PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO DE PROCEDIMIENTOS DE AUDITORÍA DE CUMPLIMIENTO DE LA NORMA NTP-ISO/IEC 17799:2007 COMO PARTE DEL PROCESO DE IMPLANTACIÓN DE LA NORMA TÉCNICA NTP-ISO/IEC 27001:2008 EN INSTITUCIONES DEL ESTADO PERUANO

Tesis para optar el Título de Ingeniero Informático, que presenta el bachiller:

Fernando Miguel Huamán Monzón

ASESOR: Dr. Manuel Francisco Tupia Anticona

Lima, julio de 2014

RESUMEN DEL PROYECTO DE TESIS

El presente proyecto de fin de carrera responde a la necesidad creada a causa de las normativas publicadas por la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) que declaran de uso obligatorio las Normas Técnicas Peruanas NTP-ISO/IEC 27001:2008 y NTP-ISO/IEC 17799:2007 (con fechas de publicación mayo 2012 y julio 2011 respectivamente) a una lista de empresas del estado peruano que pertenezcan y/o estén involucradas en la Administración Pública con la finalidad de establecer un modelo integral para el desarrollo de los planes de seguridad de la información de la misma.

Esta necesidad, a causa del carácter obligatorio de las normas mencionadas, es reconocida como la atención a la falta de procedimientos que permitan realizar auditorías que verifiquen el cumplimiento de la NTP-ISO/IEC 17799 como parte del proceso de cumplimiento integral de la NTP-ISO/IEC 27001 en las empresas del estado peruano.

La elaboración de estos procedimientos estarán basados en COBIT 5.0, publicado en mayo de 2012, nuevo estándar de facto para Tecnologías de Información reconocido internacionalmente.

Estos procedimientos estarán acompañados de la declaración de aplicabilidad para la norma NTP-ISO/IEC 17799 para poder definir los controles que serán establecidos e implementados por la institución, un Inventario de activos de información comúnmente relacionados con los controles presentes en la NTP-ISO/IEC 17799 y un Mapeo del marco COBIT 5.0 frente a la norma NTP 17799 identificando la correspondencia de los dominios de COBIT hacia los controles de la NTP.

INDICE

ÍNDICE DE FIGURAS Y TABLAS

FIGURAS

TABLAS

CAPÍTULO 1

1. INTRODUCCIÓN

En este capítulo se presentará lo concerniente al proyecto de fin de carrera. Se describe el entorno en el cual se encuentra el problema identificado con la finalidad de dar un primer paso en el proyecto. Se procederá luego a definir el objetivo general, acompañado por los objetivos específicos mapeados cada uno con sus resultados esperados. Para la consecución de lo mencionado se identificará las metodologías a utilizar.

También se justificará el proyecto presentando además su viabilidad. Se desplegará finalmente la lista de actividades a realizar para la obtención del producto final del presente proyecto.

2. DEFINICIÓN DE LA PROBLEMÁTICA

La Presidencia del Consejo de Ministros (PCM) del Perú autorizó en el año 2010 la ejecución de la “Encuesta de Seguridad de la Información en la Administración Pública” (ONGEI 2010a) a las instituciones de la Administración Pública que pertenecen al Sistema Nacional de Informática con la finalidad de actualizar la información técnica de dichas entidades en relación con la seguridad de la información. De las 271 entidades encuestadas solo se pudo recepcionar la respuesta de 150 (56% del total) indicando que un 30% no habían si quiera realizado una Política de Seguridad de la Información (ONGEI 2010b). Este escenario se produjo estando publicada la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 desde agosto de 2007.

Los sistemas de información de las organizaciones se enfrentan día a día con riesgos e inseguridades que se enfocan en explotar vulnerabilidades de sus activos de información poniendo en riesgo su continuidad de negocio. Los procesos que manejan datos, los sistemas y las redes son activos importantes de la organización por lo que es importante definir, realizar, mantener y mejorar la seguridad de la información, para que puedan alcanzar sus objetivos de negocio. Así como se ha convertido en una actividad importante dentro de las organizaciones, la seguridad de la información también ha suscitado muchos dolores de cabeza a los responsables en poner en acción una eficiente gestión de esta actividad.

La reciente publicación en mayo de 2012 aprobando el uso obligatorio de la NTP-ISO/IEC 27001:2008 en las entidades del estado demuestra la intención del gobierno peruano en establecer un modelo integral para el desarrollo de los planes de seguridad de la información en la Administración Pública donde la NTP-ISO/IEC 17799:2007 se suma también a este accionar.

Es necesario brindar procedimientos concretos o guías para poder realizar procesos de auditoría que tengan como objetivo corroborar la implantación de la NTP 27001 en las empresas del estado peruano (entidades listadas en la misma publicación de la norma) teniendo como base lo propuesto por la NTP 17799.

Teniendo como motivo lo mencionado anteriormente y con el objetivo en brindar apoyo en la actividad de gestionar un aspecto tan importante como es la Seguridad de Información, es que se desarrollará en este proyecto los procedimientos de auditoría para evaluar la implementación de la NTP-ISO/IEC 17799:2007, en respuesta a la motivación de poner en práctica los conocimientos obtenidos en ésta área de la informática, en beneficio de la sociedad peruana.

3. OBJETIVO GENERAL

Establecer un procedimiento de auditoría de cumplimiento para la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 en las instituciones del Estado Peruano basado en el marco COBIT 5.0, como parte del proceso de implantación de la Norma Técnica Peruana NTP-ISO/IEC 27001:2008 con la finalidad de mejorar la gestión de la seguridad de la información.

4. OBJETIVOS ESPECÍFICOS

Los objetivos específicos del presente proyecto son los siguientes:

- Determinar el procedimiento de elaboración de la declaración de aplicabilidad de la norma NTP 17799 con la finalidad de justificar la elección o exclusión de los controles sugeridos por ésta.

- Identificar los activos de información involucrados en cada control de la norma NTP 17799.

- Elaborar el mapeo del marco COBIT 5.0 frente a la NTP 17799
- Elaborar la guía metodológica para la ejecución de la auditoría de cada control contemplado en la norma NTP 17799.

5. RESULTADOS ESPERADOS

Presentamos ahora los resultados esperados asociados con cada objetivo específico presentados en el punto anterior:

- [Relacionado con Objetivo Específico 1] - Procedimiento y estructura (plantilla) de la declaración de aplicabilidad para la norma NTP ISO/IEC 17799 para poder definir los controles que serán establecidos e implementados por la institución.

- [Relacionado con Objetivo Específico 2] - Inventario de activos de información comúnmente relacionados con los controles presentes en la NTP ISO/IEC 17799.

- [Relacionado con Objetivo Específico 3] - Mapeo del marco COBIT 5.0 frente a la norma NTP 17799 identificando la correspondencia de los dominios de COBIT hacia los controles de la NTP.

- [Relacionado con Objetivo Específico 4] - Guía de procedimientos de auditoría de la norma NTP 17799.

6. ALCANCE Y LIMITACIONES

El proyecto de fin de carrera pertenece al área de Tecnologías de Información de Ingeniería Informática (áreas según ACM), especificada en el tópico de Auditoría.

Planteará unos procedimientos para realizar auditoría a las empresas del estado peruano en relación a la Gestión de Seguridad de la información.

Se logrará un mecanismo para verificar el cumplimiento de la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 puesto que no existe registro alguno en instituciones oficiales del estado peruano como el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), Contraloría General de la República (CGR). Asimismo para verificar el cumplimiento de la recientemente NTP-ISO/IEC 27001:2008 aprobada el 25 de mayo de 2012 por la Presidencia de Consejos de Ministros a través de la ONGEI.

Se ejecutará la aplicación del marco COBIT 5.0 como nuevo estándar de facto para Tecnologías de Información, debido a su gran integración con Val IT y Risk IT, ITIL y BIMS, marcos de la Information Systems Audit and Control Association (ISACA), todos reconocidos a nivel internacional.

Este proyecto no tiene como fin implementar alguna otra norma o marco en relación a la Gestión de Seguridad de Información ni para las empresas públicas del estado peruano ni mucho menos para empresas privadas.

La implementación de control y/o un Sistema de Gestión de Seguridad de la Información según lo estipulado en la NTP-ISO/IEC 27001:2008 no son puntos que se pretenden alcanzar con el presente proyecto de fin de carrera.

7. HERRAMIENTAS Y MÉTODOS

A continuación se detallará las herramientas y métodos a utilizarse tanto para el proyecto como para el producto, especificando además los procedimientos para cada uno respectivamente.

RESULTADO ESPERADO	HERRAMIENTA
Procedimiento y estructura (plantilla) de la declaración de aplicabilidad para la norma NTP-ISO/IEC 17799:2007 para poder definir los controles que serán establecidos e implementados por la institución	✓ NTP-ISO/IEC 17799:2007 ✓ PDCA ✓ MS Word
Inventario de activos de información comúnmente relacionados con los controles presentes en la NTP-ISO/IEC 17799:2007.	✓ NTP-ISO/IEC 17799:2007 ✓ PDCA ✓ MS Word
Mapeo del marco COBIT 5.0 frente a la norma NTP-ISO/IEC 17799:2007 identificando la correspondencia de los dominios de COBIT hacia los controles de la NTP.	✓ COBIT 5 ✓ NTP-ISO/IEC 17799:2007 ✓ MS Excel
Guía de procedimientos de auditoría de la norma NTP-ISO/IEC 17799:2007.	✓ COBIT 5 ✓ MS Word

7.1. Métodos y metodologías

7.1.1. PDCA

La metodología Plan-Do-Check-Act o también conocida como Ciclo de Deming. Se ha optado por esta metodología puesto que desde hace más de 50 años es la más utilizada en lo concerniente a auditorías y también en proyectos que optan por realizar mejoras continuas y de calidad.

El ciclo de Deming realiza cuatro pasos, que, al llegar al último de estos vuelve a iniciarse para poder de esta manera dar lugar a escenarios de mejoras. Los cuatro pasos son los siguientes:

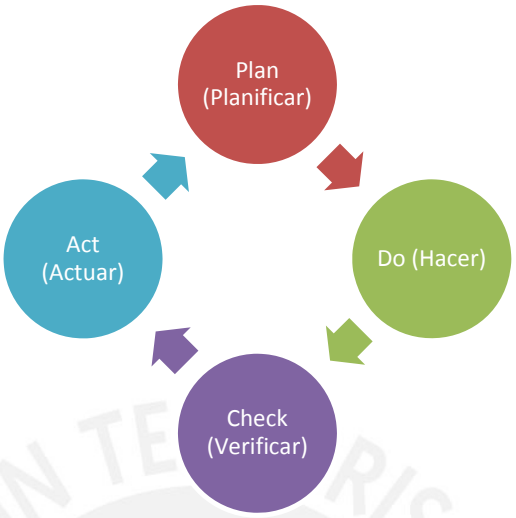


Figura 1: Metodología PDCA o Ciclo de Deming

A. Plan (Planificar): Implica la identificación del problema, la recopilación de datos y el análisis del mismo que nos permitirá elaborar un plan de trabajo que busque su solución.

   Para el proyecto presentado se planificarán las actividades para:

   a. Determinar el acta de aplicabilidad SOA de la ISO 27002 en una empresa del estado regulada por las NTP 17799 y NTP 27001

   b. Realizar los inventarios de activos y controles sugeridos según la ISO 27002.

   c. Verificar cada uno de los controles que el auditor deberá revisar en una auditoría de controles.

B. Do (Hacer): Se realiza el desarrollo del plan generado en la etapa anterior.

   En función del presente proyecto se realizará:

   a. Reconocimiento, compilación y documentación de los activos relacionados con los controles de la norma NTP-ISO/IEC 17799

   b. Diseñar la relación entre COBIT 5.0 y el código de buenas prácticas ISO 27002.
      i. Documentación del mapeo realizado.

   c. Bosquejo de la elaboración de procedimientos de auditoría para todas los controles de la NTP-ISO/IEC 17799:2007.

d. Detalle de resoluciones en ONGEI acerca de Seguridad de Información.

