de amenazas, a

[6] Tupia M. (2010). Op. Cit. (pág. 20).
[7] Tupia M. (2010). Op. Cit. (pág. 21).

fin de garantizar la continuidad del negocio, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades.

Posteriormente, Muñoz (2002) puntualiza los siguientes conceptos concernientes con la seguridad, los cuales son trascendentales tener en conocimiento claro de sus significados con el fin de comprender la temática del proceso de auditoría de las tecnologías de información y comunicaciones para el control de la seguridad:

Seguridad física

Se refiere a todos los aspectos correspondientes con la seguridad y salvaguarda de los bienes tangible de los sistemas computacionales de las empresas, tales como el hardware central, los equipos periféricos y equipos asociados, las instalaciones eléctricas, las instalaciones de comunicación y de datos, las construcciones, el mobiliario y equipo de oficina, así como la protección a los accesos al centro de comando o sistematización. Por consiguiente, es todo lo referido con la conservación de equipos, la prevención de riesgo y protección de los recursos físicos informáticos de la empresa.

Seguridad lógica

Es lo relativo con la seguridad de los bienes intangibles de los centros informáticos, tales como software (programas, aplicaciones, sistemas operativos y lenguajes), así como lo concerniente con las metodologías y procedimientos de operación, los niveles de acceso a los sistemas y programas institucionales, el uso de las contraseñas, los privilegios y restricciones de los usuarios, la protección de los archivos e información de la empresa y las medidas y programas para prevenir y erradicar cualquier virus informático. En sí, todo lo concerniente con las medidas de seguridad, protección y tipos de accesos a los datos e información del sistema.

Seguridad de las bases de datos

Es la protección específica de la información que se maneja, resguarda y protege en las áreas de sistemas de la empresa, ya sea a través de las medidas de seguridad y control que limiten el acceso y uso de esa información, o mediante sus respaldos periódicos con el fin de mantener su confidencialidad y prevenir las alteraciones, descuido, robos y otros actos delictivos que afecten su consistencia.

Seguridad en la operación

Se refiere a la seguridad en la operación de los sistemas computacionales en cuanto a su acceso y aprovechamiento por parte del personal informático y de los usuarios, al acceso a la información y los programas institucionales, a la forma de proteger la operación de los equipos, los archivos y programas, así como las instalaciones, mobiliario, etcétera.

Seguridad del personal de informática

Se refiere a la seguridad y protección de los operadores, analistas, programadores y demás personal que está en contacto directo con el sistema, así como a la seguridad de los beneficiarios de la información.

Seguridad de las telecomunicaciones

Es todo lo relacionado con la seguridad y protección de los niveles de acceso, privilegios, recepción y envío de información por medio del sistema de cómputo, protocolos, software, equipos e instalaciones que permiten la comunicación y transmisión de la información en la empresa, etcétera.

Seguridad en las redes

Es todo lo relacionado con la seguridad y control de contingencias para la protección adecuada de los sistemas de redes de cómputo, en cuanto a las salvaguardas de información y datos de las redes, la seguridad en el acceso a los sistemas computacionales, a la información y a los programas del sistema, así como la protección de accesos físicos, del mobiliario, del equipo y de los usuarios de los sistemas, incluyendo el respaldo de la información y los privilegios de accesos a sistemas, información y programas[8].

1.7.2 Normas ISO/IEC

Las normas ISO y sus principios de gestión, son marcos de estandarización que se regulan por la *International Organization for Standardization y por la International Electrotechnical Commission (ISO/IEC)*. ISO es una federación mundial de organismos nacionales de normalización alrededor de 160 países, trabajan a nivel de Comités Técnicos, tienen al menos 19,000 estándares publicados desde 1947 (creación), 1951 (publicación).

[8] Muñoz C. (2002). Auditoría en Sistemas Computacionales. México D.F. Pearson Prentice Hall. (pág. 164 y 165).

Trabaja en función a 8 principios de gestión:
1. Orientación al cliente.
2. Liderazgo.
3. Participación del personal.
4. Enfoque de procesos.
5. Enfoque de sistemas de gestión.
6. Mejora Continua.
7. Enfoque de mejora contínua.
8. Relación mutuamente beneficiosa con el proveedor.

Los estándares ISO son aplicables a cualquier tipo y tamaño de empresa u organización.

Respecto a la seguridad de la información hay toda una familia de estándares creados por la ISO/IEC, correspondientes a la serie de normas ISO 27000, tal como se detalla a continuación:

ISO	Descripción de la norma
ISO/IEC 27001:2013	Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un SGSI, según el "Ciclo de Deming", Planificar, Hacer, Verificar, Actuar. (PDCA por su nombre en inglés Plan, Do, Check, Act).
ISO/IEC 27002:2013	Proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a los interesados y responsables en iniciar, implantar o mantener SGSI.
ISO/IEC 27003:2010	Se centra en los aspectos críticos necesarios para el éxito del diseño e implementación de un SGSI.
ISO/IEC 27004:2009	Concreta cómo configurar el programa de medición, qué parámetros medir, cuándo y cómo medirlos, ayuda a las empresas a crear objetivos de rendimiento y criterios de éxito.
ISO/IEC 27005:2011	Se ocupa de la gestión de riesgos de seguridad de información. Suministra las directrices, apoyando particularmente los requisitos del SGSI.
ISO/IEC 27006:2011	Corresponde a una guía para los organismos de certificación en los procesos formales que hay que seguir al auditar SGSI.
ISO/IEC 27007:2011	Suministra una guía para las entidades acreditadas de certificación para auditar SGSI.
ISO/IEC 27008:2011	Suministra orientación acerca de la implementación y operación de los controles de SI, es aplicable a cualquier tipo y tamaño de empresa, tanto pública como privada.
ISO/IEC 27010:2012	Suministra orientación relacionada con el intercambio de información relativa a los riesgos de SI, controles, problemas e incidencias que puedan ocurrir en las organizaciones.
ISO/IEC 27013:2012	Proporciona directrices sobre la aplicación integrada de las normas ISO/IEC 27001 e ISO/IEC 20000.

1.7.3 COBIT

Es un marco de gobierno de las tecnologías de información que proporciona una serie de herramientas para que la gerencia pueda conectar los requerimientos de control con los aspectos técnicos y los riesgos del negocio. COBIT permite el desarrollo de las políticas y buenas prácticas para el control de las tecnologías en toda la organización, enfatiza el cumplimiento regulatorio, ayuda a las organizaciones a incrementar su valor a través de las tecnologías, y permite su alineamiento con los objetivos del negocio.

COBIT 5 es producto de la mejora estratégica de ISACA la cual impulsan la próxima generación de guías sobre el Gobierno y la Administración de la información y los Activos Tecnológicos de las Organizaciones.

Construido sobre más de 15 años de aplicación práctica, ISACA desarrolló COBIT 5 para cubrir las necesidades de los interesados, y alinearse a las actuales tendencias sobre técnicas de gobierno y administración relacionadas con la TI, integrando los anteriores marcos referenciales de ISACA, tales como:

Val IT: es un marco de referencia de gobierno que incluye principios rectores generalmente aceptados y procesos de soporte relativos a la evaluación y selección de inversiones de negocios de TI.

Risk IT: es un marco de referencia normativo basado en un conjunto de principios rectores para una gestión efectiva de riesgos de TI.

BMIS (Business Model for Information Security): una aproximación holística y orientada al negocio para la administración de la seguridad informática.

ITAF (IT Assurance Framework): un marco para el diseño, la ejecución y reporte de auditorías de TI y de tareas de evaluación de cumplimiento. [9]

[9] www.segurinfo.org. Prandini, P. y Szuster, R. Re-Evolucion COBIT5. Recuperado de www.isaca.org/Knowledge-Center/cobit/Documents/COBIT5-and-InfoSec-Spanish.ppt

COBIT 5 se caracteriza por basarse en el modelo relacional que emplea BMIS (por su nombre en inglés Business Model for Information Security), el cual conjunta la visión integral del mismo patrón y sus elementos a la versión más reciente. Demuestra un enfoque integral y encauzado al negocio para el proceso de los SGSI. Propuesto con un lenguaje sencillo para referirse al resguardo de la información, hace frente a la visión convencional de la inversión en seguridad de la información y manifiesta en forma puntualizada el modelo de negocio para gestionar la seguridad de la información, estimulando a aplicar una configuración holista.

COBIT@5 para seguridad de la información

Se proyecta como una guía específica para los profesionales de la Seguridad de la Información y otros interesados. Se construye sobre el marco del COBIT 5, un enfoque robusto para el gobierno y la gestión de la seguridad de la información, sobre la base de los procesos de negocios de la organización.

Mediante esta guía profesional se presentará una visión extendida del COBIT 5, que explica cada uno de sus componentes desde la perspectiva de la seguridad. Creará valor para todos los interesados a través de explicaciones, actividades, procesos y recomendaciones, así mismo propondrá una visión del gobierno y la gestión de la seguridad de la información mediante una guía detallada para establecerla, implementarla y mantenerla, como parte de las políticas, procesos y estructuras de la organización.

Principales contenidos:

- Directrices sobre los principales conductores y beneficios de la SI para la organización.
- Aplicación de los principios de COBIT 5 por parte de los profesionales de la seguridad de la información.
- Mecanismos e instrumentos para respaldar el gobierno y la gestión de la seguridad de la información en la organización.
- Alineamiento con otros estándares de seguridad de la información.

En COBIT@5 *para seguridad de la información* se limita a la vista de la seguridad de este término y se basa en esta definición para describir la forma en que la seguridad de la información se puede aplicar en la vida real, teniendo en cuenta los principios de COBIT 5. Los principios de seguridad de la información comunican las reglas de la empresa que soportan los objetivos de gobierno y los valores empresariales, según la definición del Consejo y la dirección ejecutiva. Estos principios deben ser limitados en cuanto a su número, y estar expresados en un lenguaje sencillo y declarar, de la manera más clara posible, los valores fundamentales de la empresa.[10]

Dentro de los procesos de COBIT5 a ser utilizados como base para formar parte de los criterios de evaluación en la guía de auditoría, y que se contemplarán en la herramienta propuesta para ser aplicada serán los relacionados al control de la seguridad de las TIC, los cuales se detallan a continuación:

APO13 Gestionar la Seguridad

Definir, operar y supervisar un sistema para la gestión de la seguridad de la información; con el fin de mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.

DSS04 Gestionar los Servicios de Seguridad

Establecer y conservar un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios de TI requeridos, y a su vez mantener la disponibilidad de la información a un nivel aceptable para la empresa. Continuar las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa ante el evento de una interrupción significativa.

MEA01 Supervisa Evaluar y Valorar Rendimiento y Conformidad

Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada.

[10] ISACA. COBIT 5 for Information Security. (2012)

Con miras a poder proporcionar transparencia de rendimiento y conformidad y conducción hacia la obtención de los objetivos.

MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno

Supervisar y evaluar de forma continua el entorno de control, incluyendo tanto autoevaluaciones como revisiones externas independientes. Facilitar a la dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Es imperativo que se tenga que planificar, organizar y mantener normas para la evaluación del control interno y las actividades de aseguramiento. Con el fin de poder ofrecer transparencia a las partes interesadas claves respecto de la adecuación del sistema de control interno para generar confianza en las operaciones, en el logro de los objetivos de la compañía y un entendimiento adecuado del riesgo residual.

MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos

Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de TI en el cumplimiento de la empresa general. Lo anterior de tal forma que se pueda asegurar que la empresa cumple con todos los requisitos externos que le sean aplicables. (ISACA, 2012)[11].

Así denotando los principales conceptos enunciados en los marcos de referencia sobre las buenas prácticas en la gestión de la seguridad de la información facilita al lector a comprender los objetivos trazados para este proyecto y comprender la contextualización de los mismos en el enfoque del control de los recursos y en específico sobre los datos que respaldan la información de la organización en cuestión.

[11] ISACA. COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. (2012)

1.8 Entorno organizacional

Bekaert es un líder del mercado y de la tecnología mundial en la transformación de alambre de acero y recubrimientos. Fue establecida en 1880 en Bélgica, actualmente es una compañía global con aproximadamente 30.000 empleados en todo el mundo. Para ser el proveedor preferido de productos de alambre de acero y soluciones, constantemente entrega valor superior a sus clientes alrededor de todo el mundo, con transacciones en más de 120 países y en todos los mercados y sectores industriales bajo la filosofía de "mejor juntos". La empresa Bekaert cotiza sus acciones en la bolsa Euronext® Bruselas (BEKB).

La empresa cuenta entre su plan estratégico de negocio con la misión, visión y principios corporativos que se van enunciar seguidamente:

Misión Corporativa:

"Un Gran Equipo Bekaert con la pasión para ganar, entregando las mejores soluciones con valor agregado para nuestros clientes de la manera más rentable, y a través de esto, crear valor para nuestro negocio".

Visión Corporativa:

"Consistentes con nuestra aspiración *mejor juntos*, perseguimos implacablemente el ser los proveedores preferidos de nuestros productos y soluciones en alambre de acero, ofreciendo permanentemente un valor superior a nuestros clientes alrededor del mundo".

Principios Corporativos:

Como base de su estrategia organizativa, la empresa desarrolla sus 5 principios base para cada funcionario dentro de la organización, tales son:

1) Pasión por la excelencia
2) Orientación hacia adentro desde afuera
3) Innovación ágil
4) Todos son Líder Bekaert
5) Una sola Bekaert

Además, se tienen desarrollados las políticas y principios en el área de Tecnologías de Información a nivel global. Las cuales se analizaran en el siguiente capítulo en cuanto a la comprensión de la empresa en cuanto a sus actividades y controles.

Organización del Grupo de TI Bekaert

A nivel de grupo el CIO es responsable de establecer las políticas de TI alineados con la estrategia de negocios corporativa.

El Grupo de Servicios de TI están dirigiendo la entrega de:

- Los servicios de infraestructura, comunicación e información de los trabajadores.
- Desarrollo de aplicaciones y mantenimiento (SAP centro de competencia)

Por su lado, cada Unidad de Negocio o Unidad funcional (BU / FU) tiene un Gerente de TI con personal responsable de la captura de requerimientos, coordinación e iniciación del proyecto, haciendo uso del centro de entrega. Además, cuentan con una sección de TI local y a su vez está disponible en unidades más grandes para soportar el uso diario de las herramientas informáticas.

Bekaert estrategia de TI: Principios

El gobierno corporativo quiere ser un adoptante de la corriente principal en la tecnología informática. Para ello se caracteriza por GUÍAr su estrategia bajo los siguientes principios:

- Seguidor, sólo implementamos soluciones probadas (herramientas de MS Office)
- Número limitado de software de permitido

Bekaert ha optado por un alto grado de externalización de desarrollo de software/aplicación e instalaciones de hardware, tanto de gestión y aplicación, para ello:

- Las unidades de negocio siguen siendo responsables de las aplicaciones.
- Grupo TI asume la responsabilidad de la infraestructura.

Bekaert impondrá una conducta adecuada en el uso de las TI significa toda la compañía:

- El cumplimiento de los procedimientos del Grupo
- Aplicaciones transparentes de TI deben facilitar un buen control de la gestión y presentación de informes.

CAPÍTULO II: PROPUESTA GUÍA DE AUDITORÍA

En el presente capítulo se desarrollará la propuesta de la guía de auditoría para evaluar la seguridad en sistemas y redes de comunicación de las empresas del grupo Bekaert Costa Rica, en el cual se compone básicamente del Plan General de Auditoría y los programas detallados y específicos para el desarrollo del examen de la auditoría.

Introducción

La Información se ha convertido en un recurso primordial para todas las compañías, partiendo desde el instante en que es creada hasta que sea destruida, las tecnologías de información y comunicación tienen una función importantísima dentro de los negocios. El avance de las TIC exponencialmente conforme pasa el tiempo, ha incursionado tanto en las empresas, como en los ámbitos sociales, públicos y de negocios. Esta guía estará basada en COBIT@5 *para Seguridad de la Información*, y será entrelazada con los principios de buenas prácticas para el control interno y seguridad de las tecnologías.

El marco que nos facilita COBIT 5 contiene un desarrollo integral de colaboración con las empresas para poder lograr sus objetivos para el gobierno y la gestión de las TI corporativas. En otras palabras da una ayuda a las empresas a conformar el valor óptimo desde las TIC salvaguardando la armonía que debe existir entre la producción de beneficios y mitigar los niveles de riesgo y el aprovechamiento de los recursos comúnmente escasos en las entidades o instituciones.

COBIT 5 permite que las TI se gobiernen y gestionen de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y a las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de los grupos de interés internos y externos (ISACA, 2012). [12]

[12] ISACA. COBIT 5 for Information Security. (2012)

2.1 Consideraciones para la elaboración del plan general de auditoría

2.1.1 Comprensión de las actividades de la empresa

Primeramente y antes de desarrollar el Plan General de Auditoría es necesario tener un conocimiento general de la entidad o unidad que se está auditando, por lo que a continuación se propone una guía de auditoría para obtener dicha información. La investigación preliminar debe incorporar fases de evaluación del control gerencial y el control de las aplicaciones. Durante la revisión de los controles gerenciales el auditor debe entender a la organización, las políticas y prácticas gerenciales usadas en cada nivel.

GUÍA DE AUDITORÍA **Comprensión de las actividades de la entidad**				**GA-1**
Objetivo: Obtener una mayor comprensión de las actividades de la entidad auditada mediante APO02.02 Conocer el entorno, capacidades y rendimiento actuales para revisión preliminar.				
Procedimiento: Aplicar los siguientes procedimientos.				
N.	**Procedimiento**	**Ref. P/T**	**Hecho por**	**Fecha**
1.	Realice un estudio preliminar de la dependencia o unidad por auditar, mediante el análisis de la cantidad suficiente de antecedentes e información que pueda recabarse, considerando como mínimo lo siguiente:			
	Resultados de auditorías anteriores u otros estudios relacionados con los objetivos de la auditoría por realizar, identificando las acciones correctivas que se tomaron para atender los hallazgos significativos y las recomendaciones.			
	Estructura orgánica			
	Manuales de puestos			
	Manuales de procedimientos			
	Funciones y responsabilidades asignadas			
	Misión, visión, objetivos corporativos			
	Marco jurídico aplicable			
	Plan Operativo Anual			
	Presupuesto autorizado			
	Estándares o indicadores de gestión que utiliza			
	Movimientos de personal y rotación			
	Cambios en los sistemas de información			
Elaborado por:		Revisado por:		
Fecha:		Fecha:		

2.1.2 Comprensión del sistema de control interno de la empresa

El auditor necesita comprender el sistema de control interno, para ello se propone la siguiente guía de auditoría para evaluar el control interno organizacional y cuestionario de control interno para ser aplicado a una muestra de funcionarios, con el fin de conocer su perspectiva sobre la gestión de la seguridad de la información.