C. Check (Verificar): Se revisan y analizan los resultados de manera que se pueda obtener una medida de la efectividad de la solución y una retroalimentación de lo que se podría mejorar.

   Se revisarán los documentos generados con el asesor del proyecto, además de revisar nuevas leyes nombradas por la ONGEI para el estado peruano. Se documentará estas revisiones para su posterior uso en la siguiente etapa.

D. Act (Actuar): Efectuar las correcciones que se adquirieron en la etapa anterior.

   Se realizarán las correcciones necesarias en los documentos generados en las etapas anteriores. De ser necesario, a causa de una nueva normativa en relación a Seguridad de Información, se procederá a la respectiva adecuación de los documentos.

7.2. Herramientas

7.2.1. COBIT

COBIT es un marco de gobierno de las tecnologías de información que proporciona una serie de herramientas para que se pueda conectar los requerimientos de control con los aspectos técnicos y los riesgos del negocio. También permite el desarrollo de las políticas y buenas prácticas para el control de las tecnologías en toda la organización. Además brinda ayuda a las organizaciones a incrementar su valor a través de las tecnologías, y permite su alineamiento con los objetivos del negocio. En su reciente versión (publicada el 10 de abril por ISACA) COBIT 5.0 integra varios marcos de ISACA (Val IT y Risk IT, ITIL y BIMS).

Se utilizará COBIT 5.0 pues ayuda a crear un valor óptimo de TI por mantener un equilibrio entre la obtención de beneficios y la optimización de los niveles de riesgo y el uso de los recursos. Permite también que la información y la tecnología relacionada sean gobernadas y gestionadas de manera integral para toda la empresa, abrazando de principio a fin el negocio y áreas funcionales, teniendo en cuenta los intereses de las partes interesadas internas y externas.

COBIT 5.0 presenta 5 principios:

A. Marco Integrador: Capacidades para facilitar el direccionamiento de los usuarios con prácticas y referencias de terceras partes.

B. Conductores de valor para los interesados: Las necesidades de los interesados deben traducirse a una estrategia de acción de la empresa.

C. Enfoque al Negocio y su contexto para toda la organización: Se refiere al Gobierno y Gestión de TI empresarial y las tecnologías relacionadas cubriendo todas las funciones y procesos dentro de la empresa.

D. Estructurado de manera separada para el Gobierno y la Gestión: Los procesos de Dirigir, Evaluar y Supervisar están a cargo del Gobierno. La Gestión se encargará de Planear, Construir, Ejecutar y Supervisar

E. Fundamentado en facilitadores: Provee una forma común, simple y estructurada para el tratamiento de los facilitadores y dar comodidad para gestionar sus completas interacciones.

Al llevar a cabo estas actividades, nos garantizamos la generación de procedimientos eficientes para la auditoria en relación a Gestión de Seguridad de la Información.

Más detalle de este marco de negocio para Tecnologías de Información se puede ver en el punto **3.1. COBIT** del **CAPITULO 2** del presente documento.

8. JUSTIFICACIÓN Y VIABILIDAD

Al publicarse el 25 de mayo de 2012 la normativa por parte de la Presidencia del Consejo de Ministros (mediante la ONGEI) que establece el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 27001:2008 y teniendo como antecedente que el año anterior (julio de 2011) se promulgó como fecha límite el 31 de diciembre de 2012 para que las empresas del gobierno peruano implementen el plan de seguridad de la información basado en lo dispuesto por la NTP-ISO/IEC 17799:2007; se encontró conveniente atender el vacío que estas dos normativas han generado en pos del establecimiento de un modelo integral para el desarrollo de los planes de seguridad de la información en la Administración Pública. Este vacío mencionado se identificó como la falta de procedimientos que permitan realizar auditorías que verifiquen el cumplimiento de la NTP-ISO/IEC 17799 como parte del proceso de cumplimiento integral de la NTP-ISO/IEC 27001.

El auditor para sustentar su labor profesional en relación a la evaluación de un Sistema de Gestión de Seguridad de la Información, requiere examinar las evidencias, a través de distintos métodos y/o técnicas de aplicación de forma paralela.

La propuesta de este proyecto de fin de carrera no solo es el desarrollo de guías de auditoría en base a las Normas Técnicas Peruanas antes mencionadas, sino también basarse e incluir normas y marcos de control internacionalmente reconocidos como estándares *de facto* para auditoría de sistemas y tecnologías de información tales como ISO 27001, ISO 27002 y COBIT 5.0 garantizando la calidad y eficacia de la ejecución de las actividades del proceso evaluativo. Adicionalmente

se pretende establecer una base común en la emisión de opinión sobre la correctitud de los Sistemas de Gestión de Seguridad de la Información.

La viabilidad de los procedimientos contenidos en las guías que serán desarrolladas en el presente proyecto de tesis abarcar a las empresas del estado peruano que estén en la lista de instituciones obligadas a cumplir las normas regulatorias emitidas por la ONGEI: NTP-ISO/IEC 17799:2007 y NTP-ISO/IEC 27001:2008.

Considerando otros aspectos sobre viabilidad del proyecto tenemos:

- Técnica: Estos procedimientos podrán ser viables en una actividad de auditoría de control de seguridad de la información siempre y cuando el profesional que la ejecute tenga los conocimientos del marco de control COBIT 5.0 así como su terminología relacionada.

- Temporal: Se debe tener en cuenta que este proyecto podrá ser utilizado mientras estén en vigencia de las normas técnicas NTP-ISO/IEC 27001:2008 y NTP-ISO/IEC 17799:2007 y la declaración de su obligatoriedad.

- Económica: Dependerá mucho de los controles que apliquen las instituciones del estado peruano para saber cuánto le costaría implementarlos. Además se considerará un gasto adicional si la empresa estatal peruana decide certificarse en la norma ISO 27001 (este punto es opcional dado que la NTP-ISO/IEC no indica que sea obligatorio dicha certificación).

Se debe tener en cuenta, además, que las empresas a las que se realizará la auditoría de control deberán tener documentados sus procesos para poder, consecuentemente aplicando la norma, reconocer los activos que tienen que someterse a protección.

CAPÍTULO 2

1. INTRODUCCIÓN

El presente capítulo tiene por objetivo destacar tres ítems importantes para el desarrollo del proyecto de fin de carrera como son: el marco conceptual en el cual se desenvuelve, la revisión del estado del arte y la discusión de la misma. Para finalizar, se exhibe la bibliografía consultada en la elaboración de este capítulo.

2. MARCO CONCEPTUAL

Se presentará a continuación, tres grupos de conceptos relacionados al proyecto de fin de carrera que se considera necesario para su correcto entendimiento y que marca la postura conceptual que se ha tomado para su desarrollo. Estos tres grupos son: De Auditoría, De Seguridad y De Riesgos.

2.1. Conceptos de auditoría

En esta sección del documento se darán los conceptos de auditoría que se manejaran para el desarrollo del proyecto de fin de carrera.

2.1.1. Tecnologías de Información

La Tecnología de Información es un dispositivo para transmitir, manipular, analizar o explotar información, en el cual una computadora digital procesa información integral a comunicaciones de usuarios y tareas de decisión (Huber 1990).

La IT Governance Institute define un servicio de tecnología de información es una provisión diaria de aplicaciones de tecnología de información y soporte para su uso, incluyendo help desk, provisión y movimiento de equipos, y autorizaciones de seguridad. Además define una aplicación de tecnología de información como una funcionalidad electrónica que congrega partes de procesos de negocio con soporte de tecnología de información (ITGI 2008).

Morton definió TI como un ente que comprende 5 componentes básicos: computadoras, tecnología de comunicaciones, estaciones de trabajo, robótica y circuitos de computadoras (Morton 1988).

Al realizar un compilado en los conceptos mencionados, podemos definir a una tecnología de información como un servicio relacionado que se usa en la organización para el logro de sus objetivos de negocio, tanto dentro de de ella como en sus actividades de interrelaciones con otras organizaciones.

También podemos decir que son los sistemas de información (sistemas que soportan procesos relacionados al manejo de la información en las organizaciones), el hardware de computadoras, redes y comunicaciones, así como el software de base (sistemas operativos, servidores proxy, manejadores de bases de datos, servidores web, etc.)

2.1.2. Gobierno de Tecnologías de Información

Responsabilidad del comité de dirección y de los ejecutivos. Es una parte integral del gobierno de la organización y consiste en el liderazgo y las estructuras y procesos organizativos que aseguran que las Tecnologías de Información de la organización sostienen y extienden la estrategia y los objetivos de la organización (ITGI 2003).

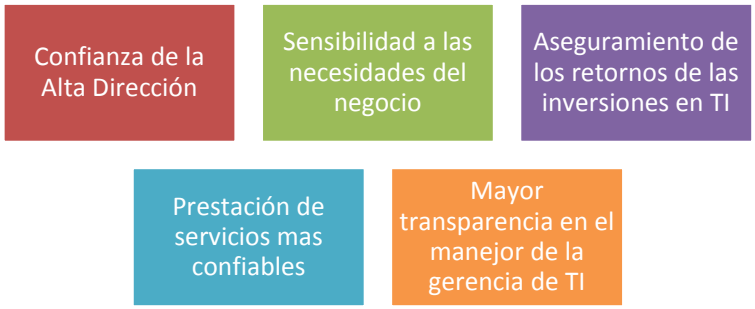


Figura 2: Beneficios más destacados de un Gobierno de TI (ISACA 2010)

La gestión de las Tecnologías de la Información está más orientada al abastecimiento interno de TI y con una ubicación temporal en el presente, el Gobierno de las Tecnologías de Información es más amplio ya que además pretende atender las demandas externas (de los clientes) y en un espacio temporal futuro. Así, la gestión se concentraría en administrar e implementar las estrategias en el día a día, mientras que el gobierno se encargaría de establecer dichas estrategias junto con la política y la cultura de la organización.

Cabe resaltar, añadiendo a lo expuesto anteriormente, que Allen define Gobierno de Tecnologías de Información como la acción de "fijar expectativas claras para la conducta (comportamiento y acciones) de la entidad que está siendo gobernada, y dirigir, controlar e influenciar fuertemente dicha entidad para cumplir estas expectativas" (Allen 2005).

El Gobierno de Tecnologías de Información tiene como objetivo principal llevar a cabo proyectos de implementación y uso de Tecnologías de Información y/o Comunicaciones como soporte a las actividades críticas y que de algún modo le brinde a la Alta Dirección la garantía de que la infraestructura tecnológica que tiene la organización va a permitir lograr los objetivos de negocio.

Es una estructura de relaciones y procesos que brinda dirección a la empresa para lograr los objetivos de negocios con una adecuada implementación de los procesos de TI en su interior, haciendo que las inversiones en TI retornen valor, logrando gestionar adecuadamente los riesgos de TI, entre otras metas.

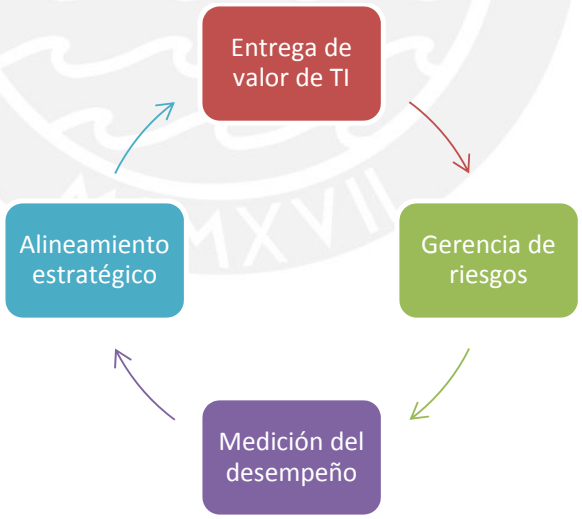


Figura 3: Estructura de relaciones en el Gobierno de TI

Definiendo cada uno de estos aspectos de esta manera (Tupia 2011):

- ✓ Alineación estratégica: alinear la tecnología a los objetivos organizacionales, para que respondan como reales soportes.

- ✓ Gestión de riesgos: el uso de TICs trae consigo una serie de riesgos a los procesos en donde están brindando soporte. La gestión de riesgos permitirá identificarlos, manejarlos y reducir el impacto que presentarían sobre los procesos mismos y los activos de información involucrados.

- ✓ Entrega de valor: optimizar las inversiones de TI.

- ✓ Medición del desempeño: monitorear los proyectos, procesos y la función misma de TI, evaluando su idoneidad – en relación con los objetivos de negocio – con métricas pertinentes

Con lo desarrollado anteriormente, podemos concluir que el Gobierno de Tecnologías de Información institucionaliza las buenas prácticas para asegurar que la TI respalda los objetivos del negocio. Con los mismos fines existen muchas buenas prácticas internacionales que ayudarán a la organización a dirigir aspectos específicos sobre estrategia, entrega de valor, prestación de servicios, gestión de riesgos y seguridad de información. Estos son:

- ✓ COBIT 5.0: estándar *de facto* para alinear el Gobierno de TI al gobierno corporativo. También es herramienta clave para la auditoría de TI.

- ✓ ISO/IEC 27001: orienta a las empresas en la aplicación y mantenimiento de programas de seguridad de información, viéndose éstos reflejados en el establecimiento de los sistemas de gestión de seguridad de información.

- ✓ ITIL: principios básicos de la estrategia, diseño, gestión y mejora continua del proceso de prestación de servicios de tecnología.

- ✓ ValIT: orienta las inversiones de TI de tal manera que se capitalicen en mayor grado.

- ✓ RiskIT: marco para la identificación, análisis y tratamiento de riesgos de Sistemas de Información y de Tecnologías de Información.

- ✓ ISO/IEC 38500: facilita las bases para la evaluación objetiva del Gobierno de Tecnologías de Información.

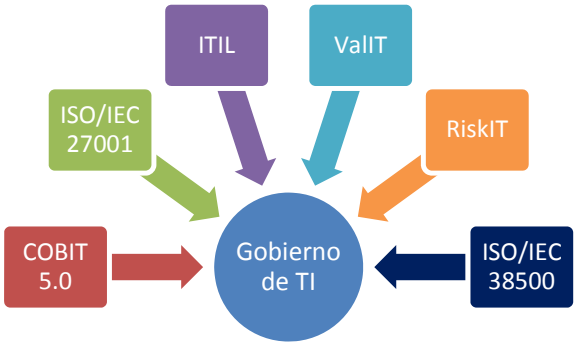


Figura 4: Buenas prácticas en Gobierno de Tecnologías de Información

2.1.3. Auditoria

La auditoría es la actividad que consiste en emitir una opinión profesional objetiva por parte de un especialista, sobre si el sujeto sometido a análisis (sea éste un sistema, proceso, producto, estructura organizacional, entre otros) cumple las condiciones que le han sido prescritas y presenta la realidad que pretende reflejar (Piattini y del Peso 2001: 4).

Paulk y otros indicaron que Auditoría es una evaluación independiente de un resultado o conjunto de resultados, con la finalidad de determinar la conformidad con las especificaciones, estándares, acuerdos contractuales (1993).

Así mismo, la ISO 19011:2002 indica que es un proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios de auditoría (ISO 2002).

Cabe resaltar que la Auditoría es una actividad que se desenvuelve, dentro de la empresa o para el sujeto que va a sufrir la auditoría, de manera independiente; que implica una opinión, profesional y especializada, sobre el estado del sujeto de auditoría; y que procura la introducción de mejoras dentro de la organización.

En el Perú, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual define la Auditoría, en la NTP-ISO/IEC 12207:2006 (INDECOPI 2006), como el proceso para determinar el cumplimiento con los requerimientos, planes y contrato, según aplique. Además se indica que este proceso puede ser empleado por cualquiera de las dos partes, donde una de ellas (la auditora) audita los productos software o actividades de la otra parte (la auditada).

2.1.4. Criterio

Son procedimientos, buenas prácticas o políticas que son utilizadas por el profesional a cargo de la actividad de auditoría para comparar la información recopilada en la misma. Son requerimiento contra los que se hace esta comparación y que pueden ser estándares internacionales, normas, requerimientos organizacionales específicos, y requerimientos legales o regulatorios.

Figura 5: Criterios de Auditoria

2.1.5. Evidencia

En auditoría, se refiere a los registros, declaraciones de hechos, código, pruebas o cualquier otra información que son pertinentes para los criterios de auditoría y que son verificables.

La evidencia de la auditoría puede ser cualitativa o cuantitativa.

Es cualquier información usada por el auditor para establecer si el objeto o los datos que están siendo auditados, cumplen con los criterios establecidos y así puede sustentar las conclusiones a las que llega y las recomendaciones que brindará más adelante.

2.1.6. Hallazgo

Un hallazgo de auditoría es el resultado de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoría.

Los hallazgos pueden indicar la conformidad o no conformidad con los criterios de auditoría y reportar oportunidades de mejora para la organización.

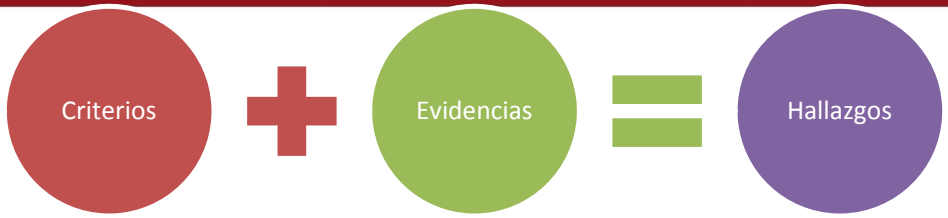


Figura 6: Concepto de Hallazgos de Auditoria

2.2. Conceptos de Seguridad

A continuación se presentará los conceptos relacionados a Seguridad como son: activo, seguridad de la información, amenaza y vulnerabilidad.

2.2.1. Activo

Elemento impreso o digital que contenga información, así como todo sistema - conformado por software, hardware y su documentación pertinente - que cree, maneje y procese información para una organización; también se puede incluir a la infraestructura tecnológica donde se desenvuelven dichos sistemas. Se considera activo esté o no registrado contablemente (Tupia 2010: 21)

2.2.2. Seguridad de la Información

La ISO/IEC 27000:2009 define la Seguridad de Información como la preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas. (ISO 2009). También amplia el concepto añadiendo que es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales.

Es necesario entender también a la Seguridad de Información como el conjunto de procesos y actividades que permiten mantener libre de peligros y daños por accidente o ataque a los activos de información que forman parte de una organización (BOSWORTH, KABAY y WHYNE 2002)

Muy importante es diferenciar seguridad de tecnologías de información y la seguridad de información: la seguridad de TI se encarga en particular, de la protección tecnológica y es administrada desde un nivel operativo por las áreas de sistemas de la mayoría de empresas.

La seguridad de información va más allá ocupándose de riesgos, beneficios, buen uso, procesos y actividades involucradas con la información y los activos relacionados a ella, impulsados por la Alta Dirección empresarial (Tupia 2010: 21)

2.2.3. Amenaza

Una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización (ISO 2004).

Son todas las actividades, eventos o circunstancias que pueden afectar el buen uso de un activo de información dañándolo y no permitiendo que brinde soporte a algún proceso, perjudicando directamente la consecución de los objetivos de negocio (Tupia 2010).

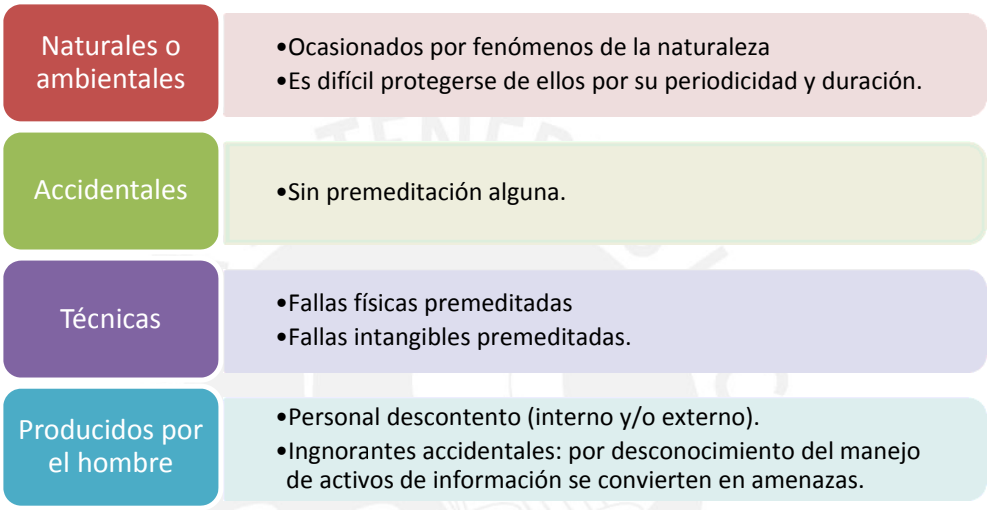


Figura 7: Tipos de amenazas

2.2.4. Vulnerabilidad

La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas. (ISO 2004)

Es una característica inherente al activo de información, siendo el grado de susceptibilidad a verse afectado por una amenaza. Los activos deben ser sometidos a pruebas para comprobar la presencia de vulnerabilidades en ellos y medir su gravedad.

Existen herramientas (software) que permiten diagnosticar y observar de forma detallada los activos para así detectar las vulnerabilidades. Esta actividad es conocida por ser hecha por peritos en materia de seguridad.

Se puede imputar a la ausencia de controles o a su deficiente establecimiento como las principales causas de vulnerabilidades sobre los activos de información (Tupia 2010).

2.3. Conceptos de Riesgos

Se requiere conocer ciertos conceptos sobre el área de Riesgos, por lo que describiremos los siguientes conceptos para el proyecto de fin de carrera.

2.3.1. Riesgo

Potencial de que una amenaza (externa o interna) explote una vulnerabilidad de uno o varios activos ocasionando daño a la organización. Su naturaleza puede depender de aspectos operativos, financieros, regulatorios (legales) y administrativos (ISO 2008).

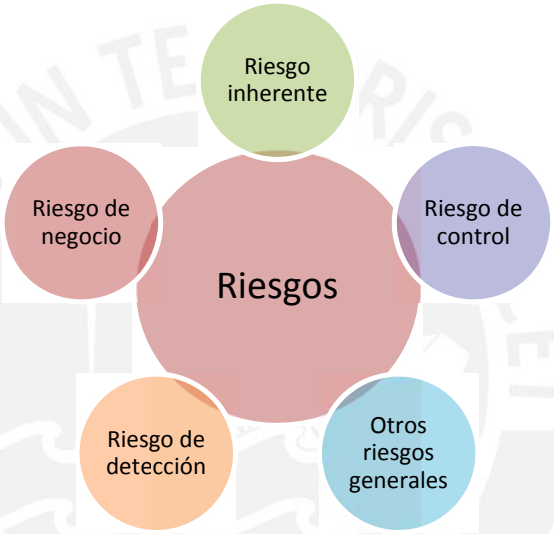


Figura 8: Tipos de Riesgos (ISACA 2011)

Un estándar australiano señala que es cualquier impedimento, obstáculo, amenaza o problema que pueda impedirle a la empresa que alcance un objetivo. Se puede ver también como la posibilidad de sufrir un daño o pérdida. Se mide en términos de impacto y probabilidad de ocurrencia. Puede tener un impacto positivo o negativo. (SA 2004)

Es la probabilidad de que una amenaza se materialice explotando una vulnerabilidad sobre un activo, provocando un impacto negativo sobre él. El proceso de identificación y evaluación de riesgos – y el de clasificación de activos – permite determinar que tan expuestos se encuentran los activos de información a ataques por la presencia de vulnerabilidades propias o inherentes a la actividad de la organización.