GUÍA DE AUDITORÍA **Evaluación de control interno organizacional**				**GA-2**
Objetivo: Evaluar el control interno organizacional para generar confianza en las operaciones, en el logro de los objetivos de la compañía y un entendimiento adecuado del riesgo residual.				
Procedimiento: Aplicar los siguientes procedimientos.				
N.	**Procedimiento**	**Ref. P/T**	**Hecho por**	**Fecha**
1.	Confeccione un papel de trabajo con el fundamento en MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno, con las directrices, manuales y procedimientos emitidos mediante el estudio de los mismos.			
2.	Analice los resultados de auditorías anteriores u otros estudios que se hayan realizado del control de las TIC.			
3.	Estudie el instructivo o manual de implementación del marco de control basado en COBIT. MEA02.01 Supervisar el control interno para determinar cumplimiento del proceso ejecutado.			
4.	Determine si para la ejecución del proceso de control se cuenta con todos los recursos financieros, humanos, técnicos, materiales y demás necesarios para su establecimiento, operación, perfeccionamiento y evaluación necesarios.			
5.	Solicite y revise el cuestionario de la última autoevaluación de control interno y la matriz de identificación y análisis de riesgo. MEA02.02			
6.	Solicite y analice las acciones realizadas por la administración de acuerdo con los resultados de la autoevaluación de control interno y verifique su cumplimiento.			
7.	Solicite y analice los informes de seguimiento de la autoevaluación por MEA02.03 Realizar autoevaluación de control.			
8.	Aplique el Modelo de Madurez del Sistema de Control Interno empresarial según APO01.07			
Elaborado por:		Revisado por:		
Fecha:		Fecha:		

2.1.3 Resultados de la autoevaluación de ese sistema

Es imperativo el conocer la gestión que se desarrolla en la entidad para el área de seguridad entre la organización, el auditor debe tomar en cuenta las consideraciones de los funcionarios y las perspectivas que se pueden obtener directamente de ellos.

Mediante esta herramienta se puede revisar de primera mano la gestión de seguridad por parte del gobierno corporativo y las guías que puedan existir para el desarrollo de las tareas y el entorno cotidiano donde se desenvuelven las actividades del negocio.

Así por medio de esta autoevaluación, el auditor tiene información precisa y veraz sobre la administración del riesgo y los servicios de seguridad que gestiona la empresa en sus funciones de dirección sobre el gobierno y las políticas en el área de las TIC.

GUÍA DE AUDITORÍA **Cuestionario de evaluación de la gestión de la seguridad de la información**				**GA-3**
Objetivo: Evaluar desde la perspectiva de los funcionarios el nivel de cumplimiento de la gestión de la seguridad por parte de la administración mediante DSS05 Gestionar Servicios de Seguridad				
Procedimiento: Tabular los resultados obtenidos y preparar un análisis estadístico.				
N.	**Pregunta**	**Sí**	**No**	**Desconoce**
1.	¿Cuántos años tiene de laborar para la empresa?			
2.	¿Se siente satisfecho (a) de laborar para la empresa?			
3.	¿Conoce la misión, visión y objetivos corporativos?			
4.	¿Se le ha informado por parte de la administración sobre la política de seguridad de la empresa?			
5.	Ha recibido alguna capacitación en seguridad de la información? ¿Hace cuándo fue recibida? ( ) Un mes ( ) Seis meses ( ) Un año ( ) Tres años o más			
6.	¿Se le ha informado cuáles son sus responsabilidades y los riesgos asociados a las tecnologías de la información?			
7.	¿Tiene claras las responsabilidades respecto a su función?			
8.	¿Conoce las implicaciones penales por robo y fraude de la información?			
9.	¿Tiene conocimiento de qué es un acuerdo de confidencialidad?			

10.	¿Ha firmado algún acuerdo de confidencialidad?			
11.	¿Conoce empleados que hayan firmado algún acuerdo de confidencialidad?			
12.	¿La empresa ha establecido y difundido una política de puertas abiertas?			
13.	¿Existen mecanismos para que los niveles inferiores puedan presentar propuestas o sugerencias?			
14.	¿Perciben que las propuestas o sugerencias son analizadas en los niveles correspondientes?			
15.	¿Las instalaciones donde labora tienen una protección adecuada contra siniestros?			
16.	¿Considera que la ubicación física de los equipos de cómputo es la más adecuada?			
17.	¿Considera que existen procedimientos para asegurar la confidencialidad de la información crítica o calificada de la empresa?			
18.	¿Sabe dónde están los extintores de fuego?			
19.	¿Tiene conocimiento de cómo utilizar un extintor?			
20.	¿Ha recibido alguna capacitación para utilizar un extintor?			
21.	¿Conoce dónde están las salidas de emergencia? Las ha utilizado?			
22.	¿En alguna ocasión se ha generado algún corto circuito dentro de las instalaciones?			
23.	¿Conoce las responsabilidades y funciones ante las pruebas de continuidad de los servicios de TI?			
24.	¿En alguna ocasión se ha extraviado alguna laptop o equipo propiedad de algún empleado de la empresa?			
25.	¿En alguna ocasión se ha extraviado algún periférico (bocinas, audífonos, teclado, mouse, teclado numérico, etc.) de una computadora?			
26.	¿Cada componente de su computadora y periféricos tienen placa inventariada por la empresa?			
27.	¿Considera usted que hay demasiada humedad o exceso de calor que pueda deteriorar los equipos informáticos?			
28.	¿Conoce los peligros que provocan los virus, *malware*, troyanos, *fishing*, etc.?			
29.	¿Cambia regularmente sus claves confidenciales?			
30.	¿Cierra las sesiones activas cuando tiene que dejar el equipo desatendido?			
Elaborado por:		Supervisado por:		
Fecha:		Fecha:		

2.2 Diseño del plan general de la auditoría

Existen aspectos clave que deben indubitablemente ser tomados en cuenta al momento de confeccionar el Plan General de Auditoría, hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características del área dentro del organismo a auditar, sus sistemas, organización y equipo. También se debe considerar las herramientas necesarias, el tiempo y costo, así como definir los alcances de la auditoría.

El trabajo de auditoría deberá incluir la planeación de la auditoría, el examen o evaluación de la información, la comunicación de los resultados y el seguimiento.

2.2.1 Objetivos de la auditoría

El objetivo general propuesto del presente proyecto de auditoría de los sistemas de la seguridad de la Tecnología de la Información a desarrollarse es el siguiente:

> Diagnosticar la situación de la empresa Bekaert C.R. en cuanto a su nivel de seguridad y cumplimiento con la ejecución de la herramienta basada en COBIT$^{@}$5 *para la Seguridad de la Información*, en el entorno y los procesos operativos de las redes de comunicación y los sistemas informáticos actuales, para poder obtener evidencias que sustenten el informe a la administración.

2.2.2 Naturaleza, alcance, oportunidad y plazo de los procedimientos

El plan general de auditoría se debe establecer claramente cuál es la naturaleza del estudio a realizar, definir el alcance del proyecto de auditoría, así como la oportunidad de fiscalización correspondiente y a su vez se debe asentar un presupuesto del plazo en que se lleve a ejecución de los procedimientos a ser aplicados en el desarrollo del mismo, tal como se define seguidamente:

Naturaleza

La naturaleza del estudio está contemplada en una investigación documental sobre el tema de seguridad de la información, con el fin de ser aplicada de forma práctica. El desarrollo del proyecto se genera con una herramienta basada en COBIT5 como marco de referencia para ejecutar la evaluación cualitativa de los cumplimientos de la norma, el cual fue alineado dentro de los programas del plan de trabajo del Grupo Corporativo de Auditoría Interna de la entidad, en concordancia con el Grupo de Servicio de TI y las unidades de negocio regionales.

Alcance

EI alcance de la auditoría debe especificar las actividades concretas que van a ser auditadas, así como la normativa aplicable, el período de estudio y la extensión de la ejecución de la auditoría, así como las limitaciones que se determinen en el estudio.

El Grupo Bekaert Costa Rica, tiene recientemente cumplido el primer año de operar en nuestro territorio (mayo 2014 inició sus operaciones), el proyecto se limita a la evaluación de la seguridad de los sistemas de información en la unidad local instalada en este país, donde cuenta con 2 plantas de producción con oficinas administrativas en ambas locaciones dentro del Parque Industrial Condal, en la Ceiba de Orotina, Alajuela. Determinando deficiencias de control y emitiendo recomendaciones para contrarrestar las causas de los hallazgos.

Oportunidad

Las unidades de negocio de Costa Rica son de muy reciente operación, luego de haber ejecutado la implementación del software ERP (SAP R3), y puesto en marcha el negocio. Se tiene la cabida para verificar la gestión de seguridad de las TIC implantadas a nivel corporativo y la recepción que han tenido estas para los funcionarios de la empresa localmente.

Plazos de los procedimientos

De acuerdo con la vasta experiencia corporativa, el Grupo de Auditoría Interna debe avocarse hacia la tarea de considerar un plazo razonable y establecer cuándo es el momento oportuno para empezar con el desarrollo de la ejecución de la auditoría y el tiempo proyectado que se requiere para realizar los procedimientos establecidos mediante cronograma de actividades y seguimiento del mismo.

2.2.3 Elementos de coordinación, dirección, supervisión y revisión requeridos

La planeación de la auditoría de TI debe contener las acreditaciones de las responsabilidades de dirección y supervisión necesaria para llevar a cabo el programa diseñado para tales fines, así también se debe contemplar coordinación de la disponibilidad del equipo de auditores con el fin de estar alineados con el plan de auditoría y los programas globales de control interno.

Para estos efectos se debió coordinar el tiempo de aplicación de pruebas en situ, coordinar las tareas con el Coordinador de TI local, planear las actividades y agendarlos para poder hacer las revisiones del proyecto según el cronograma establecido y aprobado por las partes.

2.2.4 Recursos para el desarrollo del trabajo

El plan general de auditoría debe contemplar diversos recursos necesarios para el desarrollo de la auditoría, es imperativo considerar la disponibilidad del equipo de auditores como recurso humano con conocimientos y características que cumplan con el perfil profesional de un auditor de TI. Además de los materiales, como el equipo de cómputo requerido, por ejemplo podemos considerar entre ellos los computadores portátiles (laptops), equipos multifuncionales, escáner, impresora, cámara fotográfica o de video, otros dispositivos tecnológicos como "*tablets o smartphones*", así como otros suministros de oficina básicos.

Igualmente es preciso considerar la disponibilidad de los vehículos de transporte, principalmente se debe tomar en cuenta las ubicaciones de las instalaciones de la empresa,

distancias entre una planta y la otra, oficinas de ventas comerciales, oficinas administrativas y ubicación de entidades gubernamentales o servicios de terceros que puedan ser visitados por los auditores, también para efectos de realizar una gira y reservar los fondos para cubrir los viáticos de los auditores.

En específico, se requirió la programación de disponibilidad de los recursos indicados, máxime las ubicaciones físicas que se visitaron para la elaboración de las pruebas, como los son las oficinas de ventas en las instalaciones del Edificio Forum I en San Jose, y las oficinas administrativas en las plantas de producción ubicas en Orotina de Alajuela.

Importante el uso de los sistemas de comunicación, redes locales y documentación respaldada en medios magnéticos, equipo tecnológico tanto el propio como de la entidad.

2.2.5 Plan General de Auditoría

La planeación y supervisión por parte del auditor debe ser apropiada con el fin de que los resultados sirvan como base para sustentar su opinión y elaborar las recomendaciones pertinentes, con criterio y carácter profesional. En observancia de las Normas Internacionales de Auditoría (NIA 300), el trabajo debe ser técnicamente planeado y ejercerse una supervisión adecuada sobre los asistentes, con el efecto de ser garante de la calidad hacia los usuarios.

La planeación de la auditoría conduce al establecimiento de la extensión y el alcance de las pruebas a aplicar, y la supervisión sobre el equipo profesional de auditoría que le acompañará durante el desarrollo del plan de trabajo. Además la planeación le permite:

- Comprender la administración de la gestión de la empresa o unidad a ser examinada, y acentuar las dificultades que la aquejan.
- Conocer sus instalaciones físicas en las diferentes secciones o áreas.
- Entender el sistema de información computarizado y administrativo de la entidad.
- Fundamentar el estado de confianza que se espera tener en el control interno informático.
- Determinar y programar la naturaleza, la oportunidad de los procedimientos de Auditoría que se llevarán a cabo.

Seguidamente se desarrolla la propuesta de Plan General de Auditoría para este proyecto:

Plan General de Auditoría		PGA-1		
Objetivo:	Evaluar el cumplimiento de las políticas corporativas en cuanto a la Gestión de la seguridad de la información, por medio de la revisión y análisis de los lineamientos del COBIT@5 *para la Seguridad de la Información* y la normativa interna, con el fin de promover una mejora continua de la seguridad de las TIC.			
Naturaleza:	La naturaleza del estudio está contemplada dentro de los lineamientos del plan de trabajo de la Dirección de Auditoría Interna Global para el año 2015, así como el desempeño del Grupo de TI corporativo. Lo anterior en cumplimiento del procedimiento del Grupo de Control de Bekaert Corp.			
Alcance:	Bekaert Costa Rica 2015			
Plazo:	2 meses			
N.	**Procedimiento**	**Ref. P/T**	**Hecho por**	**Fecha**
1.	Obtenga o actualice la compresión de las actividades de la unidad auditada y la organización.	GA-1		
2.	Realice una evaluación de control interno y comprenda el Sistema de Control Interno de la empresa.	GA-2		
3.	Aplique un cuestionario a los funcionarios para evaluar el cumplimiento de la gestión de la seguridad de la información.	GA-3		
4.	Elabore una serie de procedimientos por cada una de las siguientes normas de la gestión de la seguridad de la información, en función del objetivo general y de la información obtenida en las actividades anteriores.			
	AP013 Implementación de un marco de seguridad de la información.	GA-4		
	DSS05.01 Proteger contra software malicioso	GA-5		
	DSS05.02 Gestionar la seguridad de la red y las conexiones	GA-6		
	DSS05.03 Gestionar la seguridad de los puestos de usuario finales	GA-7		
	DSS05.04 Gestionar la identidad del usuario y el acceso lógico	GA-8		
	DSS05.05 Gestionar el acceso físico a los activos de TI	GA-9		
	DSS05.06 Gestionar documentos sensibles y dispositivos de salida	GA-10		
	DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad	GA-11		
	DSS4 Gestionar la Continuidad de los servicios de TI.	GA-12		
5.	Elabore un papel de trabajo con los hallazgos y realice una presentación al equipo auditor.			
6.	Elabore el informe de auditoría, sométalo a revisión y discusión de los auditados.			
Elaborado por:		Supervisado por:		
Fecha:		Fecha:		

Diseño Guía de Auditoría

En COBIT 5, los procesos APO13 Gestionar la seguridad, DSS04 Gestionar la continuidad y DSS05 Gestionar los servicios de seguridad proporcionan una guía básica acerca de cómo definir, operar y dar seguimiento a un sistema para la gestión general de seguridad. De esta forma, en la guía detallada de ISACA se considera que la seguridad de la información está presente en cada sección de toda la empresa o entidad, con aspectos de seguridad de la información dentro de cada actividad y proceso realizado, bajo la adopción de esta nueva guía que data del 2012 para el gobierno y la gestión corporativa de la seguridad de la información.

Para cada uno de los procesos de la guía COBIT@5 *para la Seguridad de la Información* enunciados en el párrafo anterior se ha desarrollado un instrumento de auditoría que busca evaluar el grado de cumplimiento de la administración, tal como se detalla a continuación.

GUÍA DE AUDITORÍA **Implementación de un marco de seguridad de la información**	**GA-4**
Objetivo:	Evaluar la implementación de un marco de seguridad de la información en la empresa, para mantener el impacto y la ocurrencia de incidentes de seguridad de la información dentro de los niveles de apetito al riesgo de la empresa.
Criterio:	APO13.01 Establecer y mantener un SGSI. Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineado con los requerimientos de negocio y la gestión de seguridad en la empresa. APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información. Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa. Asegurar que las recomendaciones para implementar las mejoras en seguridad se basan en casos de negocio aprobados, se implementan como parte integral del desarrollo de soluciones y servicios y se operan, después, como parte integral de las operaciones del negocio. APO13.03 Supervisar y revisar el SGSI. Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Recolectar y analizar datos sobre el SGSI y la

	mejora de su efectividad. Corregir las no conformidades para prevenir recurrencias. Promover una cultura de seguridad y de mejora continua.

N.	Procedimiento	Ref. P/T	Hecho por	Fecha
1.	Determine si la administración elaboró el marco de seguridad de la información corporativo y si se encuentra aprobado y divulgado.			
2.	Solicite y revise la política de seguridad local de la información y determine si ésta fue debidamente: Aprobada por la Dirección Publicada por el Gobierno Corporativo Comunicada a todos los colaboradores y las partes externas relevantes.			
3.	Determine si la política de seguridad considera: Una definición de la seguridad de la información. Objetivos de seguridad. El alcance de la política. Principios de la seguridad de la información. Estructura para la evaluación de riesgos. Políticas, principios y requerimientos. Referencias a otros documentos.			
4.	Determine si la política de seguridad de la información está alineada con las normas y procedimientos corporativos globales.			
5.	Determine cuál es la estructura organizacional de la unidad responsable de la seguridad de la información. Integrantes, nombre de los colaboradores y puestos. Funciones y responsabilidades.			
6.	Determine si las funciones y responsabilidades de los colaboradores están en concordancia con la política de seguridad, verificando actividades de los mismos.			
7.	Indague cómo se aprueban los controles de seguridad de la información, si éstos se consideran idóneos y cómo se coordina su implementación.			
8.	Determine cuál es la metodología usada para la valoración del riesgo en seguridad de TI.			
9.	Verifique si las actividades de seguridad ejecutadas concuerdan con la política de seguridad de la información.			
10.	Indague cómo la empresa ha promovido la educación, capacitación y conocimiento de la política de seguridad de la información a sus colaboradores.			
11.	Verifique la existencia de un programa formal de concienciación sobre seguridad para todos los empleados.			
12.	Verifique que el programa de concienciación sobre seguridad proporcione diversos métodos para informar y educar a los empleados, por ejemplo: carteles, cartas, notas, capacitación basada en la web, reuniones y promociones.			