2.3.2. Control

El control es un proceso por el cual la administración verifica si lo que ocurre concuerda con lo que supuestamente debe ocurrir. Permite que se realicen los

ajustes o correcciones necesarias en caso se detecten eventos que escapan a la naturaleza del proceso.

Es una etapa primordial en la administración, pues, por más que una empresa cuente con magníficos planes, una estructura organizacional adecuada y una dirección eficiente, no se podrá verificar la situación real de la organización si no existe un mecanismo que verifique e informe si los hechos van de acuerdo con los objetivos. (ISO 2005).

Figura 9: Características generales de los controles.

Son las políticas, procedimientos, prácticas y estructuras organizacionales para reducir riesgos y que además proveen cierto grado de certeza de que se alcanzarán los objetivos de negocio.

2.3.3. Impacto

Medida de las pérdidas que se podrían experimentar al explotar una vulnerabilidad de uno o varios activos en nuestra organización.

Su cálculo es importante en la Gestión de Riesgos (conjunto de actividades que permite identificar, cuantificar, tratar y monitorear el riesgo en las organizaciones). Conocer exactamente el impacto favorece las iniciativas de seguridad en la organización pues será el motivo por el cual se pueda incitar a la Alta Gerencia a ejecutar el proyecto de seguridad que se esté elaborando.

Ayuda de sobremanera en la atención de los riesgos, dándonos pautas de cómo distribuir los recursos que tenemos en la organización ya que tenemos una buena medida de las pérdidas que se podrían experimentar y por ende estar preparados desde todas las áreas de la organización.

Lo dicho en el párrafo anterior es el causante de hacernos comprender que hacer una cuantificación financiera es obligatorio. Se debe realizar esta cuantificación tanto a corto como a largo plazo e incluir además aspectos tales como pérdida de imagen de la empresa en el mercado, pérdida de dinero, disminución del valor de

las acciones de la empresa, responsabilidad penal o civil, sanciones por violaciones a las regulaciones y más.

Debemos también establecer rangos, para la cuantificación del impacto, para tener una mayor visión del mismo. Esta cuantificación puede basarse en el costo o valoración del activo de información así como la pérdida sufrida de integridad, disponibilidad y confidencialidad de la información manejada/creada/custodiada por dicho activo.

Algunas escalas comunes de impacto son cualitativas: catastrófico, muy grave, medio, moderado o bajo a las que muchas veces se les agrega un valor numérico. La mayoría de autores coinciden en que las escalas más adecuadas se encuadran dentro de matrices 5x5 (o mapa de calor de riesgos) como se puede apreciar en la siguiente figura (Tupia 2010):

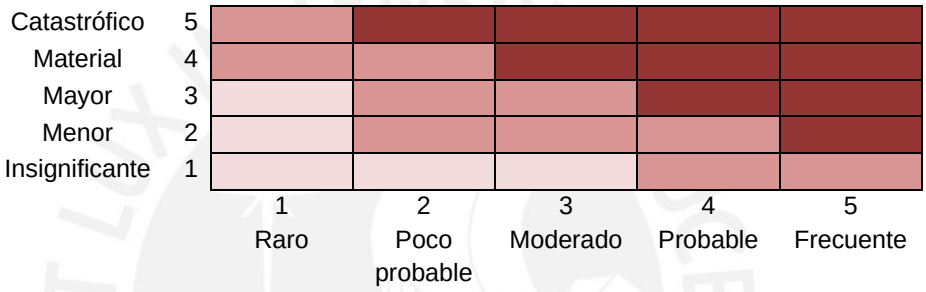


Figura 10: Matriz de riesgo basado en un análisis cualitativo

A partir de experiencias pasadas, de prácticas internacionalmente aceptadas, de investigaciones de mercado, de modelos financieros y mas se realizan tanto el cálculo del impacto como el cálculo de la probabilidad, que cabe resaltar, son predominantemente matemáticos.

Es necesario indicar que en el marco de desarrollo de estos cálculos se introducirá una dosis de subjetividad que va a depender del tipo de organización y de los activos de información que se tengan para clasificar los riesgos y calcular los impactos.

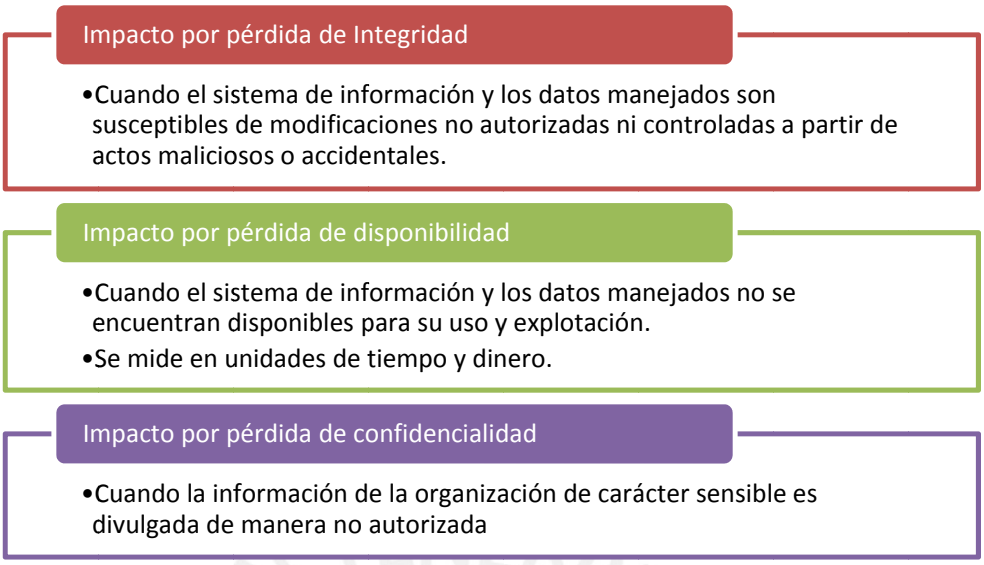


Figura 11: Análisis de impacto

2.3.4. Gestión de Riesgos

Proceso que busca establecer un equilibrio entre lo que la empresa "quiere ganar" frente a lo que "está dispuesta a sufrir": ganancias enfrentadas a las vulnerabilidades y pérdidas que pueda tener por efecto de las amenazas a sus recursos más críticos. En este caso específico, los recursos de información.

Es una herramienta base de la Seguridad de Información ya que nos muestra las amenazas a la integridad, disponibilidad y confidencialidad de la información crítica de la organización; y también nos permite la gestión y monitoreo del cumplimiento de los requisitos regulatorios a los que está sometió el negocio y que afectan directamente a su continuidad (que es gran medida, el objetivo de cualquier estrategia de seguridad de información).

Conjunto de actividades que permite identificar, cuantificar, tratar y monitorear el riesgo en las organizaciones fungiendo de balanza entre lo que se está protegiendo (por medio de un control) y lo que se estaría perdiendo:

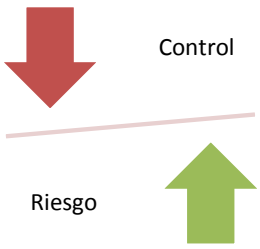


Figura 12: La gestión de riesgo como una herramienta de balance

Para lograr el éxito de la GR, es vital tener en cuenta tanto la cultura como la estructura de la organización, la misión y los objetivos de negocio que se hayan

trazado, la definición de los procesos organizacionales y el conocimiento de marcos de buenas prácticas generalmente aceptados.

En el escenario que una amenaza se materialice, la Gestión de Riesgos garantizará que el impacto que se tendrá internamente (en la organización) será manejable, es decir, que estará enmarcado dentro de los límites de costos aceptables sin perturbar la continuidad del negocio.

Sabemos que en toda actividad empresarial hay riesgo (cuando hacemos algo o cuando dejamos de hacer algo), la Gestión de Riesgos debe brindar garantía de seguridad en cualquier actividad que emprenda la institución apoyándose en la estrategia de seguridad que ésta esté llevando a cabo.

Figura 13: Esquema Amenaza-Vulnerabilidad-Riesgo-Impacto (Tupia 2010)

La Gestión de Riesgos es también tener un autoconocimiento considerable, esto es, la necesidad de conocer las amenazas y vulnerabilidades propias. En consecuencia la Gestión implicará conocer la naturaleza de los riesgos para cuantificar el impacto en el negocio. De esta manera se podrá administrar los riesgos de manera eficiente. Este es un paso crucial y previo para la determinación de la estrategia y de los planes de seguridad.

Debemos tener muy presente que la Gestión de Riesgos debe llevar, de manera adjunta a sí misma, un mensaje que transmita el equilibrio entre el costo que llevaría la implementación de los controles y contramedidas, y las exposiciones al riesgo que tiene la organización.

Figura 14: Fases de la Gestión de Riesgos

La importancia de la GR radica en convertir a la seguridad de información en un facilitador del negocio, en un ente que aporta valor al mismo. Permite dirigir las acciones que prevengan, de manera razonable, las amenazas a la seguridad a las que se ve expuesta la empresa; o sea, en cierta medida dirige los planes de seguridad.

3. REVISIÓN DEL ESTADO DEL ARTE

3.1. COBIT

Es un marco integral de Gobierno de las Tecnologías de la Información que permite, a la Alta Dirección de una organización, alcanzar sus objetivos para el gobierno y la gestión de las TI de las empresas. Ayuda a las organizaciones a obtener un retorno de valor de sus TI y les permite conectar los requerimientos de negocio y de control con los aspectos técnicos, controlando los riesgos y optimizando los recursos.

COBIT 5.0 usa varios estándares y normas internacionales convenientemente para poder convertirse en un marco integrador. Entre ellas se encuentran: ValIT, RiskIT, ITIL, Familia ISO 27000, Normas NIST, COSO, CMMI, PMBOK.

Se basa en los siguientes principios:

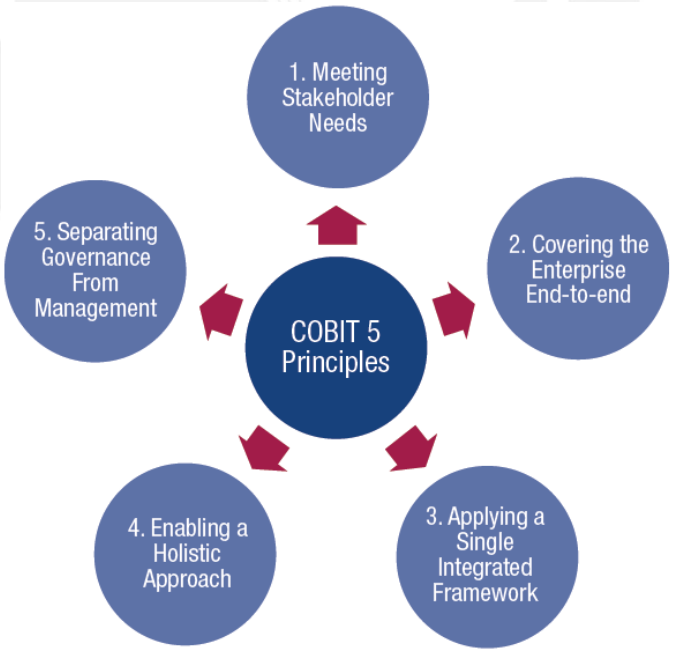


Figura 15: Principios de Cobit 5.0 (ISACA 2012)

1. Identificar las necesidades de los Stakeholders (Interesados)
   Crear valor manteniendo el equilibrio entre realización de beneficios y la optimización del uso de recursos y gestión del riesgo.

2. Cubrir y conocer el negocio de la organización
   Conocimiento profundo del negocio de la organización para conseguir una integración entre el Gobierno de la empresa y el Gobierno de las TI.

3. Aplicar un único marco de trabajo integrado
   COBIT cubre todas las necesidades y se integra con otros marcos y buenas prácticas, de forma que puede ser utilizado como marco general.

4. Aplicar un enfoque holístico
   Para obtener con eficacia y eficiencia una Gestión y Gobierno de TI.

5. Separar Gestión de Gobierno.
   Es necesario hacer la diferencia entre ambas disciplinas, resaltando su importancia y complementariedad.

También se presenta el concepto de facilitadores que son factores que individual o colectivamente influyen para que algo funcione. En COBIT 5.0 son descritas 7 categorías:

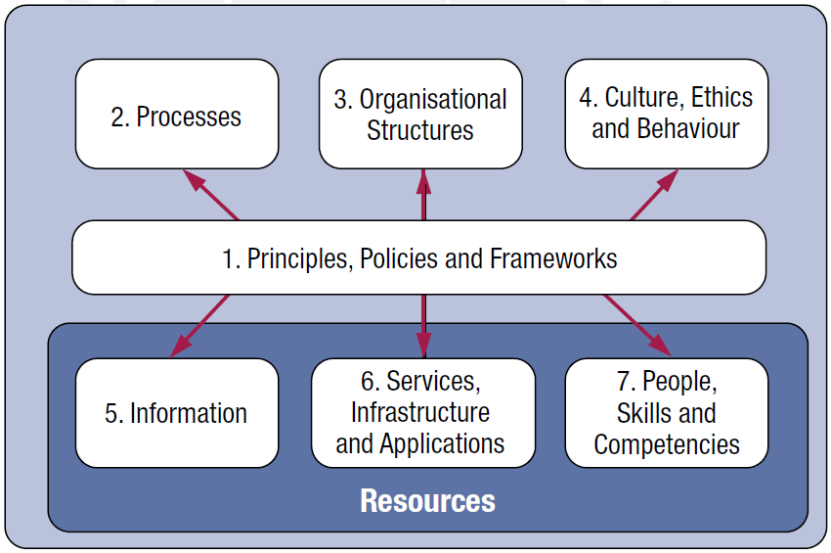


Figura 16: Facilitadores de COBIT 5.0 (ISACA 2012)

1. Principios, Políticas y Marcos de Trabajo
   Son el medio para ocasionar el comportamiento deseado para la gestión diaria mediante guías prácticas.

2. Procesos
   Especifican un grupo organizado de actividades y prácticas para cumplir con objetivos determinados y producir un conjunto de salidas para alcanzar los objetivos generales relacionados con TI que están alineados con los objetivos del negocio.

3. Estructura Organizacional

Entidades importantes y claves en la toma de decisiones de la empresa u organización.

4. Cultura, Ética y Comportamiento
   De la empresa y de los individuos que tienen que ser considerados un factor significativo para el éxito en las actividades de gobierno y gestión de TI.

5. Información
   Requerida para mantener la empresa en ejecución y bien gobernada. En el nivel operacional, la información es un producto clave de la empresa.

6. Servicios, Infraestructura y Aplicaciones
   Incluye la infraestructura, la tecnología y las aplicaciones para proveer a la empresa los servicios y procesamiento de TI.

7. Personas, Habilidades y Competencias
   Requeridas para completar con éxito las actividades y para tomar las decisiones correctas y acciones correctivas (mediante el monitoreo).

COBIT 5.0 es complementado por sus procesos facilitadores que son prácticas relacionadas de TI las cuales son subdivididas en dos áreas principales:

A. Gobierno: donde se definen siguientes actividades: (EDM, por sus siglas en Inglés)
   a. Evaluar
   b. Dirigir
   c. Monitorear

B. Gestión: donde se entregan a 4 dominios que son: (PBRM, por sus siglas en Inglés)
   a. Planear
   b. Construir
   c. Ejecutar
   d. Monitorear.

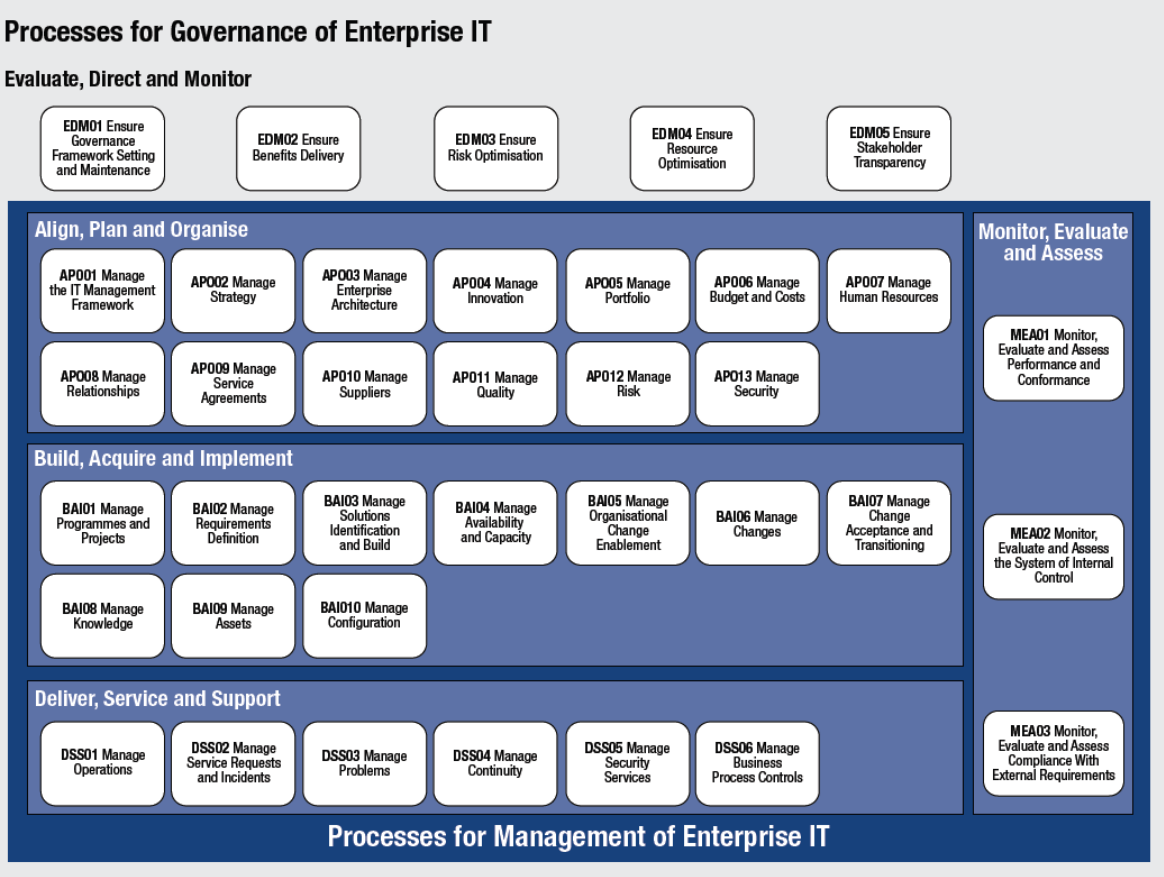


Figura 17: Modelo de Referencia de Procesos de COBIT 5.0 (ISACA 2012)

A. EMD - Evaluar, Dirigir, Supervisar

   a. EDM01 Definir y Mantener el Marco de Gobierno
   b. EDM02 Asegurar Entrega de Beneficios
   c. EDM03 Asegurar Optimización de Riesgo
   d. EDM04 Asegurar Optimización de Recursos
   e. EDM05 Asegurar Transparencia para los Interesados

B. APO - Alinear, Planear, Organizar

   a. APO01 Gestionar el Marco de Gestión de TI
   b. APO08 Gestionar Relaciones
   c. APO02 Gestionar la Estrategia
   d. APO09 Gestionar Acuerdos de Servicio
   e. APO03 Gestionar la Arquitectura Empresarial
   f. APO10 Gestionar Proveedores
   g. APO04 Gestionar Innovación
   h. APO11 Gestionar Calidad
   i. APO05 Gestionar Cartera
   j. APO12 Gestionar Riesgo
   k. APO06 Gestionar Presupuesto y Costos

l. APO13 Gestionar Seguridad
m. APO07 Gestionar Recursos Humanos

C. BAI - Construir, Adquirir, Implantar

a. BAI01 Gestionar Programas y Proyectos
b. BAI08 Gestionar Conocimiento
c. BAI02 Gestionar Definición de Requerimientos
d. BAI09 Gestionar Activos
e. BAI03 Gestionar Identificación de Soluciones y Construir
f. BAI10 Gestionar Configuración
g. BAI04 Gestionar Disponibilidad y Capacidad
h. BAI05 Gestionar Facilitación del Cambio Organizacional
i. BAI06 Gestionar Cambios
j. BAI07 Gestionar Aceptación del Cambio y Transición

D. DSS - Entrega, Servicio, Soporte

a. DSS01 Gestionar Operaciones
b. DSS02 Gestionar Requerimientos de Servicio e Incidentes
c. DSS03 Gestionar Problemas
d. DSS04 Gestionar Continuidad
e. DSS05 Gestionar Servicios de Seguridad
f. DSS06 Gestionar Control de Procesos de Negocio

E. MEA - Supervisar, Evaluar, Valorar

a. MEA01 Desempeño y Conformidad
b. MEA02 Sistema de Control Interno
c. MEA03 Cumplimiento Requerimientos Externos

ISACA propone la ejecución del diagrama presentado en la Figura 18, donde se resalta la composición de 3 círculos concéntricos, los cuales pueden ser indicados de la siguiente manera: Planificación, Cambios, Mejora Continua.

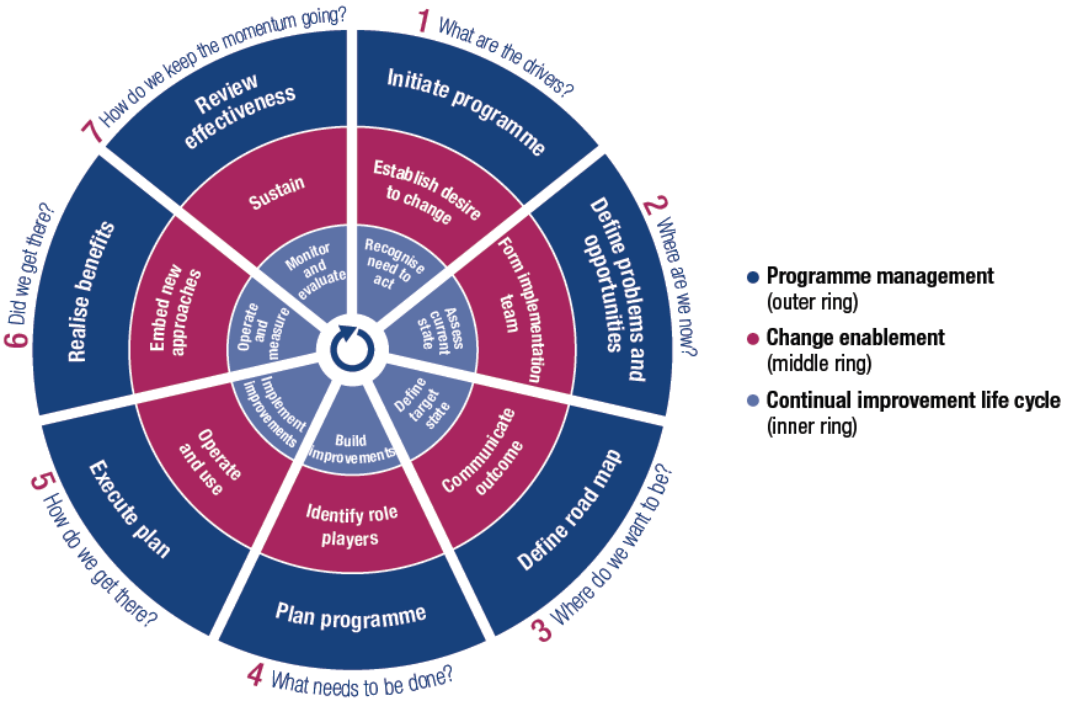


Figura 18: Ciclo de vida de implementación de COBIT 5.0 (ISACA 2012)