13.	Verifique cuáles empleados han participado de la capacitación sobre concienciación de la seguridad de la información.			
14.	Verifique que el programa de concienciación sobre seguridad exija a los empleados que reconozcan, por escrito o de forma electrónica, al menos una vez al año, haber leído y entendido la política de seguridad de la información de la empresa.			
15.	Indague si han ocurrido cambios significativos, que ameriten la actualización de la política de seguridad para asegurar su continuidad, eficiencia y eficacia; considere los siguientes aspectos: Si ha habido alguna realimentación. Alguna evaluación de la política de seguridad o revisión interna. Acciones preventivas y correctivas implementadas por la empresa. Cambio en el ambiente labora, disponibilidad de los recursos, condiciones contractuales, regulaciones internas y legales o cambio en el ambiente técnico.			
16.	Prepare un cuestionario para determinar si el personal tiene conocimiento del marco de seguridad de la información.			
17.	Verificar que se han elaborado auditorías internas al SGSI a intervalos planificados.			
18.	Comprobar el registro de las acciones y los eventos que podrían tener un impacto en la efectividad o el desempeño del SGSI.			
Elaborado por:		Supervisado por:		
Fecha:		Fecha:		

GUÍA DE AUDITORÍA Evaluación la gestión de protección contra software malicioso				GA-5
Objetivo:	Comprobar que la seguridad de las redes y las comunicaciones cubre con las necesidades del negocio.			
Criterio:	DSS05.01 Proteger contra software malicioso. Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, –spyware- o spam.			
N.	**Procedimiento**	**Ref. P/T**	**Hecho por**	**Fecha**
1.	Solicite al jefe de unidad el programa de divulgación para la concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención.			
2.	Verifique con la dirección de planificación corporativa el detalle de las capacitaciones brindadas al personal sobre seguridad de la información en protección de malware en los últimos 3 años.			
3.	Indague la existencia de herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera.			
4.	Obtenga y revise el listado del software de protección de forma centralizada (versión y parcheado) usando una configuración centralizada y la gestión de cambios.			
5.	Indague sobre el proceso de revisión y evaluación que debe realizarse regularmente sobre la información de posibles nuevas amenazas (p.ej: revisando productos de vendedores y servicios de alertas de seguridad).			
6.	Verifique la existencia de firewalls de perímetro instalados entre las redes inalámbricas y los sistemas que almacenan datos y que estos firewalls niegan y controlan todo el tráfico.			
7.	Verifique los filtros del tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de *phishing*).			
8.	Verifique que todos los mecanismos antivirus sean actuales y que estén en funcionamiento.			
9.	Obtenga el programa de formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado.			
10.	Compruebe mediante muestreo la posibilidad de instalación de programas o aplicaciones riesgosas.			
Elaborado por:		Supervisado por:		
Fecha:		Fecha:		

GUÍA DE AUDITORÍA Evaluación de la gestión de la seguridad de la red y las conexiones				GA-6
Objetivo:	Verificar la gestión de seguridad de la red y las conexiones.			
Criterio:	DSS05.02 Gestionar la seguridad de la red y las conexiones. Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.			
N.	**Procedimiento**	**Ref. P/T**	**Hecho por**	**Fecha**
1.	Obtenga la política de seguridad para las conexiones, la cual debe estar establecida y mantenida basada en el análisis de riesgos y en los requerimientos del negocio.			
2.	Valide la permisibilidad de que sólo los dispositivos autorizados puedan tener acceso a la data y a la red.			
3.	Verifique la configuración de estos dispositivos para forzar la solicitud de contraseña.			
4.	Valide la implementación de mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.			
5.	Compruebe el cifrado la información en tránsito de acuerdo con su clasificación.			
6.	Verifique la aplicación de los protocolos de seguridad aprobados a las conexiones de red.			
7.	Indague sobre la configuración de los equipamientos de red de forma segura.			
8.	Obtenga cuales mecanismos de confianza se han establecido para dar soporte a la transmisión y recepción segura de información.			
9.	Verifique la realización de pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.			
10.	Verifique la realización de pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.			
11.	Verifique que las normas de configuración del *firewall* del *router* incluyan la descripción de grupos, roles y responsabilidades para una administración lógica de los componentes de la red.			
12.	Determine si existe un inventario de las aplicaciones accesibles desde el exterior y servicios.			
13.	Determine si existe un terminal específico diseñado para monitorear la actividad dentro del sistema online.			
14.	Determine cuáles son los controles implementados para la instalación y actualización del software.			
15.	Verifique que los archivos actuales de las pistas de auditoría estén protegidos contra modificaciones no autorizadas a través de los mecanismos de control de acceso, segregación física o segregación de redes.			
Elaborado por:		Supervisado por:		
Fecha:		Fecha:		

GUÍA DE AUDITORÍA Evaluación de Seguridad de los puestos de usuario finales				GA-7
Objetivo:	Valorar la seguridad de los puestos de usuario finales.			
Criterio:	DSS05.03 Gestionar la seguridad de los puestos de usuario finales. Asegurar que los puestos de usuario finales (es decir, portátil, equipo sobremesa, servidor y otros dispositivos y software móviles y de red) están asegurados a un nivel que es igual o mayor al definido en los requerimientos de seguridad de la información procesada, almacenada o transmitida.			
N.	**Procedimiento**	**Ref. P/T**	**Hecho por**	**Fecha**
1.	Valide que la configuración de los sistemas operativos sea de forma segura.			
2.	Compruebe la implementación de mecanismos de bloqueo de los dispositivos.			
3.	Verifique el cifrado de la información almacenada de acuerdo a su clasificación.			
4.	Solicite el plan de gestión para el acceso y control remoto.			
5.	Compruebe mediante pruebas de validación la gestión de la configuración de la red de forma segura.			
6.	Valide la implementación del filtrado del tráfico de la red en dispositivos de usuario finales.			
7.	Confirme la protección de la integridad del sistema.			
8.	Valide la protección física a los dispositivos de usuario finales.			
9.	Cerciore que se cuenta con metodología para deshacerse de los dispositivos de usuario finales de forma segura.			
10.	Determine si hay un proceso para revisión de los derechos de los usuarios, dado un cambio en el puesto y las funciones o salida de un empleado, así como los derechos de privilegios para asegurarse que no se hayan obtenido accesos o privilegios no autorizados.			
11.	Seleccione una muestra de empleados cesantes en los últimos seis meses y revise las listas de acceso de usuarios actuales para verificar que sus ID se hayan desactivado o eliminado.			
12.	Indague cual es el procedimiento para registrar las fallas y las acciones que ha tomado la Administración.			
13.	Revise la aplicación, adquisición, implementación y planes de pruebas para confirmar que se han abordado la seguridad de las aplicaciones y la disponibilidad en el entorno integrado.			
Elaborado por:		Supervisado por:		
Fecha:		Fecha:		

GUÍA DE AUDITORÍA Evaluación de la gestión de la identidad del usuario y el acceso lógico.				GA-8
Objetivo:	Verificar la gestión de la identidad del usuario y el acceso lógico.			
Criterio:	DSS05.04 Gestionar la identidad del usuario y el acceso lógico. Asegurar que todos los usuarios tienen derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio.			
N.	**Procedimiento**	**Ref. P/T**	**Hecho por**	**Fecha**
1.	Obtenga y revise las políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y de aplicación, y a las bases de datos.			
2.	Obtenga y revise los manuales de procedimientos donde se definen los perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información de los usuarios.			
3.	Verifique si se mantienen los derechos de acceso lógico de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio.			
4.	Valide la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menos privilegio, necesidad de tener y necesidad de conocer.			
5.	Verifique mediante una muestra que los derechos asignados a los usuarios corresponden a los establecidos en la política empresarial.			
6.	Determine cuáles son los controles de acceso a la información impresa, visible en pantallas o almacenada en medios físicos y proteger adecuadamente dichos medios.			
7.	Compruebe la identificación de todas las actividades de proceso de la información por los roles funcionales, la coordinación con las unidades de negocio y el aseguramiento que todos los roles están definidos consistentemente.			
8.	Valide que estén autenticados todos los accesos a los activos de información basándose en su clasificación de seguridad, coordinando con las unidades de negocio que gestionan la autenticación en las aplicaciones usadas en los procesos de negocio para asegurar que los controles de autenticación han sido administrados adecuadamente.			
9.	Verifique que se cumplen los procedimientos para el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI.			
10.	Compruebe que se ha administrado todos los cambios			

	de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados.			
11.	Verifique la segregación y gestión de cuentas de usuarios privilegiadas.			
12.	Evidencie la regularidad de revisiones de la gestión de todas las cuentas y privilegios relacionados.			
13.	Compruebe el aseguramiento que todos los usuarios (internos, externos y temporales) y su actividad en los sistemas TI (aplicaciones de negocio, infraestructura TI, operación, desarrollo y mantenimiento de sistemas) son identificables unívocamente.			
14.	Valide el mantenimiento de la pista de auditoría de los accesos a la información clasificada como altamente sensible.			
15.	Verifique que todos los medios se hayan clasificado de manera que la sensibilidad de los datos se pueda determinar.			
16.	Verifique la identificación unívoca de todas las actividades de procesamiento de la información por usuario.			
17.	Indague sobre la clasificación de los recursos de TI en forma explícita, formal y uniforme de acuerdo con términos de sensibilidad.			
18.	Verifique que la responsabilidad de supervisar y controlar todos los accesos a los datos esté formalmente asignada.			
19.	Determine si existe un sistema de monitoreo que considere: usuario, fecha y hora de los eventos claves, tipos de eventos, archivos a los cuales se tuvo acceso a programas/utilidades utilizados, intentos no autorizados, detección de intrusos, alerta o falla del sistema entre otros.			
20.	Determine cuáles son los lineamientos para la selección y uso de las claves confidenciales para el uso de los sistemas.			
21.	Verifique que todos los usuarios (muestra) tengan asignada una ID (identificador único) para tener acceso a componentes del sistema.			
22.	Determine cuáles son los procedimientos para identificar la identidad de una persona antes de proporcionar una clave nueva, sustituta o temporal.			
23.	Determine cuáles son los controles para la requisición, aprobación, establecimiento, suspensión y desactivación de tales medios de autenticación, así como para su revisión y actualización periódica y atención de usos irregulares.			
Elaborado por:		Supervisado por:		
Fecha:		Fecha:		

GUÍA DE AUDITORÍA Evaluación de la Gestión del acceso físico a los activos de TI				GA-9
Objetivo:	Evaluar la Gestión del acceso físico a los activos de TI.			
Criterio:	DSS05.05 Gestionar el acceso físico a los activos de TI. Definir e implementar procedimientos para conceder, limitar y revocar el acceso a los locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a locales, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Esto aplicará a todas las personas que entren en los locales, incluyendo empleados, personal temporal, clientes, proveedores, visitantes o cualquier otra tercera parte.			
N.	**Procedimiento**	**Ref. P/T**	**Hecho por**	**Fecha**
1.	Obtenga y revise las políticas, reglas y procedimientos relacionados con el acceso a las terminales y otros recursos de comunicación.			
2.	Valide las gestiones de las peticiones y concesiones de acceso a las instalaciones de procesamiento.			
3.	Compruebe que las peticiones formales de acceso estén completadas y autorizadas por la dirección del emplazamiento de TI, y conservarse las solicitudes registradas.			
4.	Verifique que los formularios contengan la identificación específica de las áreas a las que el individuo tiene acceso concedido.			
5.	Asegúrese que los perfiles de acceso están actualizados. El acceso a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) debe basarse en función del trabajo y responsabilidades.			
6.	Verifique el registro y supervisión de todos los puntos de entrada a los emplazamientos de TI. A su vez, valide la bitácora de registro de todos los visitantes a las dependencias, incluyendo contratistas y proveedores.			
7.	Corrobore la instrucción a todo el personal para mantener visible la identificación en todo momento.			
8.	Compruebe la prevención de expedición de tarjetas o placas de identidad sin la autorización adecuada.			
9.	Valide la regulación de escoltar a los visitantes en todo momento mientras estén en las dependencias. Valide que si se encuentra a un individuo que no va acompañado, que no resulta familiar y que no lleva visible la identificación de empleado, es alertado al personal de seguridad.			
10.	Determine cuáles son los controles para definir la propiedad, custodia y responsabilidad sobre los recursos			

11.	Verifique la restricción del acceso a ubicaciones de TI sensibles validando las prohibiciones en el perímetro, tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores.			
12.	Compruebe que los dispositivos restringen el acceso y disparen una alarma en caso de acceso no autorizado. Ejemplos de estos dispositivos incluyen placas o tarjetas de acceso, teclados (keypads), circuitos cerrados de televisión y escáneres biométricos.			
13.	Verifique que el acceso físico a los puntos de acceso inalámbricos, puertas de enlace (gateways), dispositivos manuales, hardware de redes/comunicaciones y líneas de telecomunicaciones haya sido correctamente limitado.			
14.	Verifique que los archivos actuales de las pistas de auditoría estén protegidos contra modificaciones no autorizadas a través de los mecanismos de control de acceso, segregación física o segregación de redes.			
15.	Verifique que los registros de auditoría se encuentren disponibles durante al menos un año y que se implementen los procesos para restaurar al menos los registros de los últimos tres meses para el análisis inmediato.			
16.	Verifique que solo las personas que lo necesiten por motivos relacionados con el trabajo, puedan ingresar al cuarto de servidores. Y que se mantenga una bitácora.			
17.	Compruebe la práctica regular de formación de concienciación de seguridad física, verificando la existencia de un programa o plan al respecto.			
Elaborado por:		Supervisado por:		
Fecha:		Fecha:		

GUÍA DE AUDITORÍA **Evaluación de la Gestión de documentos sensibles y dispositivos de salida.**				GA-10
Objetivo:	Comprobar la idónea Gestión de documentos sensibles y dispositivos de salida.			
Criterio:	DSS05.06 Gestionar documentos sensibles y dispositivos de salida. Establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para activos de TI sensibles, tales como formularios especiales, títulos negociables, impresoras de propósito especial o credenciales (tokens) de seguridad.			
N.	**Procedimiento**	**Ref. P/T**	**Hecho por**	**Fecha**
1.	Obtenga los procedimientos para gobernar la recepción, uso, eliminación y destrucción de formularios especiales y dispositivos de salida hacia, dentro y fuera de la empresa.			
2.	Valide la asignación de los privilegios de acceso a documentos sensibles y dispositivos de salida basándose en el principio del menor privilegio, equilibrando riesgo y requerimientos del negocio.			
3.	Verifique que se ha establecido un inventario de documentos sensibles y dispositivos de salida			
4.	Valide que se realizan las conciliaciones de este inventario con regularidad periódica.			
5.	Compruebe el establecimiento de salvaguardas física apropiadas sobre formularios especiales y dispositivos sensibles.			
6.	Verifique los procesos de destrucción de la información sensible (por ejemplo, desmagnetizando los soportes magnéticos, destruyendo físicamente los dispositivos de memoria, poniendo trituradoras o papeleras cerradas para destruir formularios especiales y otros documentos confidenciales).			
7.	Verifique la existencia de un programa de protección de los dispositivos de salida.			
Elaborado por:		Supervisado por:		
Fecha:		Fecha:		

GUÍA DE AUDITORÍA Supervisión de la infraestructura para detectar eventos relacionados con la seguridad				GA-11
Objetivo:	Supervisar la infraestructura para detectar eventos relacionados con la seguridad de TI.			
Criterio:	DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad. Usando herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.			
N.	**Procedimiento**	**Ref. P/T**	**Hecho por**	**Fecha**
1.	Verifique el registro de los eventos relacionados con la seguridad, que sean reportados por las herramientas de monitorización de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse en base a la consideración de riesgo.			
	Compruebe que estos registros sean retenidos durante un período apropiado para ayudar en futuras investigaciones.			
2.	Corrobore la existencia de un procedimiento que logre definir y comunicar la naturaleza y características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos para permitir una respuesta acorde.			
3.	Verifique las revisiones regulares de los registros de eventos para detectar incidentes potenciales.			
	Determine cuáles son los controles de los medios de desarrollo, prueba y operación.			
4.	Obtenga el procedimiento apropiado para la recopilación de evidencias en línea con las normas de evidencias forenses locales y cerciorar que todos los empleados están concienciados de los requerimientos.			
5.	Asegúrese que los tiques de incidentes de seguridad se crean en el momento oportuno cuando el monitoreo identifique incidentes de seguridad potenciales.			
6.	Determine si los servicios prestados por terceros son monitoreados y revisados regularmente considerando: Niveles de desempeño del servicio, Reportes de servicios, Incidentes de seguridad de la información, Rastros de auditoría, Eventos de seguridad, Problemas operacionales y Fallas de monitoreo e interrupciones del servicio entregado.			
Elaborado por:		Supervisado por:		
Fecha:		Fecha:		