La implementación cubre:

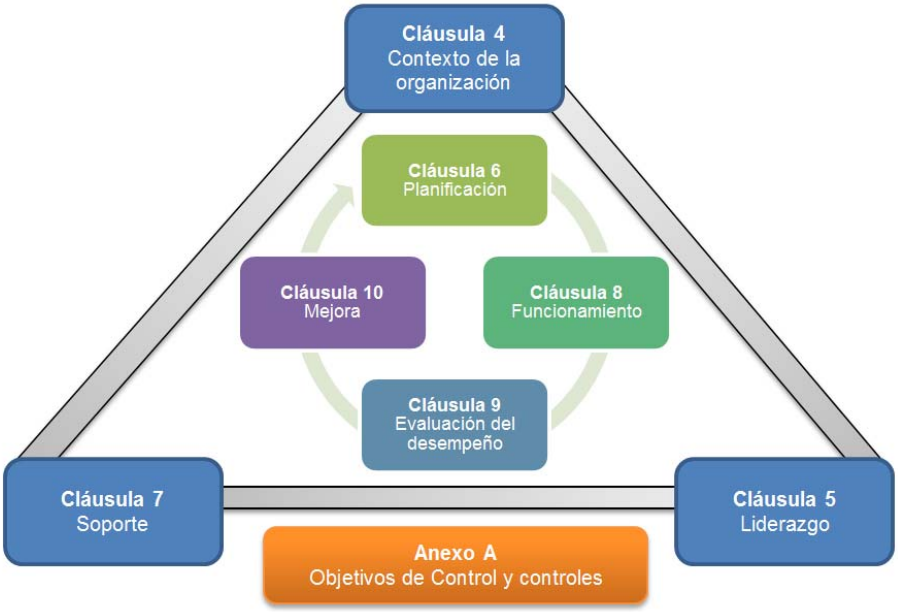
- Posicionamiento del Gobierno de TI empresarial dentro de la organización
- Tomar los primeros pasos hacia la mejora del Gobierno de TI
- Desafíos de la implementación y factores de éxito.
- Facilitar los cambios organizacionales y el comportamiento de los mismos.
- Implantado la Mejora Continua que incluye posibilitación del cambio y gestión del programa.
- La utilización del marco integral COBIT ® y sus componentes.

3.3. ISO 27001 y 27002

Se refiere a las normas internacionales del International Organization for Standardization (ISO). Pertenecen a la familia de normas ISO 27001. Recientemente han sido actualizadas a una nueva versión: ISO/IEC 27001:2013 e ISO/IEC 27002:2013.

El objetivo de la ISO 27001 es que la empresa sea capaz de priorizar y seleccionar controles en base a sus posibilidades y a sus necesidades/riesgos de seguridad. Es que los riesgos se analicen y se gestionen, que la seguridad se planifique, se implemente y, sobre todo, se revise y se corrija y mejore.

La ISO 27001 se ha modificado para adaptarse a la nueva estructura de alto nivel utilizado en todas las normas de Sistemas de Gestión, lo que simplifica su integración con otros sistemas de gestión.



La ISO 27002 es una guía para, en distintos ámbitos, conocer qué se puede hacer para mejorar la seguridad de la información. Expone, en distintos campos, una serie de apartados a tratar en relación a la seguridad, los objetivos de seguridad a perseguir, una serie de consideraciones (controles) a tener en cuenta para cada objetivo y un conjunto de "sugerencias" para cada uno de esos controles. Sin embargo, la propia norma ya indica que no existe ningún tipo de priorización entre controles, y que las "sugerencias" que realiza no tienen por qué ser ni siquiera convenientes, en función del caso en cuestión.

La ISO 27002 es en esencia una guía que describe los objetivos de control y los controles recomendables en cuanto a seguridad de la información en las organizaciones.

3.2. NTP 27001

Norma Técnica Peruana NTP-ISO/IEC 27001:2008 que especifica los requisitos para el establecimiento, implantación, la puesta en funcionamiento, control, revisión, mantenimiento y mejoramiento de un Sistema de Gestión de Seguridad de la Información de una organización.

Adopta la aplicación de un sistema de procesos dentro de una organización, junto con la identificación y la interacción de estos procesos, así como su gestión, adoptando el modelo “Plan-Do-Check-Act”, que se aplica para estructurar todos los procesos del Sistema de Gestión de Seguridad de la Información. Este proceso requiere:

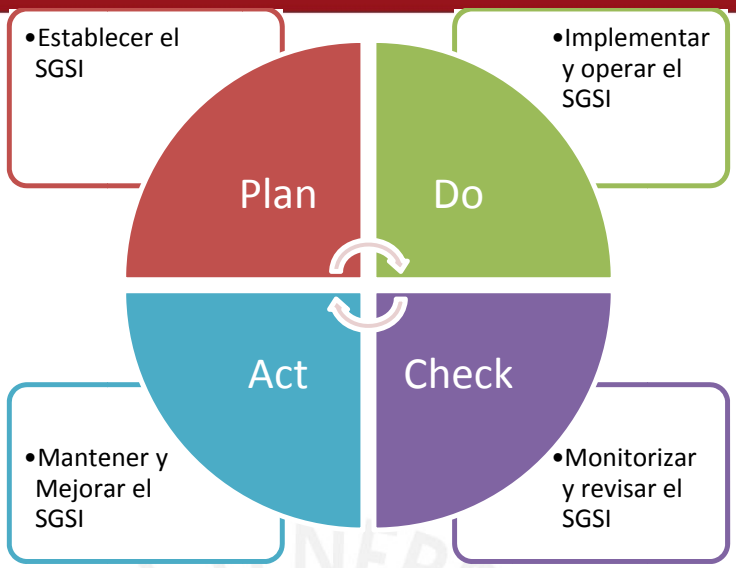


Figura 19: Plan-Do-Check-Act para NTP 27001

- ✓ Establecer el SGSI: Crear política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en correspondencia con las políticas y objetivos generales de la organización.

- ✓ Implementar y operar el SGSI: Implementar y manejar la política, controles y procedimientos SGSI.

- ✓ Monitorear y revisar el SGSI: Evaluar y, donde sea aplicable, calcular el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para revisión.

- ✓ Mantener y mejorar SGSI: Tomar acciones correctivas y preventivas, establecidas en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.

La norma se encuentra estructurada en los siguientes ítems:

A. Prefacio e introducción.

B. Alcance del modelo.

C. Referencias normativas.

D. Términos y definiciones.

E. El sistema de gestión de la seguridad de información en sí.

F. Responsabilidad de la gerencia.

G. Auditorías internas al Sistema de Gestión de Seguridad de la Información.

H. Revisión gerencial del Sistema de Gestión de Seguridad de la Información.

I. Mejoramiento continuo del Sistema de Gestión de Seguridad de la Información.

J. Anexo A: Objetivos y controles.

K. Anexo B: Guía de los principios OECD para administración de riesgos y su correspondencia con el ciclo de Deming PDCA.

L. Anexo C: Correspondencia de esta norma como los estándares ISO 9001:2000 e ISO 14001:2004

3.4. NTP 17799

Norma Técnica Peruana elaborada por el comité Técnico de Normalización de codificación e Intercambio Electrónico de Datos (EDI) en el año 2006, siendo oficializada al año siguiente. Es una adopción de la Norma ISO/IEC 17799:2007.

La NTP 17799:2007 tiene como finalidad proporcionar una base común en el desarrollo de normas de seguridad en las organizaciones y ser una buena práctica de la gestión de la seguridad.

Comprende de 11 ítems de control de seguridad que envuelven un total de 39 categorías principales, que (con sus respectivos objetivos) son:

A. Política de seguridad

a. Política de seguridad de la información: para la gestión de Seguridad de la Información según los requerimientos del negocio, las leyes y regulaciones.

B. Aspectos organizativos para la seguridad

a. Organización interna: gestionar internamente la seguridad de la información.
b. Seguridad en los accesos de terceras partes: para mantener la seguridad de los activos de información y los recursos que manejen información por parte de terceros.

C. Clasificación y control de activos

a. Responsabilidad sobre los activos: para la protección adecuada de los activos de la organización.

b. Clasificación de la información: para establecer un nivel de protección a los activos de información.

D. Seguridad en Recursos Humanos

a. Seguridad antes del empleo: asegurando que los empleados, contratistas y terceros sean los adecuados y que conozcan sus responsabilidades, reduciendo así el riesgo de fraude, hurto o mal uso de las instalaciones.
b. Durante el empleo: que los empleados, contratistas y terceros sean consientes de las políticas de seguridad de información de la organización.
c. Finalización o cambio del empleo: que los empleados, contratistas y terceros terminen su relación laboral con la organización de manera ordenada.

E. Seguridad física y del entorno

a. Áreas seguras: Prescindir los accesos no autorizados, daños e interferencias contra los locales y la información de la organización.
b. Seguridad de los equipos: para los activos de información y la interrupción de las actividades de la organización.

F. Gestión de comunicaciones y operaciones

a. Procedimientos y responsabilidades de operación: manejo correcto y seguro de los recursos que utilicen información de la organización.
b. Gestión de servicios externos: para mantener un nivel de seguridad apropiado y de entrega de servicio en línea con los acuerdos con terceros.
c. Planificación y aceptación del sistema: atenuar los riesgos de fallos del sistema.
d. Protección contra software malicioso: dar protección a la integridad del software y de la información
e. Gestión de respaldo y recuperación: que los servicios que manejan la información y comunicación se mantengan en fluidez continua.
f. Gestión de seguridad en redes: asegurar la información en las redes así como de su infraestructura.
g. Utilización de los medios de información: que las actividades de información no se interrumpan y que los activos no sufran modificaciones, daños y accesos no autorizados.
h. Intercambio de información: evitar la pérdida, modificación o mal uso de información que se intercambia entre organizaciones.
i. Servicios de correo electrónico: dar seguridad al uso y servicios de comercio electrónico.
j. Monitoreo: para detectar las actividades no autorizadas que quieran manejar la información de la organización.

G. Control de accesos

a. Requisitos de negocio para el control de accesos: controlar los accesos a la información.
b. Gestión de acceso de usuarios: asegurar el acceso de usuario autorizados y minimizar los no autorizados.
c. Responsabilidades de los usuarios: evitar los accesos no autorizados y el compromiso o robo de la información.
d. Control de acceso a la red: impedir el acceso no autorizado a los servicios de red.
e. Control de acceso al sistema operativo: evitar los accesos no autorizados a las computadoras.
f. Control de acceso a las aplicaciones y la información: para dificultar el acceso no autorizado a la información que está en los sistemas.
g. Informática móvil y teletrabajo: acreditar la seguridad de la información mediante dispositivos móviles y de teletrabajo.