GUÍA DE AUDITORÍA Evaluación de la Continuidad de los Servicios de TI				G-12
Objetivo:	Continuar las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa ante el evento de una interrupción significativa.			
Criterio:	DSS04 Gestionar la Continuidad. Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.			
N.	**Procedimiento**	**Ref. P/T**	**Hecho por**	**Fecha**
1.	Obtenga el plan de continuidad de servicio de TI o recuperación de desastres para todas las funciones de negocio claves y procesos.			
2.	Determine si los diferentes actores tienen establecidos su rol, responsabilidades y los procedimientos para la efectiva ejecución del plan de continuidad de los servicios de TI y si están documentados y actualizados.			
3.	Verifique si el Plan de Continuidad de los servicios de TI esta: Actualizado. Aprobado. Comunicado a los colaboradores. Es de conocimiento de los colaboradores.			
4.	Determine que hay un control de cambios para asegurar que la seguridad de la información forma parte del ciclo de vida de la continuidad de negocio. Si existe, verifique que se mantiene actualizado y responde a los requerimientos actuales del negocio, considerando: La adquisición de nuevo equipo Actualización de los sistemas, y Cambios en: Personal. Direcciones o número de teléfono. Estrategia comercial. Local, medios y recursos. Legislación. Contratista, proveedores y clientes clave. Proceso, los nuevos o los eliminados. Riesgo (operacional y funcional).			
5.	Determine si el Plan de Continuidad de los Servicios de TI considera: Guía sobre cómo utilizar el plan de continuidad de los servicios de TI. Procedimientos de respuesta definidos para			

	retornar al estado que estaba antes del incidente o desastre. Procedimientos de recuperación en un eventual desastre. Procedimientos para salvaguarda y reconstrucción de las instalaciones de procedimientos normales. Procedimientos de coordinación con autoridades públicas. Procedimientos de comunicación con los funcionarios, dependencias externas, proveedores críticos, directores y el Gobierno Corporativo. El almacenamiento externo de copias de respaldo, documentación y otros recursos de TI, catalogados como críticos. Análisis del impacto por la falta de continuidad de los servicios de TI.			
6.	Verifique que se ha identificado los eventos a los que está expuesta la empresa, que pueden causar interrupciones a los procesos, junto con la probabilidad de impacto, así como las consecuencias que puede tener sobre la seguridad de la información.			
7.	Constate que se han asegurado en los acuerdos de copia de respaldo y recuperación se incluye requerimientos de seguridad de la información.			
8.	Determine si el Plan de Continuidad de los Servicios de TI establece los responsables de la ejecución.			
9.	Determine, luego de verificar la evaluación de riesgo, si se ha establecido una estrategia de continuidad de los servicios de TI.			
10.	Dado que en el plan de continuidad de los servicios de TI hay información confidencial, solicite: – La estrategia de distribución de los planes de continuidad de TI. – Lista de personal con acceso al Plan. – Ubicación de los lugares donde están almacenados las copias de los planes de continuidad de los servicios de TI. – Solicite al personal con acceso a los planes el Plan de Continuidad de TI. Asegúrese de que los planes se distribuyen de forma apropiada y segura y que están disponibles entre las partes involucradas y autorizadas cuando se requiera.			
11.	Solicite los reportes o informes con los resultados de las			

	pruebas realizadas al plan de continuidad de los servicios de TI y determine si el programa de pruebas considera: Pruebas flexibles de simulación con varios escenarios. Simulaciones. Pruebas de recuperación técnica, asegurado que los sistemas puedan restaurarse de manera efectiva. Pruebas de recuperación local alternativas, corriendo los procesos en paralelo a las operaciones. Pruebas de los medios y servicios del proveedor. Ensayos completos, con toda la organización y el personal. Además, analice los resultados obtenidos en las pruebas y las acciones tomadas.			
12.	En el caso de una reanudación de las funciones de TI, determine cuáles han sido las acciones de la Administración para valorar el adecuado plan y si se requiere alguna actualización. Además, determine si existen procedimientos para tal fin.			
13.	Determine si existen procedimientos alternativos de procesamiento, que puedan ser utilizados mientras la función de TI sea capaz de restaurar completamente los servicios después de un evento o desastre.			
14.	Solicite el inventario actualizado de los equipos informáticos, su ubicación y nivel de uso institucional para los procesos críticos.			
15.	En el caso de que los equipos sean arrendados, solicite y analice los acuerdos del contrato. Además, solicite copia de las pólizas de segura que cubren los equipos informáticos y determine que equipos están cubiertos y cuál es el tipo de cobertura y el monto asegurado.			
16.	Determine si existe un procedimiento para efectuar el proceso de evaluación y selección y contratación de los seguros.			
17.	Determine si hay datos y operaciones críticas debidamente identificadas, documentadas, priorizadas y probadas por los dueños de la información, en razón de una política institucional y mediante un manual de procedimientos.			
18.	Determine si existe un procedimiento para el almacenamiento de los medios de respaldo, documentación y otros recursos de TI críticos,			

	necesarios para la recuperación de TI.			
19.	Determine si la Administración ha realizado alguna evaluación de los centros de almacenamiento externos, respecto al contenido, la protección ambiental y la seguridad.			
20.	Validar si se consideran los incidentes de seguridad de la información como disparadores importantes para mejorar el plan de continuidad de negocio			
21.	Determine el impacto que pueden tener las interrupciones causadas por incidentes en la seguridad de la información.			
22.	Verifique que se hayan asegurado que las revisiones pos-reanudación incluyen la seguridad de la información.			
Elaborado por:		Supervisado por:		
Fecha:		Fecha:		

Diseño de la hoja de hallazgos

Se denomina hallazgo de auditoría al resultado de la comparación que se realiza entre un criterio y la situación actual encontrada durante el examen a un departamento, un área, actividad u operación. Se refiere a toda información que a juicio del auditor le permite identificar hechos o circunstancias significativos que inciden en la gestión de recursos en la organización, programa o proyectos bajo examen, y que por lo tanto deben ser comunicados en el informe.

Los elementos o atributos que componen un hallazgo son los siguientes:

Condición: constituye la situación actual encontrada por el auditor con respecto a una operación, actividad o transacción, es el escenario que visualiza el observante, lo que es en el momento. La condición refleja el grado en que los criterios están siendo logrados o aplicados.

Criterio: Es representado por la norma o parámetro con la cual el auditor mide la condición. Son las metas que la entidad u órgano auditado está tratando de lograr, las guías básicas para el debido funcionamiento o las normas relacionadas con su logro, es lo que

debe ser o como debe de hacerse. Constituyen las unidades de medida que permiten la evaluación de la condición.

Causa: Es la razón u origen fundamental por las cuales se presentó la condición, o es el motivo por el que no se cumplió el criterio o la norma. Las recomendaciones que se formulen como resultado del estudio, deben estar directamente relacionadas con las causas que se hayan identificado, indicando quien o que lo origino.

Efecto: Es el resultado o consecuencia real o potencial que resulta de la comparación entre la condición y el criterio que debió ser aplicado. Sean estos reales o potenciales, deben definirse en lo posible en términos cuantitativos, el impacto debe traducirse en cifras financieras, moneda, tiempo, unidades de producción o números de transacciones. El establecimiento de efectos ayuda a demostrar la necesidad de acción correctiva y provee la importancia relativa del hallazgo. Algunas veces no es posible la cuantificación del efecto, sin embargo esto no es una razón válida para no informar sobre observaciones significativas.

Los hallazgos se caracterizan por contener los siguientes requisitos básicos:

- Importancia relativa que amerite su desarrollo y comunicación formal.
- Basado en hechos y evidencia precisos que figuren en los papeles de trabajo.
- Objetivo, al fundamentarse en hechos reales.
- Basado en una labor de auditor/a suficiente para respaldar las conclusiones resultantes.
- Convincente para una persona que no ha participado en la ejecución de la auditoría.

Adicionalmente, es importante que para calificar los hallazgos el auditor deba tener muy presentes los subsiguientes elementos:

- Identificar las líneas de mando y de responsabilidad en la organización con respecto a la condición encontrada en el objeto auditado.
- Determinar si la inconsistencia es aislada o muy difundida, verificar el grado de frecuencia de la deficiencia con el fin de evaluar si se trata de un caso aislado o representa una debilidad sistemática general.
- Obtener criterios y opiniones de los colaboradores y entidades relacionadas.
- Establecer las conclusiones de auditoría con base en la evidencia acumulada.
- Definir las acciones correctivas emitiendo las recomendaciones pertinentes.

CAPÍTULO III: PROCESO DE AUDITORÍA

3.1 Objetivo

Tanto los objetivos generales como los específicos se han definido detalladamente en la sección introductoria.

3.2 Alcance

El alcance ha de definir con precisión el entorno y los limites en que se van a desarrollar la auditoría informática, se complementa con los objetivos de la misma. El alcance ha de figurar expresamente en el Informe Final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas.

Tal como se detalla en el apartado de desarrollo del informe, el estudio se orientará a verificar las generalidades de un entorno de seguridad física-lógica, en las áreas sensibles de la organización, las redes y conexiones, así como los procesos de continuidad del negocio de la empresa Bekaert Corp. en sus entidades locales de Costa Rica para el período 2015.

3.3 Criterios Generales de Auditoría

Los criterios constituyen las normas, estándares y procedimientos razonables, contra los cuales los controles de seguridad física y lógica, aplicados a los sistemas de información pueden ser evaluados, y éstos deberán ser definidos de previo a la iniciación de la evaluación.

Como principal fuente de criterio a utilizar durante el desarrollo del trabajo, el marco de referencia será los Objetivos de Control para la Información y las Tecnologías Relacionadas (COBIT), por cuanto al reunir las buenas prácticas en el uso de las tecnologías de información, reúne los mejores principios que una organización como la

evaluada, ausente de la adopción de un estándar internacional en ese sentido, puede utilizar, aplicando de él aquellas condiciones que puedan ser aplicables a su entorno.

En la sección del Informe se detallarán ampliamente los criterios utilizados, los cuales están basados primordialmente en la herramienta de ISACA específica para el área de seguridad de las TIC como lo es el COBIT@5 *para Seguridad de la Información.*

3.4 Planificación

El objetivo en esta etapa es proveer al auditor un entendimiento de la importancia de TI en la organización por auditar, para establecer el enfoque de la auditoría con base en la selección de los componentes significativos de TI, la indagación o exploración de los más prioritarios y la determinación de los proyectos de auditoría para el examen y verificación de los criterios y el cumplimiento de las metas de auditoría.[13]

La planificación del trabajo de auditoría específicamente incluye las siguientes fases:

3.4.1 Planificación preliminar

Un conocimiento de la entidad con énfasis en la seguridad de las tecnologías y sistemas de información.

Podemos definir el conocimiento como un conglomerado de datos sobre hechos, verdades o de información obtenida mediante la experiencia o del aprendizaje con características a posteriori del evento, o en contraposición a través de introspección con cualidades a priori. El conocimiento es una valoración de la posesión de múltiples datos conexos que por sí solos poseen menor cualitativo[14] que en su conjunto.

En el caso sujeto de estudio, el conocimiento de entidad está integrado por el análisis general de todos los elementos relacionados con TI, de los cuales dispone la organización y que considera aspectos como planes estratégicos institucionales y de sistemas de información, estructura organizacional y departamental de TI, plataforma de TI, estándares

[13] Curso Proceso de Auditoría de TI/SI, UCR, Maestría en Auditoría de Tecnologías de Información.

[14] http/www,google.co.cr/search?hl=es&q=define:conocimiento&sa=x&oi=glossarydefinition&act=title, abril 2015.

internacionales concernientes, normativa, políticas, procedimientos y demás aspectos que han sido desarrollados.

Asimismo abarca la realización de las siguientes actividades:

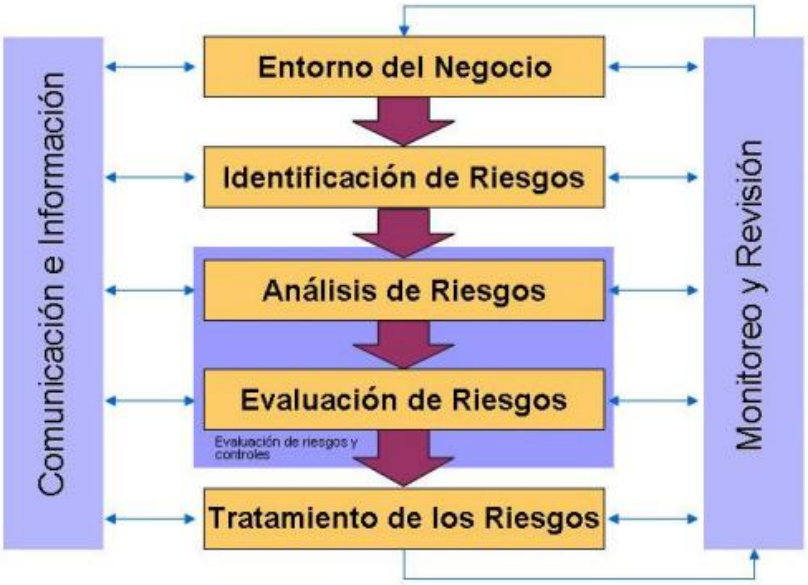
- Observación de las metas globales y objetivos mediante de un análisis de la legislación relevante de la entidad, auditorías anteriores y archivos permanentes de auditoría de estudios similares.
- Análisis del proceso de planificación y presupuesto, especialmente los relativos a las tecnologías y sistemas de información.
- Investigación de la estructura de la organización, particularmente estructura del Departamento de Tecnologías de Información, su integración y conformación funcional.
- Elaboración de entrevistas preliminares con el personal y usuarios clave de TI.
- Preparación de una exploración preliminar a las instalaciones.
- Reconocimiento y selección de áreas de potencial importancia de TI para ser examinadas con detalle.
- Elaboración de un Programa de Planificación detallada con los elementos relevantes de TI por investigar.

Identificación y selección de aspectos de seguridad que constituyen elementos significativos de TI con base en criterios preestablecidos

Para el reconocimiento de los elementos de seguridad física y lógica sobre los cuales se alinearán los recursos, se debe efectuar una evaluación de riesgo que genere los resultados de identificación de estos aspectos relevantes a evaluar. Para realizarse el análisis de riesgo se recomienda utilizar la metodología estructurada en la siguiente gráfica[15]:

[15]Riesgos de tecnología de información implicaciones y retos para la auditoría. Solano, M. Deloitte & Touche, S.A. 2013 Recuperado de http://www.ccpa.or.cr/file/mayo_2013/charlas/21-riesgos-de-tecnologia-de-informacion-implicaciones-y-retos-para-la-auditoría.pdf el 14 de marzo del 2014.

Ilustración 1. Analisis y evaluación de Riesgos



Fuente: Charla Riesgos de tecnología de información implicaciones y retos para la auditoría. 2013

Uno de los elementos más importantes que fortalecen el análisis del riesgo es la definición de los factores que inciden de manera general en cada uno de los procesos TI.

Los factores más comunes son:

- Gente (recurso humano).
- Herramientas para el manejo de los procesos de TI.
- Complejidad de los procesos de TI y de las aplicaciones.
- Documentación de los procesos de TI y de las aplicaciones.
- Nivel de supervisión y monitoreo de los procesos y prácticas de TI.
- Ambiente de control y controles sobre los procesos de TI y de las aplicaciones.
- Efecto en clientes y usuarios de T.I.

Propiamente las actividades contenidas en la metodología para realizar el inventario de riesgos que se deben realizar serian las siguientes:

- Analizar el plan estratégico de TI con el fin de listar los riesgos identificados.
- Consulta a la Auditoría Interna sobre los riesgos identificados como parte del proceso de desarrollo del plan anual.
- Indagación con los miembros del Comité de TI sobre riesgos percibidos por ellos.
- Entrevistas con jefes funcionales o dueños de procesos de TI.
- Entrevista con el responsable de riesgos de la Entidad.
- Recopilación de riesgos de TI según bases de datos de las mejores prácticas.

Elaborar un Programa de Planificación Detallada

Conlleva la preparación de un programa detallado con los componentes significativos de TI por explorar.

3.4.2 Planificación detallada

Para el desarrollo de esta sección de la planificación detallada se desenvuelve a través de técnicas de recopilación de información, realización de reuniones, observación, aplicación de cuestionarios y una evaluación de la información obtenida, con el objeto de identificar las áreas de relevancia y decidir si conciernen ser examinadas con mayor profundidad de análisis en la etapa de examen y pruebas de auditoría. Sobre ellas se aplicarán las herramientas como guías de auditoría, procedimientos de investigación, listas de chequeo, entrevistas, reuniones, pruebas a los distintos sistemas que el auditor considere necesarias para realizar su trabajo.

Comprende las siguientes etapas:

- ✓ Preparación de papeles de trabajo (PT)
- ✓ Examen o Verificación:
  - Preparación de programas de auditoría
  - Efectuar pruebas de control
  - Efectuar pruebas sustantivas
  - Desarrollo de oportunidades de mejora
  - Preparar el borrador del informe

3.5 Preparación de papeles de trabajo

Los papeles de trabajo son documentos de diversa índole que registran el planeamiento, naturaleza, oportunidad y alcance de los procedimientos de auditoría empleados por el auditor, así como los resultados y conclusiones conseguidas de la evidencia adquirida.

Se manejan para controlar y guiar el progreso del trabajo realizado, y por supuesto para respaldar la opinión del auditor. Los papeles de trabajo pueden estar conformados por datos conservados en papel, película, medios electrónicos u otros medios.

Este informe ha sido sustentado en resultados obtenidos a partir de la información analizada y plasmada en el legajo de papeles de trabajo existente, mediante documentos físicos y electrónicos.

3.6 Examen o verificación

La etapa de auditoría correspondiente al examen o verificación aplicando el programa elaborado resume la actividad generadora de insumos para la redacción del documento pertinente y la comunicación de resultados al auditado. En ésta fase se desarrollan los programas respectivos, se ejecutan las pruebas de control y sustantivas que le permite al auditor de identificar las oportunidades de mejora detectadas mediante los hallazgos, las cuales serán expuestas e informadas al auditado por medio de un informe de auditoría.

3.7 Comunicación de resultados

De acuerdo con lo que establece las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna (NIA) en su apartado 2400 de Comunicación de Resultados, los auditores internos deben comunicar los resultados del trabajo oportunamente y la comunicación debe contener, entre otros aspectos, los siguientes:

- Los objetivos y alcance del trabajo, así como las conclusiones correspondientes.
- Las recomendaciones.
- Los planes de acción.
- Debe incluir, si corresponde, la opinión general del auditor interno.
- Se debe reconocer cuando se observa un desempeño satisfactorio.
- Las comunicaciones deben ser precisas, objetivas, claras, concisas, constructivas, completas y oportunas.
- Comunicar los resultados finales a las personas que puedan asegurar la debida consideración.

La comunicación final de resultados del trabajo según la norma NIA 2410 de Criterios para la Comunicación, debe incluir, si corresponde, la opinión y/o las conclusiones del auditor interno. Cuando se está formulando una opinión o conclusión, debe tomarse en consideración las expectativas del Consejo, la alta dirección y de otras partes interesadas, además esta debe sustentarse por información suficiente, fiable, relevante y útil. Así, las

opiniones en los informes de auditoría pueden ser categorizaciones o calificaciones de *rating*, conclusiones u otras descripciones o tipos de exposición de los resultados. El desarrollo de una auditoría puede estar relacionado con controles sobre un proceso específico, riego o unidad de negocio, en nuestro caso está diseñada sobre el área de seguridad de las tecnologías de información. La conformación de opiniones al respecto precisa de la contemplación de los resultados del trabajo, su importancia y repercusión.

Se confeccionará el borrador del informe para ser discutido con el gobierno corporativo local, seguidamente se obtendrá el informe definitivo; el cual se mostrará esquemáticamente en forma de matriz, cuadros o redacción simple y concisa que destaque las inconsistencias halladas, los efectos y las recomendaciones correspondientes. Las comunicaciones deben ser precisas, objetivas, claras, concisas, constructivas, completas y oportunas.

Seguidamente se muestra el informe realizado como producto del examen desarrollado.

"INFORME DE REVISIÓN DE LA EVALUACIÓN DE LOS PROCESOS DE AUDITORÍA DE LA SEGURIDAD EN SISTEMAS Y REDES DE COMUNICACIÓN DEL GRUPO BEKAERT C.R.""

1. INTRODUCCIÓN

1.1 Origen

El presente estudio se realizó de conformidad con lo programado en el Plan Anual de Trabajo de la Auditoría Interna para el año 2015 para la región Bekaert Latinoamérica, desde la plataforma corporativa del Grupo de Control sobre el Grupo de TI.

1.2 Objetivos

Tanto los propósitos generales como los específicos han sido definidos detalladamente en la sección introductoria. No obstante, se resalta para este informe como intensión o finalidad del examen desarrollado dentro de la empresa el siguiente:

> Diagnosticar la situación de la empresa Bekaert C.R. en cuanto a su nivel de seguridad y cumplimiento con la ejecución de la herramienta basada en COBIT@5 *para la Seguridad de la Información*, en el entorno y los procesos operativos de las redes de comunicación y los sistemas informáticos actuales, para poder obtener pruebas que sustenten el informe a la administración.

1.3 Alcance

El estudio se orientará a verificar las generalidades del entorno de seguridad informática, tanto física como lógica, partiendo de la existencia de un marco de buenas prácticas corporativas que se han basado en COBIT. Validar la normativa, políticas y procedimientos internos para los procesos vinculados con la seguridad de la información, existente en las áreas sensibles de la organización dentro del Departamento de Tecnologías de Información, tales como accesos físicos, lógicos, redes de interconexión, sistemas de comunicación, y plan de continuidad.

La aplicación de las pruebas radicará principalmente en un seguimiento al programa de la herramienta diseñada especialmente para el negocio con base en el COBIT@5 *para*

Seguridad de la Información, y que se aplicará a las unidades de negocio implantadas en Costa Rica desde mayo del 2014, y que ya cuentan con su primer año de funcionamiento y operación, tomándolo dentro del plan anual de auditoría del 2015 del Grupo de Auditoría Interna para la región de Latinoamérica.

1.4 Criterios Generales de Auditoría

Como principal fuente de criterio a utilizar durante el desarrollo del trabajo, serán los Objetivos de Control para la Información y las Tecnologías Relacionadas (COBIT), por cuanto al reunir las buenas prácticas en el uso de las tecnologías de información, incorpora los mejores principios que una organización como la revisada, en circunstancias donde está alejada la adopción de un estándar internacional se puede aplicar y tomar como marco de referencia completo, adoptando de él aquellas condiciones que pueden ser adaptables a su entorno, y más aun con la inserción en el año 2012 del COBIT$^{@}$5 *para Seguridad de la Información* como la nueva guía profesional de ISACA para el gobierno y la gestión corporativa de la seguridad de la información, la cual conjunta los marcos de referencia de COBIT, considerando también Val IT, Risk IT, el Marco de Aseguramiento TI (ITAF), la publicación titulada *"Board Briefing on IT Governance"* y el recurso Llevando el Gobierno hacia Adelante (TGF).

En específico para nuestro examen en Bekaert Corp. se tomaron los procesos APO13 Gestionar la seguridad, DSS04 Gestionar la continuidad y DSS05 Gestionar los servicios de seguridad, los cuales suministran una guía fundamental sobre cómo definir, operar y dar un monitoreo a un sistema para la gestión de la seguridad. Este marco de referencia asume que la seguridad de la información se encuentra presente a lo largo de toda la empresa, con aspectos de seguridad de la información dentro de cada actividad y proceso realizado. Además, se consideran también los aspectos de seguimiento, supervisión y monitoreo que se encuentran en los procesos MEA01 Supervisa Evaluar y Valorar Rendimiento y Conformidad, MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno, y MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.

Seguidamente se detallan los criterios utilizados:

APO13.01 Establecer y mantener un SGSI.
Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineado con los requerimientos de negocio y la gestión de seguridad en la empresa.

APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.
Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa. Asegurar que las recomendaciones para implementar las mejoras en seguridad se basan en casos de negocio aprobados, se implementan como parte integral del desarrollo de soluciones y servicios y se operan, después, como parte integral de las operaciones del negocio.

APO13.03 Supervisar y revisar el SGSI.
Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. Corregir las no conformidades para prevenir recurrencias. Promover una cultura de seguridad y de mejora continua.

DSS05.01 Proteger contra software malicioso.
Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, –spyware- o spam.

DSS05.02 Gestionar la seguridad de la red y las conexiones.
Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.

DSS05.03 Gestionar la seguridad de los puestos de usuario finales.
Asegurar que los puestos de usuario finales (es decir, portátil, equipo sobremesa, servidor y otros dispositivos y software móviles y de red) están asegurados a un nivel que es igual o mayor al definido en los requerimientos de seguridad de la información procesada, almacenada o transmitida.

DSS05.04 Gestionar la identidad del usuario y el acceso lógico.
Asegurar que todos los usuarios tienen derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio.

DSS05.05 Gestionar el acceso físico a los activos de TI.
Definir e implementar procedimientos para conceder, limitar y revocar el acceso a los locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a locales, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Esto aplicará a todas las personas que entren en los locales, incluyendo empleados, personal temporal, clientes, proveedores, visitantes o cualquier otra tercera parte.

DSS05.06 Gestionar documentos sensibles y dispositivos de salida.
Establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para activos de TI sensibles, tales como formularios especiales, títulos negociables, impresoras de propósito especial o credenciales (tokens) de seguridad.

DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.
Usando herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.

DSS04 Gestionar la Continuidad.
Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.

MEA01 Supervisar, evaluar y valorar el rendimiento y la conformidad
Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada.

MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno
Supervisar y evaluar de forma continua el entorno de control, incluyendo tanto autoevaluaciones como revisiones externas independientes. Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar y mantener normas para la evaluación del control interno y las actividades de aseguramiento.

MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos
Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de TI en el cumplimiento de la empresa general.

2. HALLAZGOS – OPORTUNIDADES DE MEJORA

Hallazgo 1

REF. P/T	**TÍTULO:** Seguridad Física dentro del cuarto de redes y unidad de servidores
PC-AC-01	
	CONDICIÓN:
	Durante el examen y aplicación de pruebas se observó que el centro de cómputo carece de controles ambientales y de acceso. Por ejemplo: sistema detector de líquidos, Piso falso a prueba de inundaciones, controles de humedad, cielorraso a prueba de filtraciones, bitácora de entrada de terceros, alarma contra robo, inexistencia de políticas y directrices relativas por parte de la gerencia.
	CRITERIO:
	DSS05.02 Gestionar la seguridad de la red y las conexiones. *Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.* *La seguridad en TIC deberá ser administrada de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos del negocio.*
	CAUSA:
	Carencia de una política irrestricta sobre el tema por parte de la administración. Aunado a la falta de prioridad en el tema de seguridad y resguardo de los equipos de TIC y la salvaguarda de los mismo.
	EFECTO:
	Se tiene un alto grado de exposición física y ambiental ante los riesgos detectado en el área de cuartos de cómputo. Podría traer consecuencias derivadas de la interrupción del servicio y operaciones, quebranto de credibilidad ante clientes, tanto internos como externos, retrasos en la operatividad y producción que podría conllevar a perdidas monetarias.
	RECOMENDACIÓN:
	A la Dirección de Tecnologías de Información:
	Dada la importancia del riesgo descubierto debe trasladarse el resultado a la administración e incluir la verificación física de los aspectos a mejorar, implementar los controles ambientales y de acceso requeridos. Se debe promulgar un procedimiento relativo al tema de seguridad y resguardo del equipo en los centros de cómputo para las redes y conexiones de los sistemas de información. Este debe ser aprobado y publicado a la mayor brevedad.

Hallazgo 2

REF. P/T	**TÍTULO:** Responsable de la función administrativa de la Seguridad Informática.
PC-AC-02	
	CONDICIÓN:
	En el análisis de la estructura organizacional del departamento de TI, el grupo está falto de un responsable directo con la función de Administrador de la Seguridad Informática, actualmente estas actividades recaen sobre el Encargado de Soporte Tecnico en Sistemas de Información, situación que repercute en la correcta gestión del control de la seguridad de la información.
	CRITERIO:
	APO13.01 Establecer y mantener un SGSI. *Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineado con los requerimientos de negocio y la gestión de seguridad en la empresa. Se debe asignar un responsable del área de seguridad.*
	CAUSA:
	Se dispone de un presupuesto anual establecido por la corporación, tanto en cantidad de personal por área y costo financiero para esos funcionarios. Este presupuesto no contempla el puesto de Administrador de Seguridad de la Información Regional, por lo cual las tareas deben asumirlas los responsables de cada unidad.
	EFECTO:
	Pérdida del control de situaciones relativas al monitoreo de actividades de seguridad, y a la vez el seguimiento escaso a los eventos que puedan ocurrir a partir de los riesgos denotados. Esta carencia de disponibilidad para administrar proyectos de seguridad de la información contrarresta el logro efectivo y eficiente de los mismos.
	RECOMENDACIÓN:
	A la Dirección de Tecnologías de Información:
	Confeccionar una valoración de la necesidad implícita de recurso humano especializado en esta área que venga a coadyuvar con las funciones del SGSI, la administración y monitoreo de las actividades de control bajo estándares globales. Verificar las políticas globales de la corporación con relación al tema de la Seguridad de la Información, y evaluar el planteamiento mediante estudio previo de la necesidad de cubrir esta área con el fin de mitigar los riesgos enumerados.

Hallazgo 3

REF. P/T	**TÍTULO:** Carencia de un Plan de Contingencia específico local.
PC-AC-03	
	CONDICIÓN:
	El grupo a nivel local, carece de un plan de contingencia específico formalmente documentado, divulgado, aprobado y que sea funcional. Debe estar alineado con el plan de contingencia corporativo del negocio, relacionado con los requerimientos, roles de funciones, responsabilidades y procedimientos detallados a seguir en caso de enfrentarse con una eventualidad que afecte la continuidad del negocio.
	CRITERIO:
	DSS04 Gestionar la Continuidad. *Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.*
	CAUSA:
	Debido al ciclo de madurez corporativo, no se cuenta con el nivel de detalle para un plan de contingencia local. No se han dado las orientaciones al respecto para atender las necesidades de contingencias a raíz de los riesgos prominentes.
	EFECTO:
	Se pueden generar acciones correctivas ineficientes, o insuficientes para solventar los casos afrontados. Afectación en la operación del negocio por desatender los procesos, o atender los fallos de forma incorrecta según las directrices o procedimientos correspondientes. Se vería afectado por interrupción del negocio y posibles pérdidas cuantiosas al tener una respuesta imprecisa o incorrecta al tema.
	RECOMENDACIÓN:
	A la Gerencia General:
	La administración debe promover la elaboración del plan, que este sea aprobado, comunicado y divulgado a los funcionarios correspondientes. Estos planes deberán definir detalladamente los procesos alternativos con miras a mitigar los impactos de las posibles interrupciones causadas por fallas en los funcionamientos óptimos. El plan desarrollado deberá ser comprobado mediante procesos de simulación periódicos, que se recaben los resultados y sean actividades de corrección al plan.

Hallazgo 4

REF. P/T	**TÍTULO:** Control de los dispositivos de almacenamiento
PC-AC-04	
	CONDICIÓN:
	Se carece de un control específico sobre los dispositivos eliminados del centro de cómputo. En aplicación al cuestionario de control interno se detectó la ausencia de proceso mediante bitácora de control, verificando que no existe un procedimiento sobre el uso y desecho de dispositivos de almacenamientos, discos duros, barras de memoria, etc. ni se controla el tipo de información que pueda contener los mismos.
	CRITERIO:
	DSS05.06 Gestionar documentos sensibles y dispositivos de salida. *Establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para activos de TI sensibles, tales como formularios especiales, títulos negociables, impresoras de propósito especial o credenciales (tokens) de seguridad.*
	CAUSA:
	Se carece de política o lineamiento relativo al tema en específico para el uso, manejo, resguardo y desecho de dispositivos de almacenamiento.
	EFECTO:
	La fuga de información sensible para la empresa puede originar contracciones fuertes en su gestión administrativa, financiera y operativa. La manipulación y uso de esa información calificada con fines no autorizados puede acaecer pérdida de imagen, información valiosa, daños financieros y parálisis empresarial.
	RECOMENDACIÓN:
	A la Dirección de Tecnologías de Información:
	Se deben establecer los procedimientos adecuados y poner en práctica las políticas y lineamientos en cuanto al uso, manejo y desecho de dispositivos de almacenamiento. El procedimiento deberá contener medidas para procurar un correcto uso y custodia de la información sensible para la organización, y contener validaciones de la integridad del resguardo de la misma.

Hallazgo 5

REF. P/T	**TÍTULO:** Vulnerabilidad de la infraestructura del ambiente de TI
PC-AC-05	
	CONDICIÓN:
	Inexistencia de dispositivos de control de acceso a las salas de servidores, cuartos de cómputo, oficinas administrativas, etc. Se observa la ausencia de sistemas de alarma para detección de intrusos en horas no laborales, así como la ausencia de dispositivos de identificación de usuarios en la entrada principal y en la sala de cómputo y servidores de redes.
	CRITERIO:
	DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad. *Usando herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.*
	CAUSA:
	A pesar de contar con la política de seguridad física, al momento de reconstrucción y remodelación del espacio físico del edificio asignado al área de TI, no fueron consideradas como de importancia relativa ante la necesidad de concluir el proyecto y el límite de presupuesto con que se contaba para el edificio.
	EFECTO:
	El grado de vulnerabilidad excesivo por intrusión física de terceros no autorizados a los sistemas de información contrae elevado apetito al riesgo. Lo que conllevaría a pérdidas de información confidencial, llegando al extremo de provocar la interrupción del negocio parcial o permanente.
	RECOMENDACIÓN:
	A la Gerencia General:
	Se deben establecer que los dispositivos restringen el acceso y disparen una alarma en caso de acceso no autorizado. Ejemplos de estos dispositivos incluyen placas o tarjetas de acceso, teclados (keypads), circuitos cerrados de televisión y escáneres biométricos A pesar que se cuenta con el servicio de seguridad las 24 horas, se debe ejercer un rol de verificación de puerta cerrada y verificación de intrusos dentro del perímetro de las oficinas administrativas y primordialmente cuartos de servidores.

Hallazgo 6

REF. P/T	**TÍTULO:** Control de acceso de funcionarios y terceros a las salas de servidores.
PC-AC-06	**CONDICIÓN:**
	Carencia de una bitácora que enumere los accesos a los cuartos de servidores, donde sean registradas las horas de entrada y salida, tanto para los funcionarios, como para visitantes o terceros que vayan a dar algún servicio sobre las TIC o requieran ingresar a los cuartos por motivos específicos de operación, a su vez que contenga los recursos que fueron utilizados por las personas o usuarios.
	CRITERIO:
	DSS05.05 Gestionar el acceso físico a los activos de TI. *Definir e implementar procedimientos para conceder, limitar y revocar el acceso a los locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a locales, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Esto aplicará a todas las personas que entren en los locales, incluyendo empleados, personal temporal, clientes, proveedores, visitantes o cualquier otra tercera parte.*
	CAUSA:
	El procedimiento interno está siendo incumplido por la norma general del manejo y gestión de las bitácoras correspondientes. Se asume que al contar con un único responsable localmente del área de TI sea el quien se apropie de los gravámenes por eventos subsecuentes en contra el sistema.
	EFECTO:
	De materializarse el riesgo de acceso a los sistemas por intrusión física no autorizada de desconocería la trazabilidad de los individuos que han ingresado al espacio físico delimitado de acceso restringido. No se conocería los momentos de ingresos de las personas, los recursos utilizados y el fin para el cual fue usado. De ser funcionarios no se podrían aplicar medidas correctivas al desconocer el usuario.
	RECOMENDACIÓN:
	A la Gerencia General:
	Se deben establecer medidas de control de acceso físico, utilización de los sistemas, identificación de personal autorizado y visitantes que requieran ingresar al cuarto de sistemas de información, tal cual es el uso de la bitácora. Se debe incluir en los procedimientos que las personas externas, visitantes, o terceros que requieran permanecer en el cuarto de TI deban estar acompañados, y a su vez disponer de cámaras de vigilancia en las secciones de mayor impacto o sensibilidad para el negocio.

Hallazgo 7

REF. P/T	**TÍTULO:** Gestión de creación y mantenimiento de cuentas de usuario.
PC-AC-07	
	CONDICIÓN:
	Fue observado que el procedimiento de creación de cuentas de usuario se basa en un ticket en línea denominado BITS (Bekaert IT Support), aprobados por vía de correo electrónico. Se carece de un formulario específico para la creación y administración de cuentas de usuarios, que gestione las modificaciones o eliminaciones de usuarios existentes. Se carece de un reporte mensual que enliste y verifique los usuarios existentes y de un responsable asignado a comprobar esto.
	CRITERIO:
	DSS05.04 Gestionar la identidad del usuario y el acceso lógico. *Asegurar que todos los usuarios tienen derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio.*
	CAUSA:
	Falta de un procedimiento local y la asignación de un responsable que aplique las regulaciones corporativas. Esta carencia de visibilidad sobre la administración y gestión de los usuarios yace en la limitada afluencia de control hacia este tipo de actividades de seguimiento y monitoreo. El procedimiento corporativo da las pautas a seguir, pero no se han tropicalizado a la realidad local.
	EFECTO:
	Se pueden generar duplicidad de usuarios, usuarios con perfiles de acceso no requeridos a sus funciones, y hasta existencias de cuentas activas para ex funcionarios. Se eleva el riesgo de acceso o transmisión de claves de usuarios, inclusive la utilización de usuarios no correspondientes. Cargos financieros elevados por cuentas de usuarios no requeridos en los sistemas de información, por ejemplo SAP, Intranet, Citrix, Microsoft, etc.
	RECOMENDACIÓN:
	A la Gerencia General:
	Se recomienda generar la creación, aprobación y comunicación del procedimiento sobre gestión de cuentas de usuarios a nivel local. A la vez, generar el proceso de capacitación del mismo a los responsables del área en cuestión, y mandos medios. **A la Dirección de Tecnologías de Información:** Se debe asignar un responsable específico, ya sea de TI o de Control Interno, para que verifique mensualmente la creación de usuarios nuevos, las modificaciones que hayan realizado y las eliminaciones solicitadas y efectuados en el mes, a su vez que este comunique los resultados de tal verificación mediante reporte dirigido a las Gerencias de TI y de Control Interno.