H. Adquisición, desarrollo y mantenimiento de sistemas

a. Requisitos de seguridad de los sistemas: que los sistemas de información sean seguros desde su concepción.
b. Seguridad de las aplicaciones del sistema: que los datos de usuarios no experimenten mal uso, pérdida o modificaciones en las aplicaciones.
c. Controles criptográficos: para proteger la información referente a su confidencialidad, integridad y autenticidad.
d. Seguridad de los archivos del sistema: preservar la seguridad de los archivos del sistema.
e. Seguridad en los procesos de desarrollo y soporte:
f. Gestión de la vulnerabilidad técnica

I. Gestión de incidentes en la Seguridad de Información

a. Reportando eventos y debilidades de la seguridad de información
b. Gestión de las mejoras e incidentes en la seguridad de información

J. Gestión de continuidad del negocio

a. Aspectos de la gestión de continuidad del negocio

K. Cumplimiento

a. Cumplimiento con los requisitos legales
b. Revisiones de la política de seguridad y de la conformidad técnica
c. Consideraciones sobre la auditoria de sistemas

La Presidencia del Consejo de Ministros, decretó que de uso obligatorio esta norma con la finalidad de poder generar un plan de seguridad de la información en la Administración Pública. Esta medida muestra que el estado peruano tiene como

consigna el introducir cada vez más la cultura de seguridad en sus empresas estatales para brindar mejor servicio a los ciudadanos peruanos.

4. DISCUSIÓN SOBRE LOS RESULTADOS DE LA REVISIÓN DEL ESTADO DEL ARTE

Al realizarse la revisión del estado del arte para nuestro proyecto de fin de carrera y después de consultarse en instituciones oficiales del estado peruano como el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), Contraloría General de la República (CGR) se pudo constatar que no existen registro alguno de guías o procedimientos para poder realizar auditorías de cumplimiento de la NTP-ISO/IEC 17799.

El marco internacional COBIT se ha actualizado y en su nueva versión 5.0 presenta una mejora que es valorada por los profesionales, ya que al ser el estándar de facto en Tecnologías de Información brinda una combinación de otros estándares de ISACA.

Cabe resaltar que la reciente normativa NTP-ISO/IEC 27001:2008 obliga a una lista de empresas del estado peruano a implantarla, pero no estipula que necesiten ser certificadas en ISO 27001:2005. Cualquiera sea el caso, se debe tener en cuenta los gastos que implicaría bien la implantación de la norma técnica peruana o la consecución de la certificación en su relacionada norma internacional.

La NTP-ISO/IEC 17799, que es el descenso de la norma ISO 27002:2005 en el escenario peruano, es ideal para tomarse como base para el desarrollo de los procedimientos que se proponen en este proyecto de fin de carrera que serán utilizados como parte de los controles del proceso de implantación de la NTP-ISO/IEC 27001.

Es importante indicar que las normas ISO 27001 e ISO 27002 han sido actualizadas recientemente a las versiones ISO 27001:2013 e ISO 27002:2013. Estas normas son internacionales y en el marco peruano aún están siendo introducidas por los profesionales de seguridad de la información en las distintas empresas. Las NTP (normativa vigente) aún mantienen su versión anterior (ISO 27001:2005 e ISO 27002:2005) con sus respectivas equivalencias. Mientras no se actualice al equivalente a las nuevas versiones ISO, las empresas del estado peruano pueden seguir trabajando bajo la versión anterior.

CAPÍTULO 3:
PROCEDIMIENTOS GENERALES DE AUDITORÍA

1. INTRODUCCIÓN

Para poder dar inicio a una Auditoría de Control de Seguridad de la Información basada en la NTP-ISO/IEC 17799:2007 para empresas públicas del Estado Peruano, es fundamental identificar las entidades que tienen las facultades de ejecutar ésta actividad.

En el contexto peruano, se reconocen las siguientes entidades de las cuales puede preceder esta motivación:

- ✓ Control Interno, de la empresa pública (si es que existiese dicha área)
- ✓ Gerencia General, como ente superior de la empresa pública.
- ✓ Contraloría General de la República, como Entidad Fiscalizadora Superior (EFS) en el Perú

Se necesita recabar la información necesaria mediante la solicitud de los documentos oficiales, registrados y difundidos de la empresa, así como también, mediante entrevistas personales con la(s) personas(s) a cargo en las áreas relacionadas al objeto de auditoría.

2. PROCEDIMIENTOS PARA DETERMINAR EL ALCANCE DE LA AUDITORÍA

Como primer punto a atender es determinar el alcance que tendrá la Auditoría. Para ello se revisará la documentación de la empresa que se hayan compuesto al implementar los controles sugeridos por la NTP-ISO/IEC 17799:2007.

Al ser, la auditoría de control de Seguridad de la Información basada en la NTP-ISO/IEC 17799:2007, parte del proceso de implementación de la Norma Técnica Peruana NTP-ISO/IEC 27001:2008, se hace obligatoria también la revisión de la documentación generada al establecer el Sistema de Gestión de Seguridad de la Información.

Además se realizarán entrevistas personales al grupo de personas profesionales de la entidad de la cual viene el pedido de ejecutar el proceso de Auditoría.

A continuación se lista los ítems que ayudarán a poder establecer de manera detallada el Alcance de la Auditoría:

Ítem	Descripción
Documento de Política de Seguridad y objetivos	Políticas, principios, normas y requisitos de conformidad para la empresa en Seguridad de la Información.
Documento de Alcance del Sistema de Gestión de Seguridad de la Información	Determinar el alcance de la seguridad de la información, su importancia en la empresa. Establecimiento de los objetivos de la Gerencia como soporte de los objetivos de la Seguridad de la Información.
Documento de Establecimiento de Roles y Responsabilidades para la Seguridad de la Información	Descripción específica de las responsabilidades en relación a gestión de la Seguridad de la Información en la empresa. Incluye también la comunicación de las incidencias.
Documento de Evaluación de Riesgos	Identifica, cuantifica y prioriza los riesgos contra el criterio para la aceptación del riesgo y los objetivos relevantes para la organización.
Documento de Declaración de Aplicabilidad	Describe los controles a implementarse y sus objetivos descendidos a la realidad de la empresa.
Informes de Auditorías previas y/o de terceros.	Presentaciones de recomendaciones y constataciones resultantes de auditorías pasadas y/o actos de incumplimiento regulatorio.
Entrevistas Personales	Determinar de manera exacta y detallada el alcance que se pretende tener para la Auditoría.

Tabla 1 - Ítems para establecer Alcance de la Auditoría

Como aporte, el Auditor, en base a su juicio profesional, puede ampliar y/o disminuir el alcance de la Auditoría. Esto puede darse siempre y cuando se informe por escrito a los interesados.

Al terminar de detallar el Alcance que tendrá la Auditoría, se debe comunicar y recibir la aceptación del mismo por la empresa auditada.

3. PROCEDIMIENTOS PARA DETERMINAR EL OBJETIVO DE LA AUDITORÍA

Las auditorías a las que va dirigido el presente proyecto de fin de carrera, son eminentemente de *cumplimiento regulatorio.* Esto debido fundamentalmente a que el universo de empresas del Estado (que podrían hacer uso de los procedimientos planteados en este proyecto) están obligadas a cumplir las normas técnicas NTP ISO/IEC 27001:2008 y NTP ISO/IEC 17799:2007.

En la medida que se hayan hecho avances progresivos de la implementación de ambas normas y que a su vez, se hayan hecho auditorias de cumplimiento parcial de las mismas, los objetivos pueden variar (reducirse paulatinamente, hasta que se verifique el cumplimiento total de cualquiera de las normas en cuestión)

Los criterios de la auditoría —como se verán más adelante— serán los aspectos específicos de cualquiera de las normas (en especial la NTP-ISO/IEC 17799:2007) que formarían parte del alcance y se deberán detallar en sendas declaraciones de aplicabilidad.

Adicionalmente, la definición del objetivo general dependerá de varios factores. Entre los más importantes y más recurridos se encuentran:

- ✓ El mandato y el cometido de una de las tres entidades mencionadas anteriormente (Control Interno, Gerencia General o Contraloría General de la República) que sea específico para la auditoría a realizar y que pueda escapar del cumplimiento de cualquiera de las normas anteriormente mencionadas.
- ✓ Leyes y regulación interna pertinentes a la empresa auditada y que guardan relación con las normas auditadas (los denominados *cuestionarios de control interno*)

Estos factores podrían modificar (ampliar) el objetivo de la auditoría de cumplimiento.

4. PROCEDIMIENTOS PARA ESTABLECER LOS CRITERIOS DE LA AUDITORÍA

Dependiendo del documento de Declaración de aplicabilidad de la empresa del estado, se establecerán los criterios para la auditoria. Se detallan en los anexos el universo de criterios que abarca la NTP-ISO/IEC 17799:2007.

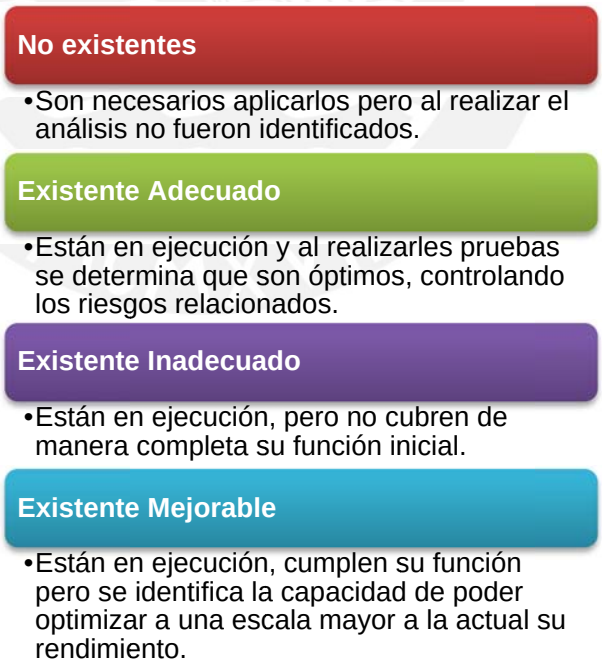
5. PROCEDIMIENTOS PARA EL LEVANTAMIENTO DE EVIDENCIAS

En esta etapa de la auditoría es necesario reconocer las vías por las cuales se podrá realizar el levantamiento de evidencias. Para este propósito, se revisan los siguientes aspectos:

Se inicia por la revisión de la Declaración de Aplicabilidad, la cual dará luces y ayudará a entender lo que implantó la empresa en relación a la gestión de seguridad de la información. De todos los controles de la NTP-ISO/IEC 17799:2007, el SOA establece los controles que aplican para la empresa del estado en cuestión. Para tal efecto, se solicita los documentos referidos a:

- ✓ la identificación de riesgos,
- ✓ la definición de los controles,
- ✓ la identificación de requisitos legales, regulatorios, de contratos, etc.,
- ✓ las necesidades propias de la empresa.
- ✓ otros relacionados.

Teniendo el acceso a esta información se podrá realizar luego la clasificación de los controles de acuerdo a la declaración de aplicabilidad. Para esta clasificación se define la siguiente tipificación de controles:



Es necesario poder desarrollar una tabla con todos los controles indicados por el SOA indicando el tipo según lo especificado líneas arriba.

Cabe resaltar que los controles se podrían agrupar en dos grandes conjuntos: No existentes y Existentes. En el caso de los Existentes, se subdivide en otros tres, con la finalidad de poder manejarlos y analizarlos con las salidas de un sistema de gestión de incidentes y problemas.

Esta gestión se adaptará como herramienta fundamental en esta etapa, pues al ser un manejo de los eventos que se dan en el día a día de la empresa, es el activo más cercano y constante en la empresa que nos dará información certera y directa de cómo reacciona toda la infraestructura informática antes los incidentes o problemas que pudieran ocasionarse en el flujo normal de actividades a la que está expuesta la empresa.

Los controles existentes serán evaluados mediante su comportamiento con la gestión de incidentes y problemas, teniendo como idea general la siguiente ilustración:

De cada control existente, se analizarán los siguientes ítems:

Finalmente, los reportes de auditorías pasadas en relación a seguridad de la información que tuviera la empresa, serán también vitales en esta etapa. Nos permitirán identificar los puntos más críticos en los cuales adolecía la empresa.