Hallazgo 8

REF. P/T	**TÍTULO:** Sistema de alimentación corriente alterna inexistente
PC-AC-03	
	CONDICIÓN:
	Basado en los cuestionarios de control, se evidencio la inexistencia de un sistema de generación alterna de electricidad. Las instalaciones carecen de abastecimiento de energía eléctrica alterna en caso de fallo en el fluido eléctrico principal. A su vez, se observa la carencia de una red independiente para el centro de cómputo, además de dispositivos de liberación de energía estática.
	CRITERIO:
	DSS04 Gestionar la Continuidad. *Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.*
	CAUSA:
	Debido al grado de madurez de la entidad, el nivel corporativo no tiene entre sus prioridades el abastecimiento alterno como medida de contingencia o mitigación del riesgo. El nivel de importancia para este aspecto ha sido relegado por las prioridades de productividad de la empresa con mayor producción y el incremento en las ventas, para soportar los costos presupuestados.
	EFECTO:
	El fallo en el fluido de energía puede conllevar alteraciones en la información de los diversos sistemas y daños de equipos tecnológicos, así como la salvaguarda de sus componentes. La carencia de un sistema de generador de energía alternativo provocaría una afectación directa a la continuidad del negocio, lo que contraería tanta pérdida de imagen como afectación a las cifras financieras de la empresa.
	RECOMENDACIÓN:
	A la Gerencia General:
	Se debe evaluar en el Comité Gerencial la implementación de un sistema de alimentación alterna de fluido eléctrico, que contribuya a mitigar los riesgos de pérdida de información por cortes de energía, daños en los equipos tecnológicos y sus componentes, además de darle mayor confianza a la continuidad de la producción y el servicio que brinda la empresa. Se debe analizar el costo financiero de implementar este sistema y darle un análisis de retorno de la inversión, versus las pérdidas cuantiosas que puede generar la interrupción del negocio.

Hallazgo 9

REF. P/T	**TÍTULO:** Uso indebido del sistema de correo electrónico
PC-AC-03	
	CONDICIÓN:
	Se observó la carencia de una política apropiada para la seguridad, procedimientos y controles para el uso correcto del sistema de correo electrónico Microsoft Outlook. Si bien es cierto, los colaboradores cuentan con el principio de privacidad de los usuarios sobre sus comunicaciones, pero acá radica en el uso adecuado que se le dé al sistema por parte de los funcionarios.
	CRITERIO:
	DSS05.01 Proteger contra software malicioso. *Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, –spyware- o spam.*
	CAUSA:
	Al estar iniciando operaciones y con tanta información recibida por parte de los colaboradores con respecto a los lineamientos corporativos, existen aspectos que han sido relegados y este es uno de ellos. Se cuenta con una escaza concienciación para el correcto uso de la herramienta de comunicación y cambio de información.
	EFECTO:
	Al carecer de una inducción certera sobre el uso de los correos electrónicos, por el uso distinto a los fines propios conlleva a pérdida de tiempo de los usuarios. La intromisión del administrador del Servicio de Correo en las comunicaciones viola los derechos de confidencialidad y secreto que promulga la legislación internacional y local. Uso irracional del servicio y generación de SPAM de información (correos basura), así como anexos que pueden contener información de peligro para los sistemas de información, tales como virus y gusanos.
	RECOMENDACIÓN:
	A la Gerencia General:
	Se recomienda en primera instancia emitir la comunicación a todos los usuarios de la política interna corporativa sobre el uso de los medios de comunicación por correo electrónico, con el fin de alinear el uso del mismo a nivel global con la operación de nuestro país. Posteriormente es aconsejable emitir un procedimiento local sobre el seguimiento del uso apropiado del programa de correo electrónico, así mismo que esté aprobado y sea comunicado a los mismos usuarios.

Hallazgo 10

REF. P/T	**TÍTULO:** Uso de los puertos para dispositivos de almacenamiento externo
PC-AC-04	
	CONDICIÓN:
	Se constató el uso inapropiado de los dispositivos externos, tales como *USB data traveler* (llave maya), *smartphones*, discos duros, etc. los cuales al ser conectados pueden trasladar virus que contengas estos dispositivos hacia los equipos de la empresa. Además, a pesar de las medidas de seguridad sobre los equipos en cuanto al almacenamiento y extracción de información desde los equipos hacia los dispositivos, se detectó la posibilidad de emigrar información hacia ellos.
	CRITERIO:
	DSS05.03 Gestionar la seguridad de los puestos de usuario finales. *Asegurar que los puestos de usuario finales (es decir, portátil, equipo sobremesa, servidor y otros dispositivos y software móviles y de red) están asegurados a un nivel que es igual o mayor al definido en los requerimientos de seguridad de la información procesada, almacenada o transmitida.*
	CAUSA:
	Se carece de política o lineamiento relativo al tema en específico para el uso, manejo, resguardo y desecho de dispositivos de almacenamiento, como se mencionó anteriormente. Además, el grado de madurez es escaso y con ausencia de seguimiento a los procedimientos por parte de los usuarios.
	EFECTO:
	Se puede generar una infección masiva a los sistemas de información, lo cual puede generar atrasos en la operación diaria, perdida de información sensible o intrusión lógica no autorizada por este aspecto. La extracción directa de información sensible puede perjudicar en grandes ámbitos de caer en manos de competidores, o distribuidores.
	RECOMENDACIÓN:
	A la Dirección de Tecnologías de Información:
	Como primera acción, se debe validar la configuración de los puertos de salida USB para la transacción de datos desde el equipo a los dispositivos externos. Erradicar la posible fuga de información corrigiendo esta configuración de los equipos de cada usuario. Ejecutar filtros de virus, por medio de programas seguros de detección de este tipo de malware. Generar comunicación constante sobre la aparición de nuevos virus, y educar a los usuarios sobre el uso de los BYOD correctamente, con enfoque a la seguridad y cumplimiento de las regulaciones corporativas.

Hallazgo 11

REF. P/T	**TÍTULO:** Capacitación continua de los usuarios
PC-AC-04	
	CONDICIÓN:
	Como resultado de las pruebas generales y revisión del cuestionario de control se pudo inferir que los usuarios están escasos de capacitación en el área específica de Control de la Seguridad y Riesgos de los Sistemas de Información. Se evidencia la existencia de un impasse entre los procesos globales y los procedimientos locales instruidos en un inicio de la inducción general por arranque de operaciones en el país.
	CRITERIO:
	APO13.03 Supervisar y revisar el SGSI. *Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. Corregir las no conformidades para prevenir recurrencias. Promover una cultura de seguridad y de mejora continua.*
	CAUSA:
	La organización local está enfocada en el desarrollo de la productividad y el alcance de los logros comprometidos durante el primer año de operación. SE han efectuado capacitaciones, pero carentes de contenido y tiempo de análisis de las exposiciones efectuadas en el rol de estos temas de seguridad de TI.
	EFECTO:
	Al carecer de información clara y manejada por cada usuario, los riegos de materialización aumentan considerablemente. Temas de intromisión a las redes, accesos no permitidos al espacio físico, riesgo de extracción de información, ingreso de virus y malware, perdida de equipo por hurto, pérdida de tiempo por interrupción de negocio, son aspectos que repercuten gravemente en la productividad y gestión de los sistemas de información.
	RECOMENDACIÓN:
	A la Gerencia General:
	Se debe recurrir a un plan de capacitación general sobre los temas de seguridad de la información, que los usuarios puedan comprender la importancia y relevancia que tiene el cuido y resguardo de las actividades de control sobre los sistemas de información. Coordinar con Recursos Humanos, el diseño de la campaña de conocimiento del tema de los aspectos de seguridad de TI y el apoyo que se requiere de los usuarios.

CAPÍTULO IV: CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

El proceso de conclusiones de un trabajo, examen o proyecto se producen cuando a partir de hechos conocidos se obtiene un nuevo conocimiento, que a raíz de ello se desprenden las deducciones a ser emitidas por el ejecutor. En esta línea procederemos a exponer nuestras conjeturas posteriores al análisis, evaluación y registro de los hechos relevantes que soportan el trabajo realizado en la empresa Bekaert Costa Rica.

Podemos indicar que hoy por hoy la Auditoría de Sistemas de Información es de vital importancia para las empresas innovadoras con visión de futuro, máxime las que se encuentran inmersas en el mundo globalizado y van de la mano con el uso de las TIC. Al no prevenirse los mecanismos de control, seguridad y respaldo de la información dentro de una corporación, esta se percibirá sumergida a contraer altos riesgos lógicos, físicos y humanos, que puedan inducir a fraudes no solamente económicos sino de información sensible, es decir, pérdidas económicas cuantiosas para la compañía.

Los siguientes ejemplos nos invitan a la necesidad apremiante de un tener mayor y mejor acercamiento sistemático a la seguridad de la información:

- Una infraestructura crítica corporativa depende de los sistemas de información, y una intrusión exitosa podría provocar un impacto significativo en la economía y en la seguridad empresarial.
- Información financiera no pública que podría ser usada para obtener beneficios económicos.
- Divulgación de información confidencial que puede causar problemas a las empresas, así como daños de reputación o poner en peligro relaciones de negocio.
- Intrusión en las redes comerciales, por ejemplo, para obtener datos de tarjetas de crédito o de otros medios de pago, que puede llevar a un daño de reputación y financiero sustancial debido a multas, así como un mayor escrutinio por parte de organismos reguladores.
- El espionaje industrial puede permitir que se copien secretos comerciales e incrementar la competencia entre empresas manufactureras.
- Una filtración de datos personales puede resultar en pérdidas financieras y en esfuerzos innecesarios para reconstruir la reputación financiera de la empresa.

- Costes significativos no planificados relacionados con contener, investigar y remediar brechas de seguridad, que pueden impactar a cualquier empresa que haya sufrido un fallo de control.

La corporación mantiene el COBIT como adopción de marco de referencia y guía en sus buenas prácticas para la gestión de los sistemas de información a nivel corporativo, no obstante al ser evaluada mediante una herramienta desarrollada con base en la Guía Profesional COBIT$^{@}$5 *para Seguridad de la Información* para efectos locales, se hace la salvedad que la adaptación de la guía tuvo dificultades por ser efectuada durante este primer año de operaciones en el país.

Del estudio realizado se pueden enunciar claramente aspectos que confrontan los principios de buenas prácticas a ser aplicadas cotidianamente, y que a su vez representan oportunidades de mejora para el ambiente de TI empresarial, las cuales se expondrán a continuación:

- Se denota un ciclo de madurez iniciante para la empresa, lo cual causa desalineaciones con referencias a los marcos y guías para las buenas prácticas, que su vez favorece a oportunidades de reforzar la arquitectura de TI con enfoque a los objetivos corporativos.
- Se determinaron aspectos de alta exposición al riesgo, lo cual puede afectar tanto la continuidad de la operatividad y servicio del negocio, así como la integridad de la información administrada.
- Existe una escasa conciencia gerencial sobre la seguridad informática, principalmente originada por la carencia de algunas políticas, procedimientos y directrices en función del ordenamiento de la gestión de las TIC que hace parecer insipientes a los usuarios sobre este tema.
- La inexistencia de un Administrador de la Seguridad de TI regional que este cercano al control y monitorio de las actividades de Gestión del SI, que dirija las sanas prácticas del entorno informático a nivel local, guiando a los Coordinadores de TI de cada país en estas funciones. Si observamos la estructura corporativa esta figura está en el más alto nivel corporativo sin tener equipo de apoyo por región del mundo que ejerza mayor capacidad de mitigación de riesgos.
- Existencia de alto riesgo por la metodología de conducción de los dispositivos de almacenamiento, el control de los mismos en cuanto a mantenimiento, cambios y desechos que van en contrariedad de procurar una adecuada protección de los datos.
- Se carece de un control de accesos por medio de bitácoras de administración de los centros de cómputo, a falta de procedimientos y guías locales. Los visitantes y usuarios ingresas y hacen uso de los servicios de TI sin tener un registro histórico que permita verificar y dar trazabilidad a casos que puedan suscitarse de una mala gestión o quebranto de la norma.

- Se denota la ausencia de una gestión adecuada de la administración de usuarios, se observa que existen usuarios duplicados en algún momento, usuarios activos de ex-empleados que aún están en los cargos mensuales por cobros de usuarios activos en SAP y otras licencias por usuario.
- La carencia de un ordenamiento hacia el uso del sistema de correo electrónico hacia los usuarios, la falta del procedimiento específico local en este tema ha repercutido en las malas prácticas enunciadas en los hallazgos, conllevando a riesgos de intrusión, denegación de servicio y descargue de virus, saturación de bases de datos, etc.
- Se revela la ausencia de procesos de capacitación al personal clave y usuarios finales sobre los temas de gestión de las Tecnologías de Información. Se han desarrollado programas de capacitación en cuanto a las aplicaciones y sistemas de información, pero el contenido de estos no ha llegado al nivel de detalle en el tema de la gestión de la seguridad de las TIC.

El grupo cuenta con una gama de oportunidades de mejora por desarrollar, los cuales se basan en los puntos principales indicados anteriormente en conjunto con otros menores que han sido enunciados en los hallazgos y que cuentas con el patrocinio de la gerencia general para elaborarlos, basados en los principios de seguridad de COBIT5.

Es aquí donde toma fuerza el ambiente de control y el manejo de las auditorías de sistemas de información, las cuales deberán comprender no sólo la consideración de los equipos de cómputo de un sistema o procedimiento específico, sino que conjuntamente habrá de examinarse los sistemas de información en general desde sus entradas, procedimientos, y controles.

Generalmente en las corporaciones existe una constante preocupación por la materialización de riesgos sobre seguridad de TI, de enfrentarse ocasionalmente a fraudes, denegación de información, disponibilidad del servicio, hurtos, etc.; más sin embargo, muchos de estos podrían ser prevenidos mediante una correcta gestión y seguimiento de los principios de seguridad informática. En la mayoría de los países de América Latina, donde habitualmente los sueldos y salarios son bajos, las crisis reiteradas y las necesidades de los trabajadores no son completamente del todo satisfechas; y aunado a lo anterior le agregamos fallas en el control interno y la falta de vigilancia o monitoreo adecuado en las operaciones de TI, nos conlleva a generar mayores posibilidades de sufrir la materialización de los riesgos. Evitar esta situación es responsabilidad de todos los empleados, por ello es pertinente la creación de una cultura empresarial orientada a minimizar los riesgos que conciernen la seguridad de la información.

4.2 Recomendaciones

El culmen de todo proceso de auditoría es enumerar las recomendaciones apropiadas para los resultados obtenidos de las pruebas realizadas, el auditor basa sus sugerencias en las mejoras prácticas y marcos de referencia, por ejemplo el COBIT5 en este caso.

El implementar un uso habitual de COBIT$^{@}$5 *para Seguridad de la Información* proporciona a la empresa el marco sistemático que fomenta fortalecer los controles de la seguridad de TIC, ya que pueden resultar de gran apoyo y soporte a la gestión de las mismas, tales como por ejemplo:

- Menor complejidad y mayor coste-beneficio debido a una mejorada y fácil integración de estándares sobre las buenas prácticas y/o guías específicas del sector de seguridad de TI.
- Mayor satisfacción de usuario con la estructura y resultados de seguridad de TI.
- Mejor integración de la seguridad de la información en la empresa.
- Toma de decisiones de riesgo con conocimiento y conciencia del riesgo.
- Mejor prevención, detección y recuperación.
- Reducción del impacto de los incidentes de seguridad de la información.
- Soporte mejorado a la innovación y la competitividad.
- Mejor gestión de los costes relacionados con la función de seguridad de la información.
- Mayor conocimiento de la seguridad de la información.

Entre las recomendaciones específicas como resultado de los objetivos planteados y basados en los procesos de revisión efectuados en el examen realizado, se dan las siguientes:

- Dada la importancia del riesgo descubierto, debe trasladarse el resultado a la administración e incluir la verificación de los aspectos a mejorar, implementar los controles ambientales y los controles de acceso requeridos. Se debe promulgar un procedimiento relativo al tema de seguridad y resguardo del equipo en los centros de cómputo para las redes y conexiones de los sistemas de información. Este debe ser aprobado y publicado a la mayor brevedad.
- Confeccionar una valoración de la necesidad implícita de recurso humano especializado en esta área que venga a coadyuvar con las funciones del SGSI, la administración y monitoreo de las actividades de control bajo estándares globales. Además de verificar las políticas globales de la corporación con relación al tema de la Seguridad de la

Información, y evaluar el planteamiento mediante estudio previo de la necesidad de cubrir esta área con el fin de mitigar los riesgos enumerados.

- La administración debe promover la elaboración del plan de contingencia, que este sea aprobado, comunicado y divulgado a los funcionarios correspondientes. Estos planes deberán definir detalladamente los procesos alternativos con miras a mitigar los impactos de las posibles interrupciones causadas por fallas en los funcionamientos óptimos. El plan de contingencia desarrollado deberá ser comprobado mediante procesos de simulación periódicos, que se recaben los resultados y sean actividades de corrección al plan.
- Se deben establecer los procedimientos adecuados y poner en práctica las políticas y lineamientos en cuanto al uso, manejo y desecho de dispositivos de almacenamiento. El procedimiento deberá contener medidas para procurar un correcto uso y custodia de la información sensible para la organización, y contener validaciones de la integridad del resguardo de la misma.
- Se deben establecer que los dispositivos restringen el acceso y disparen una alarma en caso de acceso no autorizado. Ejemplos de estos dispositivos incluyen placas o tarjetas de acceso, teclados (keypads), circuitos cerrados de televisión y escáneres biométricos. A pesar que se cuenta con el servicio de seguridad las 24 horas, se debe ejercer un rol de verificación de puerta cerrada y verificación de intrusos dentro del perímetro de las oficinas administrativas y primordialmente cuartos de servidores.
- Se deben establecer medidas de control de acceso físico, utilización de los sistemas, identificación de personal autorizado y visitantes que requieran ingresar al cuarto de sistemas de información, tal cual es el uso de la bitácora. Además de incluir en los procedimientos que las personas externas, visitantes, o terceros que requieran permanecer en el cuarto de TI deban estar acompañados, y a su vez disponer de cámaras de vigilancia en las secciones de mayor impacto o sensibilidad para el negocio.
- Se recomienda generar la creación, aprobación y comunicación del procedimiento sobre gestión de cuentas de usuarios a nivel local. A la vez, generar el proceso de capacitación del mismo a los responsables del área en cuestión, y mandos medios. Se debe asignar un responsable específico, ya sea de TI o de Control Interno, para que verifique mensualmente la creación de usuarios nuevos, las modificaciones que hayan

realizado y las eliminaciones solicitadas y efectuados en el mes, a su vez que este comunique los resultados de tal verificación mediante reporte dirigido a las Gerencias de TI y de Control Interno.

- Se debe evaluar en el Comité Gerencial la implementación de un sistema de alimentación alterna de fluido eléctrico, que contribuya a mitigar los riesgos de pérdida de información por cortes de energía, daños en los equipos tecnológicos y sus componentes, además de darle mayor confianza a la continuidad de la producción y el servicio que brinda la empresa. Además de analizar el costo financiero de implementar este sistema y darle un análisis de retorno de la inversión, versus las pérdidas cuantiosas que puede generar la interrupción del negocio.
- Se recomienda en primera instancia emitir la comunicación a todos los usuarios de la política interna corporativa sobre el uso de los medios de comunicación por correo electrónico, con el fin de alinear el uso del mismo a nivel global con la operación de nuestro país. Posteriormente es aconsejable emitir un procedimiento local sobre el seguimiento del uso apropiado del programa de correo electrónico, a su vez que este sea aprobado, que sea publicado y comunicado a los mismos usuarios.
- Como primera acción, se debe validar la configuración de los puertos de salida USB para la transacción de datos desde el equipo a los dispositivos externos. Erradicar la posible fuga de información corrigiendo esta configuración de los equipos de cada usuario. Ejecutar filtros de virus, por medio de programas seguros de detección de este tipo de malware. También es recomendable generar una comunicación constante sobre la aparición de nuevos virus, y educar a los usuarios sobre el uso de los BYOD correctamente, con enfoque a la seguridad y cumplimiento de las regulaciones corporativas.
- Se debe planificar un programa de capacitación general sobre los temas de seguridad de la información, que los usuarios puedan comprender la importancia y relevancia que tiene el cuido y resguardo de las actividades de control sobre los sistemas de información. Coordinar con Recursos Humanos, el diseño de la campaña de conocimiento del tema de los aspectos de seguridad de TI y el apoyo que se requiere de los usuarios.

REFERENCIAS

Libros

Echenique, J. (2001). *Auditoría en Informática*. México D.F.: McGraw-Hill.

Delgado, X. (1997). *Auditoría Informática*. San José: Editorial Universidad Estatal a Distancia.

Muñoz C. (2002). *Auditoría en Sistemas Computacionales*. México D.F. Pearson Prentice Hall.

Tupia, M. (2010). *Administración de la Seguridad de la Información.* Lima: GRAFICAR.

Arens, A y Loebbecke, J. (1996). *Auditoría un Enfoque Integral*. 6° edición, México D.F.: Pearson Prentice Hall.

Gómez A. y Suárez C. (2009). Sistemas de información: herramienta práctica para la gestión. 3° edición. México D.F. Alfaomega Grupo Editor.

Hernández, E. (2000). *Auditoría en Informática*. 2da edición. México D.F.:CECSA.

Piattini, M. y Navarro, E. (2001). *Auditoría informática, un enfoque práctico*. 2° edición ampliada y revisada. México D.F.: Alfaomega Grupo Editor.

Otros documentos

IT Governance Institute, ITGI. (COBIT 5, 2012) COBIT@5 Control Objective for Information and Related Technologies. EE.UU.

IT Governance Institute, ITGI. (COBIT 5, 2012) COBIT@5 *para Seguridad de la Información*. EE.UU.

IT Governance Institute, ITGI. (COBIT 5, 2012) COBIT@5 Procesos Catalizadores. EE.UU.

IT Governance Institute, ITGI. (COBIT 5, 2012) COBIT@5 Implementación. EE.UU.

International Organization for Standardization. ISO/IEC 27002:2005. Information technology – Security techniques – Code of practice for information security management. EE.UU.

International Organization for Standardization. (2005) 27001:2005. Information technology – Security techniques – Information security management systems-Requirements. EE.UU.

International Organization for Standardization. (2005) ISO/IEC 27002:2005. Information technology – Security techniques – Information security management systems-Requirements. EE.UU.

Documentos electrónicos

http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3LEMA=seguridad. Recuperado el 09 de diciembre de 2014.

http://www.iso.org. Recuperado el 12 de diciembre de 2014.

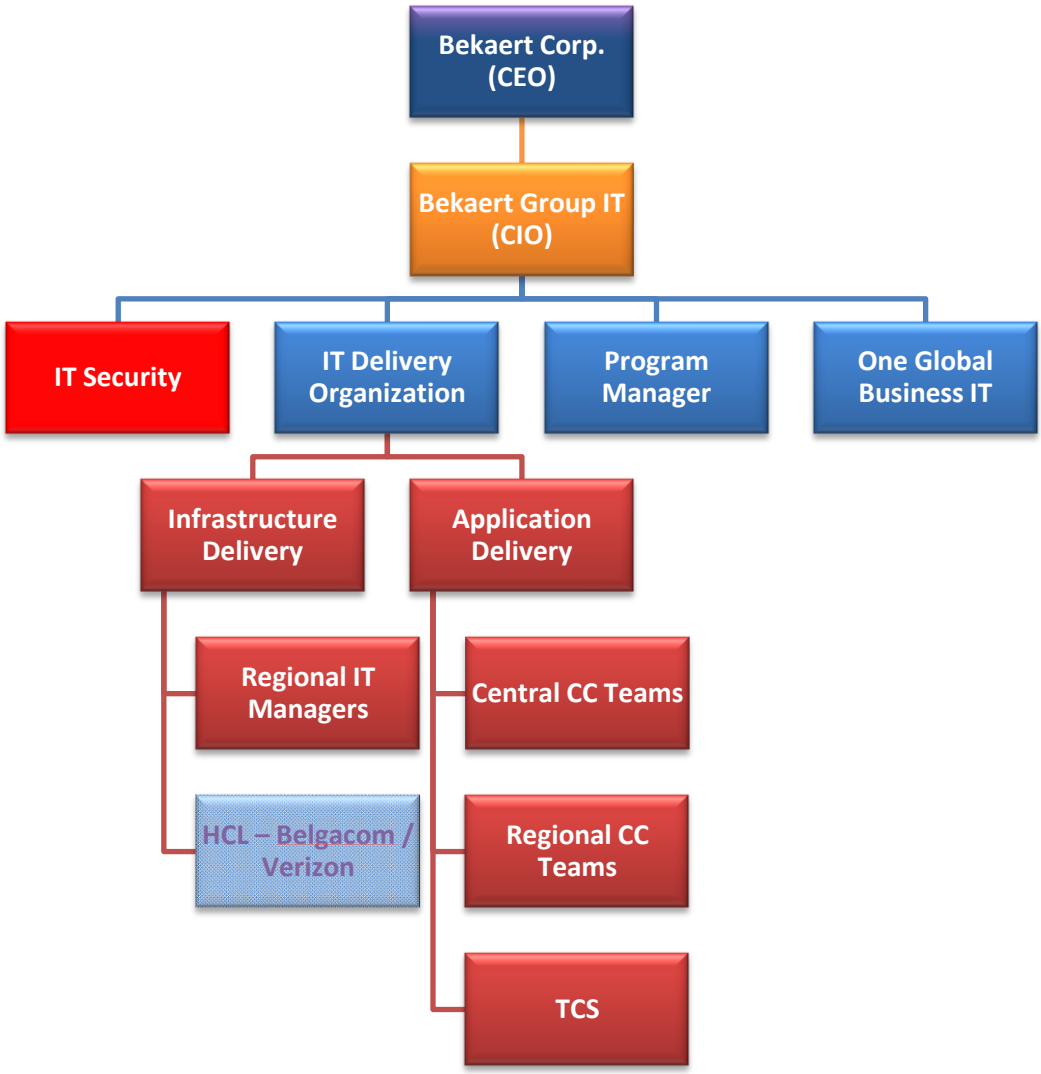
www.segurinfo.org. Prandini, P. y Szuster, R. Re-Evolucion COBIT5 2012. Recuperado de www.isaca.org/Knowledge-Center/cobit/Documents/COBIT5-and-InfoSec-Spanish.ppt el 12 de diciembre de 2014.

Riesgos de tecnología de información implicaciones y retos para la auditoría. Solano, M. Deloitte & Touche, S.A. 2013 Recuperado de http://www.ccpa.or.cr/file/mayo_2013/charlas/21-riesgos-de-tecnologia-de-informacion-implicaciones-y-retos-para-la-auditoría.pdf el 14 de marzo del 2014.

ANEXOS

Figura 1

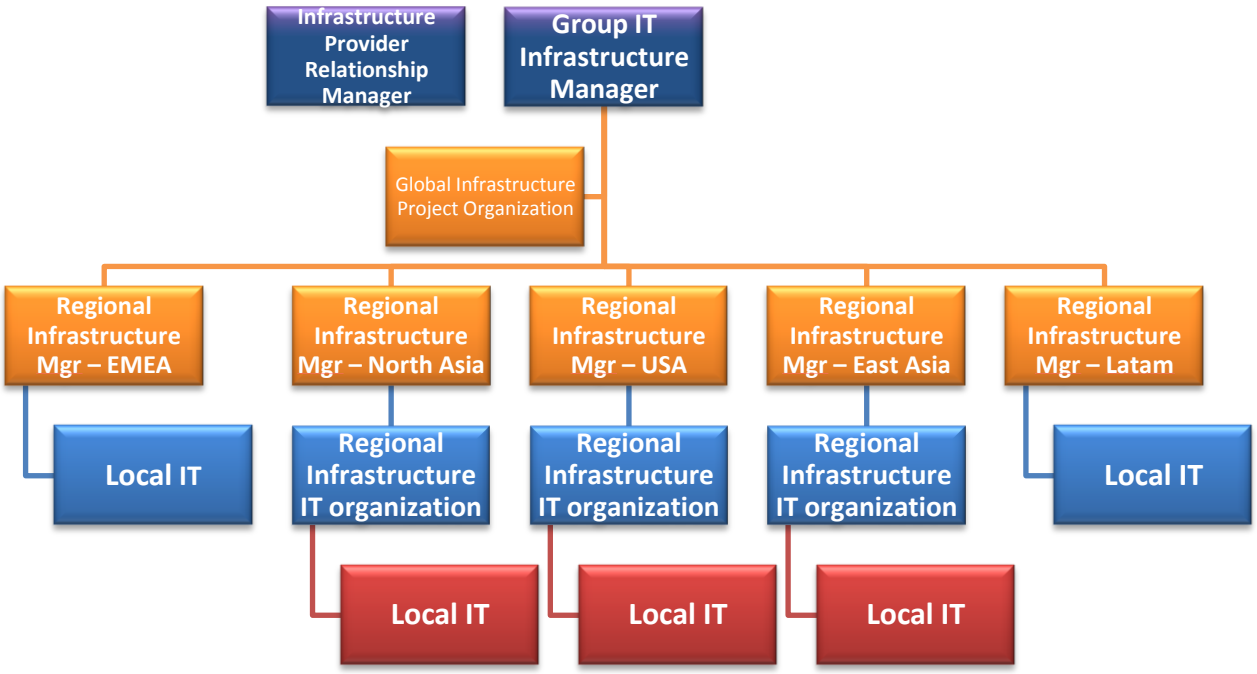
Organización TI Corporativa Global



Fuente: Bekaert Corporation, 2015

Figura 2

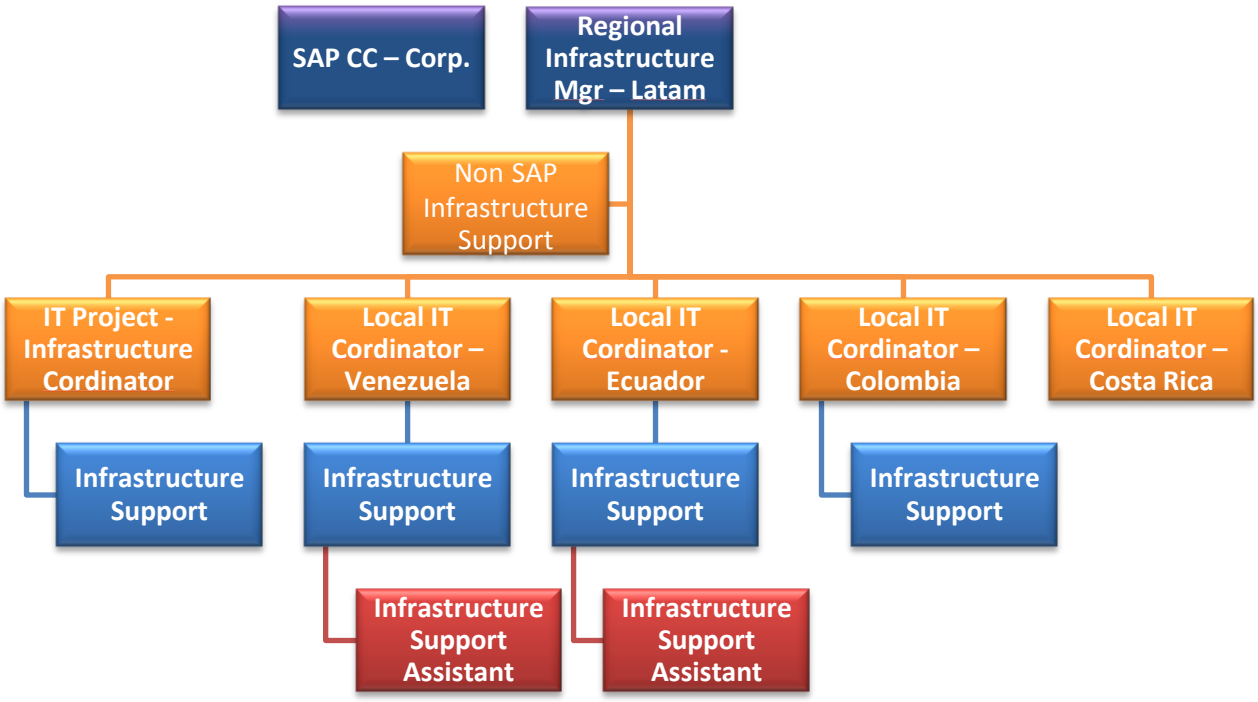
Organización Infraestructura de TI Corporativa por regiones



Fuente: Bekaert Corporation, 2015

Figura 3

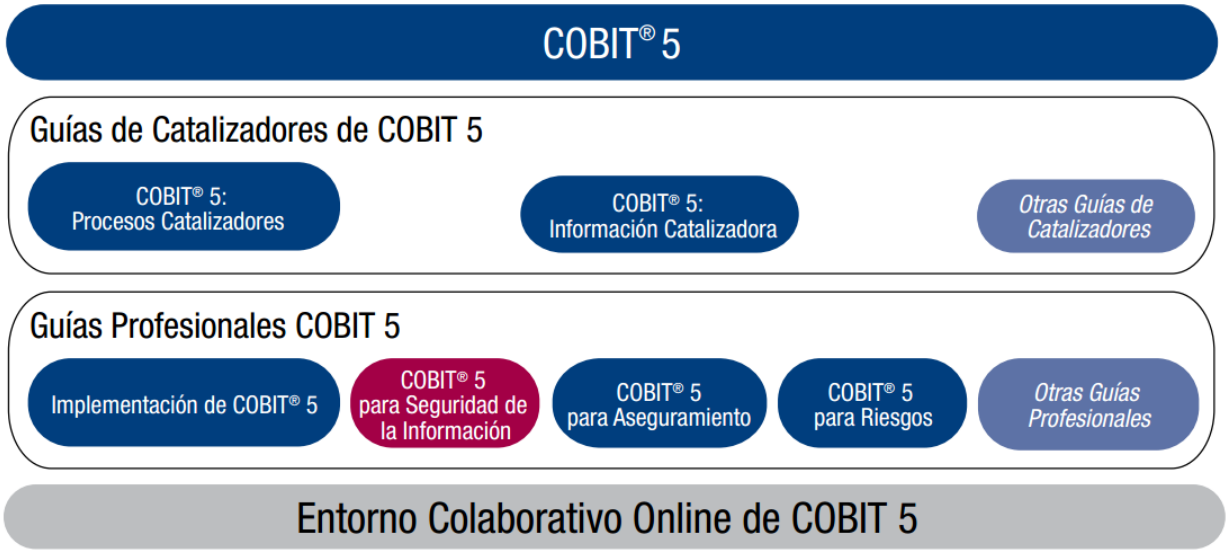
Organización Infraestructura de TI Corporativa Región de Latinoamerica



Fuente: Bekaert Corporation, 2015

Figura 4

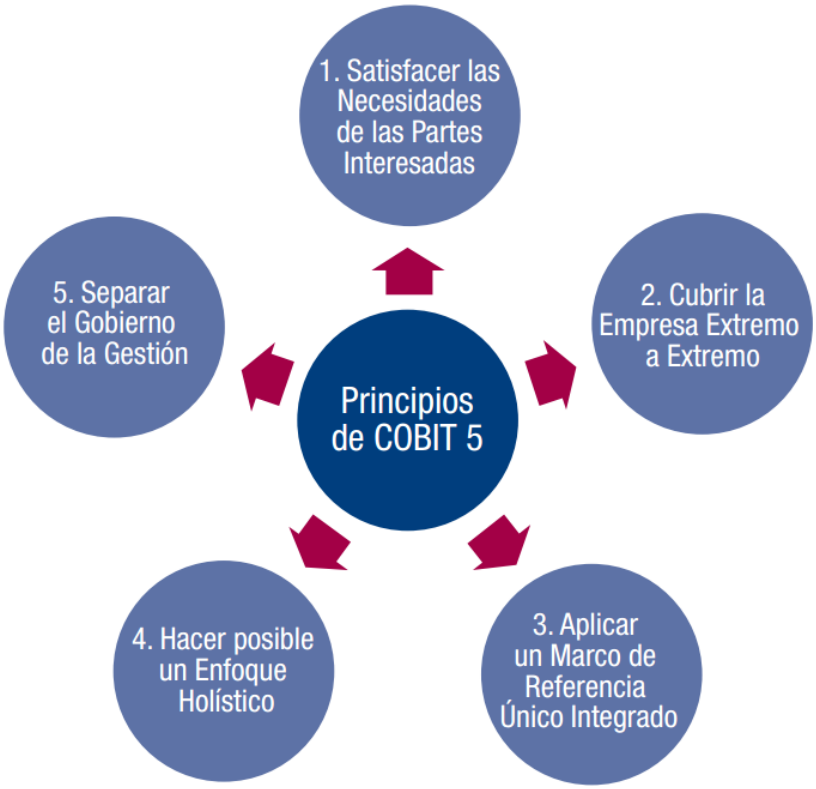
Familia de Productos COBIT 5



Fuente: IT Governance Institute, ITGI. (COBIT 5, 2012) COBIT[@]5 *para Seguridad de la Información*.

Figura 5

Principios de COBIT



Fuente: IT Governance Institute, ITGI. (COBIT 5, 2012) COBIT@5 *para Seguridad de la Información*.

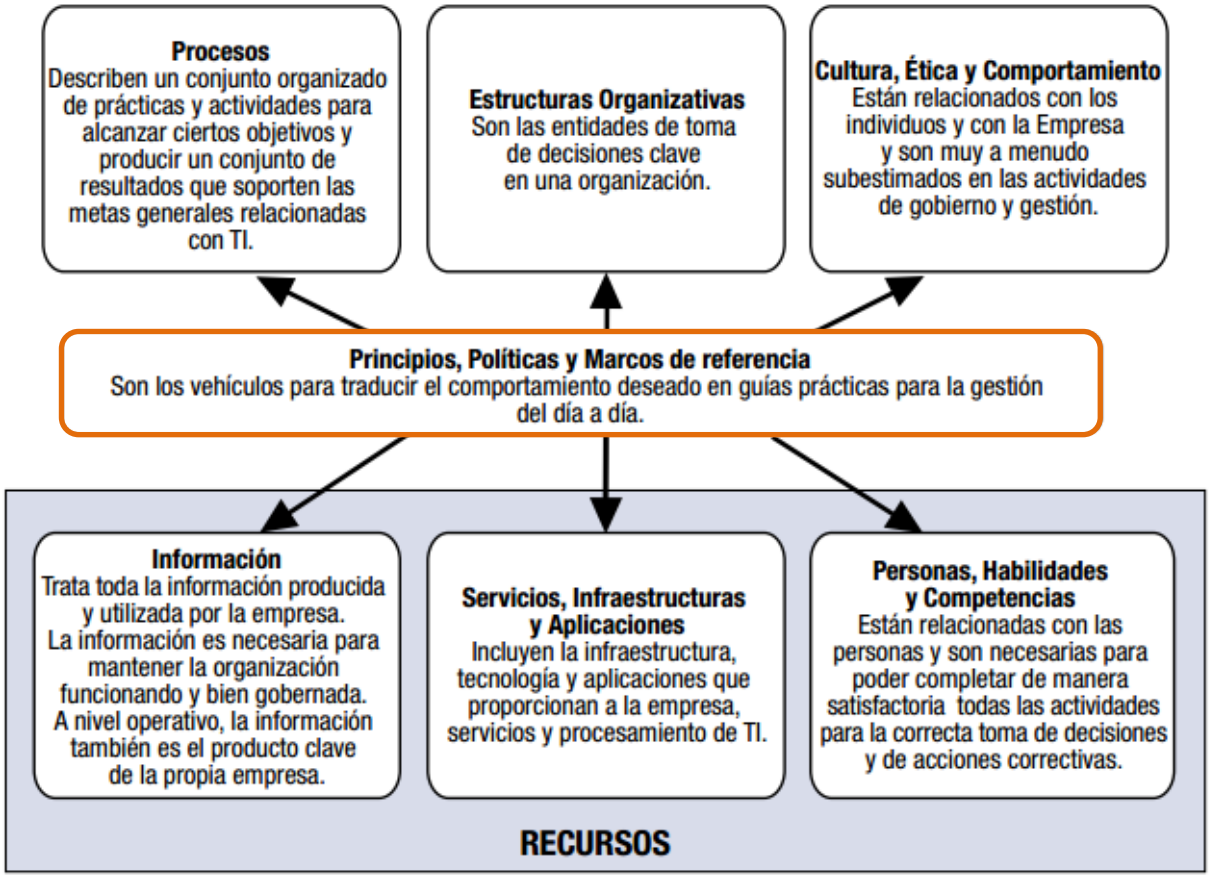
Figura 6

General de la Cascada de Metas de COBIT 5

Fuente: IT Governance Institute, ITGI. (COBIT 5, 2012) COBIT®5 *para Seguridad de la Información*.

Figura 7

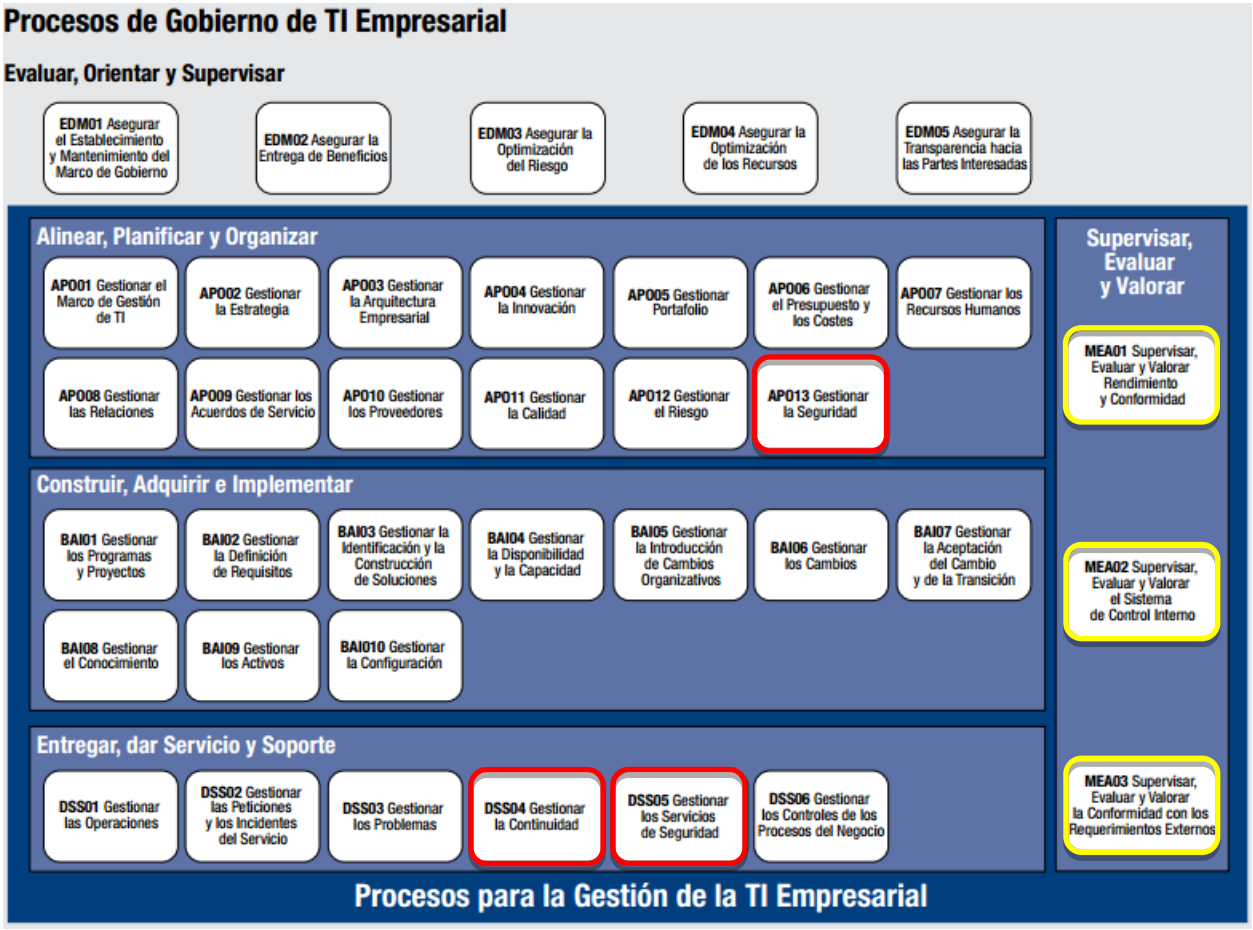
Catalizador de COBIT5: Modelo Sistémico con Interactuación de Catalizadores



Fuente: IT Governance Institute, ITGI. (COBIT 5, 2012) COBIT[@]5 *para Seguridad de la Información*.

Figura 8

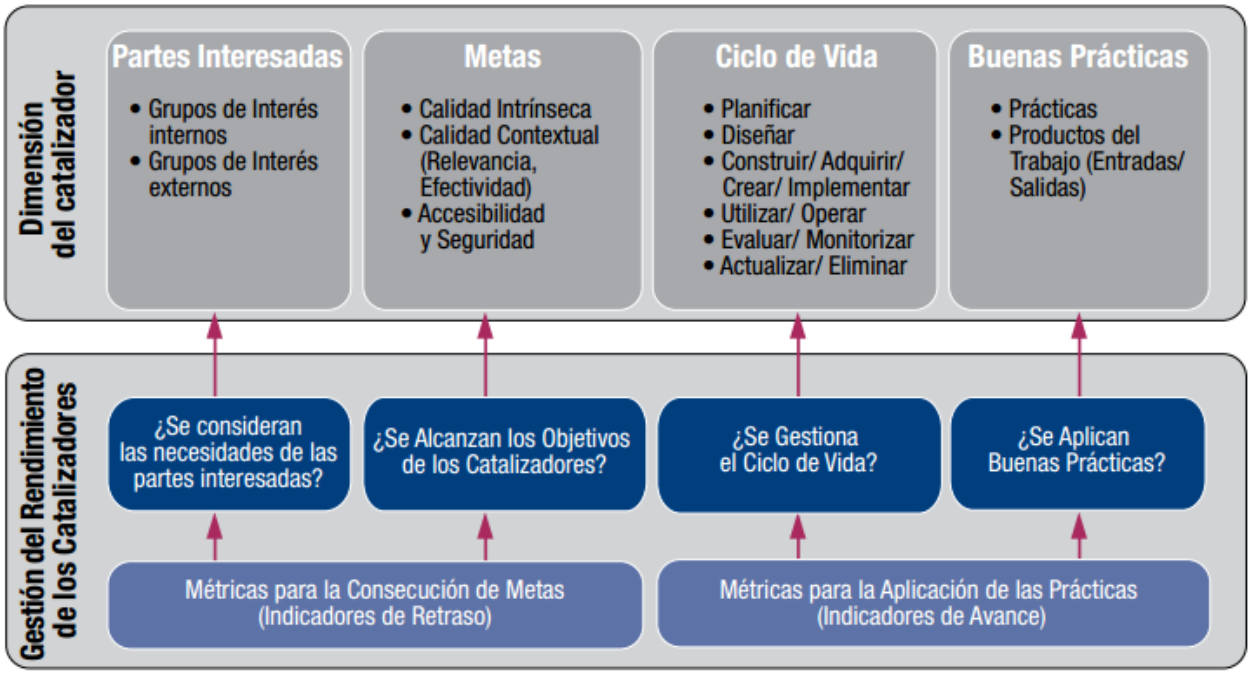
Modelo de Referencia de Procesos de COBIT 5



Fuente: IT Governance Institute, ITGI. (COBIT 5, 2012) COBIT@5 *para Seguridad de la Información*.

Figura 9

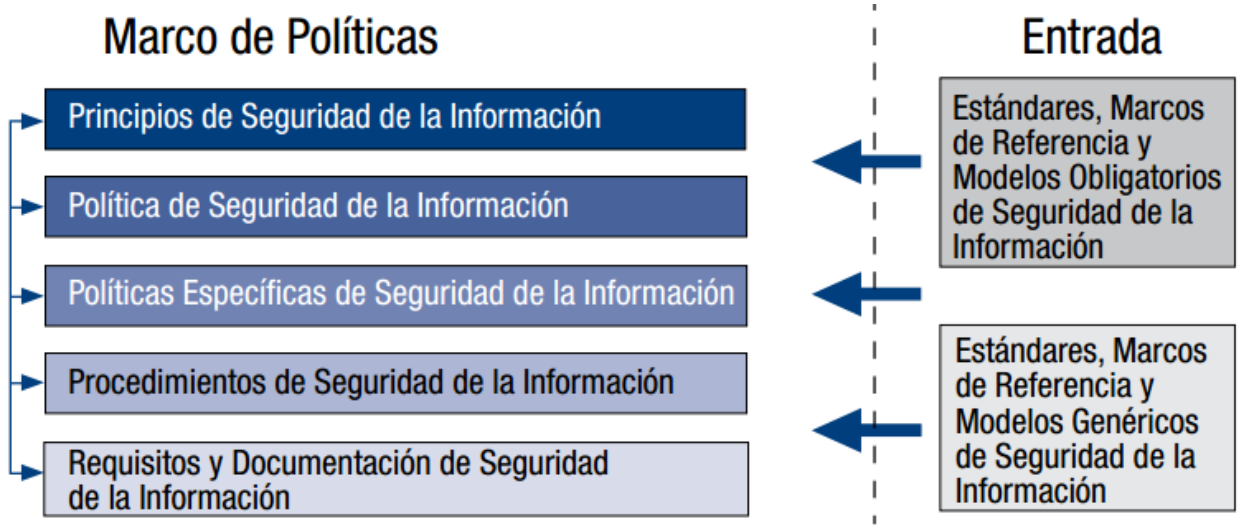
Catalizadores COBIT 5: Genéricas



Fuente: IT Governance Institute, ITGI. (COBIT 5, 2012) COBIT[@]5 *para Seguridad de la Información*.

Figura 10

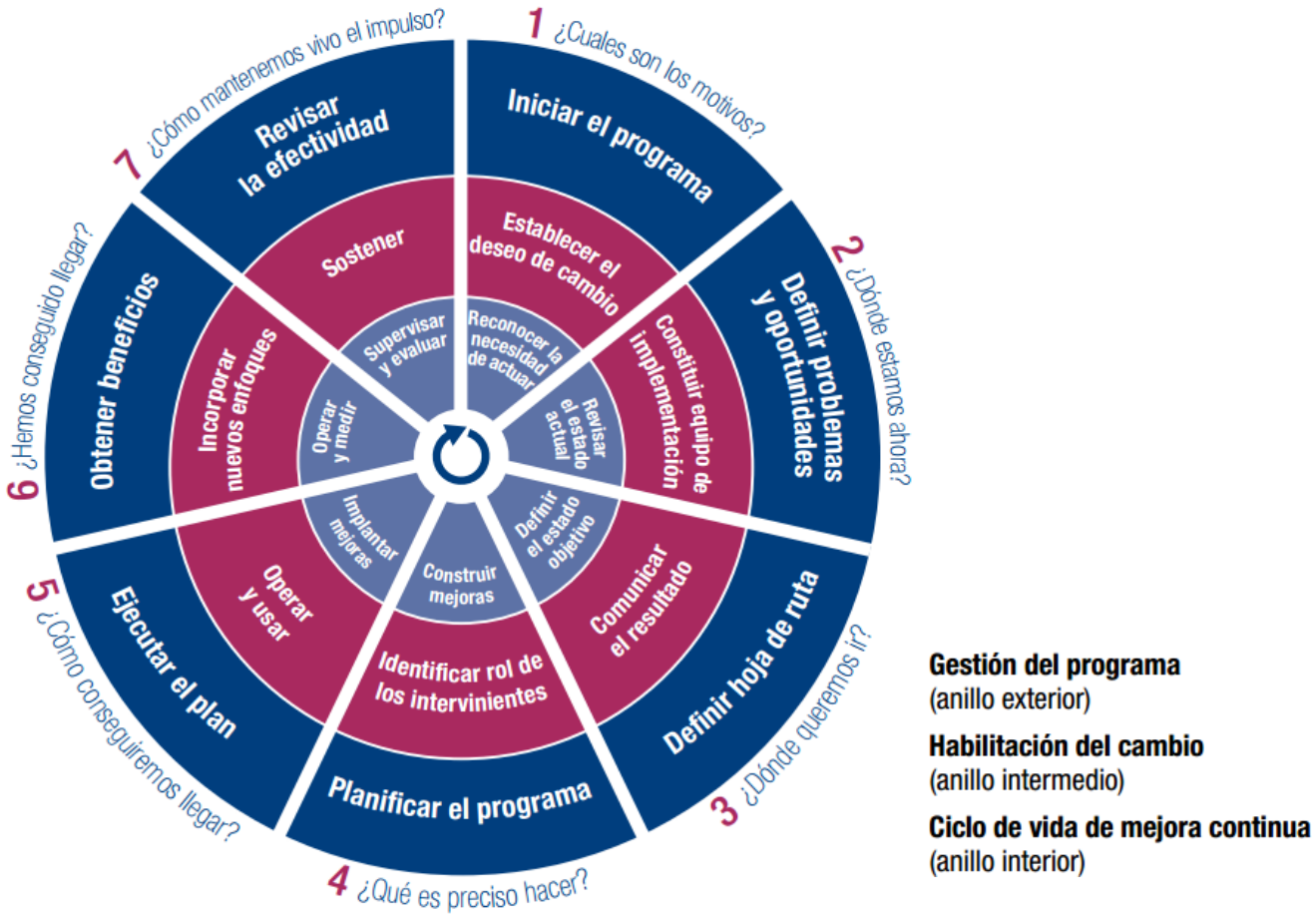
Marco de Políticas



Fuente: IT Governance Institute, ITGI. (COBIT 5, 2012) COBIT[@]5 *para Seguridad de la Información*.

Figura 11

Las siete fases de la implementación del Ciclo de Vida



Fuente: IT Governance Institute, ITGI. (COBIT 5, 2012) COBIT[@]5 *para Seguridad de la Información*.