Además existen una gran gama de diversos documentos que puedan estar relacionados a los controles existentes y no existentes que se hará

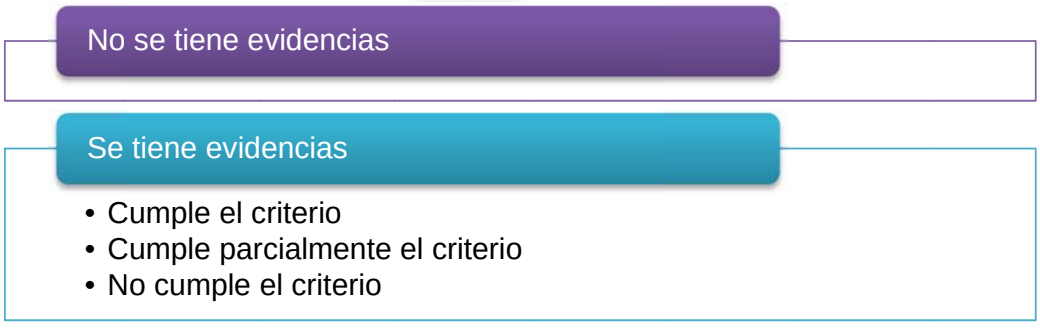
necesario poder analizar y determinar con ello de manera íntegra la evaluación de cómo se encuentra la empresa con respecto a la seguridad de la información

6. PROCEDIMIENTOS DE DOCUMENTACIÓN DE HALLAZGOS

La presentación de hallazgos contempla mostrar los resultados de la evaluación de la recopilación de las evidencias de la auditoría frente a los criterios de auditoria.

El tipo de auditoria al cual aplica el presente proyecto de fin de carrera exige la verificación del cumplimiento real de la norma técnica peruana NTP-ISO/IEC 17799:2007. Esto obliga a buscar evidencias objetivas, las cuales deben ser evaluadas siguiendo los criterios de auditoría previamente definidos, para obtener los hallazgos.

Como resultado de la evaluación de las evidencias, se podría encontrar diversos escenarios, entre los cuales destacan:



- ✓ **No se tiene evidencia**: Escenario donde el auditor no pudo obtener una manera de relacionar un criterio de la Norma Técnica Peruana con la respectiva evidencia a pesar de haberse aplicado los mecanismos de levantamiento y/o análisis. Cabe resaltar que no se pueden realizar

asunciones si no se tiene forma de poder corroborar lo que se quiera presentar como hallazgo.

- ✓ **Si tiene evidencia:** Si el auditor cuenta con la evidencia(s) necesaria(s) y justificables para relacionarlo con un criterio.

Los criterios de la NTP (que están listados en la Declaración de Aplicabilidad – SOA) que hayan podido ser enfrentados con al menos una evidencia, proseguirán a agruparse de la siguiente manera, siguiéndose de manera estricta (por tratarse de una auditoria de cumplimiento):

- ✓ **No se cumple el criterio:** Donde las evidencias obtenidas revelen que el criterio evaluado no se está insertado en su totalidad en la empresa.

- ✓ **Sí se cumple el criterio:** De la evaluación se obtiene que el criterio, en su totalidad, es atendido por controles y/o procesos los cuales pueden ser corroborados por las evidencias respectivas.

- ✓ **Se cumple el criterio parcialmente:** Cuando las evidencias nos permiten determinar que el criterio está siendo asistido no en su totalidad, sino en un porcentaje que será dispuesto a criterio profesional del auditor.

7. PROCEDIMIENTOS PARA LA DOCUMENTACIÓN DE LAS CONCLUSIONES Y RECOMENDACIONES

El informe final de auditoría consiste en la presentación de las conclusiones y recomendaciones de acuerdo a los hallazgos encontrados.

Partiendo de la base del Documento de aplicabilidad - SOA se insertan las conclusiones una a una. Esta será presentada de manera detallada.

Luego se pasará a generar las conclusiones generales de toda la auditoria que tendrá como punto de inicio el objetivo general de la auditoría. Nuevamente se hace uso del Documento de aplicabilidad SOA para cuantificar el nivel de cumplimiento que se ha detectado a causa de la auditoria.

CAPÍTULO 4:
PRUEBAS DE LOS PROCEDIMIENTOS

1. INTRODUCCIÓN

A continuación se hará presente la documentación que sustenta las pruebas realizadas a los procedimientos de auditoría antes detallados en el presente proyecto de fin de carrera. Esto es con la finalidad de verificar la utilidad de dichos procedimientos en procesos de auditoría a empresas del estado.

2. ALCANCE DE LAS PRUEBAS

Las pruebas realizadas se ejecutaron en el marco de una empresa del estado peruano que está normada en cumplir con lo estipulado en las NTP-ISO/IEC 17799:2007 y NTP-ISO/IEC 27001:2008.

En este caso específico se referirá al Dominio 5 y al Dominio 7 de la NTP-ISO/IEC 17799:2007 concerniente a las Políticas de Seguridad que maneja una empresa del estado peruano.

3. OBJETIVO DE LAS PRUEBAS

El objetivo de las pruebas realizadas es el cumplimiento por parte de una empresa del estado peruano en la implementación de las Normas técnicas peruanas NTP-ISO/IEC 17799:2007 y NTP-ISO/IEC 27001:2008.

4. EJECUCIÓN DE LAS PRUEBAS

Los criterios que se van a utilizar son todos los relacionados al Dominio 5 de la NTP-ISO/IEC 17799:2007 (refiérase 5.1.1 y 5.1.2) y al Dominio 7 (refiérase 7.1.1, 7.1.2, 7.1.3, 7.2.1 y 7.2.2). Como evidencias se ha manejado el documento de Política Corporativa de Seguridad de Información de una empresa pública del estado peruano el cual reemplaza a los documentos antes manejados por la empresa estatal: Documento de Política General de Seguridad de Información y el Documento de Seguridad de Información.

El documento cuenta con un índice que se divide en 4 secciones:

1. Consideraciones Generales
2. Lineamientos
   2.1. Declaración de Seguridad de la Junta de Directores.
   2.2. Cumplimiento.
   2.3. Definiciones y responsabilidades.
3. Organización de Seguridad
   3.1. Generalidades.
   3.2. Objetivo.
   3.3. Responsabilidad.
   3.4. Comité de Seguridad de Información.
   3.5. Jefe de Seguridad de Información.
4. Control de Versiones

Además para las pruebas se tuvo acceso a los Inventarios de Activos y el Documento de Políticas del Inventario de Activos.

El Inventario de Activos es un conjunto de hojas de cálculo bajo la herramienta MS Excel de Windows, que tiene como estructura lo siguiente:

1. Número
2. Activo
3. Proceso Relacionado
4. Tipo de Activo
5. Activo de TI
6. Dueño del Activo
7. Responsable del activo
8. Confidencialidad
9. Integridad
10. Disponibilidad
11. Evaluación del activo
12. Criticidad del activo.

La Política del Inventario de Activos cuenta con un índice que se divide en ## secciones:

1. Consideraciones Generales
2. Lineamientos
   2.1. Clasificación del Activo de Información.
   2.2. Evaluación del Activo de Información.
   2.3. Criticidad del Activo de Información.
3. Definiciones.
   3.1. Campos del Inventario de Activos de Información.
4. Control de Versiones

A continuación se hace el resumen de hallazgos (siguiendo los procedimientos descritos en el capítulo anterior) y después de una exhaustiva lectura del documento antes mencionado:

Dominio	**5.**	**POLÍTICA DE SEGURIDAD**	**CUMPLIMIENTO**
Categoría	**5.1.**	**Política de seguridad de la información**	
Control	**5.1.1.**	**Documento de política de seguridad de la información.**	
Objetivo	Aprobar, publicar y comunicar, por parte de gerencia a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información		✔ (83,33%)
Proced. Específicos	P1	Definición, objetivos globales, alcance e importancia	✓
	P2	Apoyo de gerencia	✓
	P3	Objetivos de control y mandos.	✓
	P4	Políticas, principios, normas y requisitos	✓
	P5	Responsabilidades y comunicación de incidencias	X
	P6	Referencias de documentación	✓

Tabla 2 - Hallazgos 1 de las Pruebas de los Procedimientos

Dominio	**5.**	**POLÍTICA DE SEGURIDAD**	**CUMPLIMIENTO**
Categoría	**5.1.**	**Política de seguridad de la información**	
Control	**5.1.2.**	**Revisión y evaluación**	
Objetivo	Revisar la política de seguridad en intervalos planificados o si cambios significantes ocurren con el fin de asegurar su uso continuo.		✔ (100%)
Proced. Específicos	P1	Propietario de la política	✓
	P2	Revisión de la política	✓

Tabla 3 - Hallazgos 2 de las Pruebas de los Procedimientos

Dominio	**7.**	**CLASIFICACIÓN Y CONTROL DE ACTIVOS**	**CUMPLIMIENTO**
Categoría	**7.1.**	**Responsabilidad sobre los activos**	
Control	**7.1.1.**	**Inventario de activos**	
Objetivo	Identificar todos los activos elaborando y manteniendo un inventario de todos los activos importantes.		✔ (100%)
Proced. Específicos	P1	Identificación de activos	✓
	P2	Clasificación de activos	✓

Tabla 4 - Hallazgos 3 de las Pruebas de los Procedimientos

Dominio	**7.**	**CLASIFICACIÓN Y CONTROL DE ACTIVOS**	**CUMPLIMIENTO**
Categoría	**7.1.**	**Responsabilidad sobre los activos**	

Control	**7.1.2.**	**Propiedad de los activos**	
Objetivo	Toda la información y los activos asociados con el proceso de información deben ser poseídos por una parte designada de la organización.		✔ (100%)
Proced. Específicos	P1	Responsabilidad de propietarios de activos	✓
	P2	Asignación de propiedad	✓

Tabla 5 - Hallazgos 4 de las Pruebas de los Procedimientos

Dominio	**7.**	**CLASIFICACIÓN Y CONTROL DE ACTIVOS**	**CUMPLIMIENTO**
Categoría	**7.1.**	**Responsabilidad sobre los activos**	
Control	**7.1.3.**	**Uso adecuado de los activos**	
Objetivo	Identificar, documentar e implementar las reglas para un uso aceptable de la información y de los activos asociados con las instalaciones del procesamiento de la información.		✔ (100%)
Proced. Específicos	P1	Reglas para empleados, contratistas y terceras partes	✓
	P2	Provisión de reglas específicas	✓

Tabla 6 - Hallazgos 5 de las Pruebas de los Procedimientos

Dominio	**7.**	**CLASIFICACIÓN Y CONTROL DE ACTIVOS**	**CUMPLIMIENTO**
Categoría	**7.2.**	**Clasificación de la información**	
Control	**7.2.1.**	**Guías de clasificación**	
Objetivo	Clasificar la información en función de su valor, requisitos legales, sensibilidad y criticidad para la organización		✔ (66,66%)
Proced. Específicos	P1	Impacto de compartir o restringir información	✓
	P2	Reclasificación a través del tiempo	X
	P3	Responsabilidad del propietario del activo	✓

Tabla 7 - Hallazgos 6 de las Pruebas de los Procedimientos

Dominio	**7.**	**CLASIFICACIÓN Y CONTROL DE ACTIVOS**	**CUMPLIMIENTO**
Categoría	**7.2.**	**Clasificación de la información**	
Control	**7.2.2.**	**Marcado y tratamiento de la información**	
Objetivo	Definir un conjunto adecuado de procedimientos para marcar y tratar la información de acuerdo con el esquema de clasificación adoptado por la organización		✔ (50%)
Proced. Específicos	P1	Alcance de los procedimientos de marcado de la información	✓
	P2	Marcado en la salida de sistemas de información	X
	P3	Definición de procedimientos	✓
	P4	Acuerdos con otras organizaciones	X

Tabla 8 - Hallazgos 7 de las Pruebas de los Procedimientos

5. CONCLUSIONES Y RECOMENDACIONES DE LAS PRUEBAS.

Luego del levantamiento de evidencias y la presentación de los hallazgos se concluye el cumplimiento por parte de la empresa del estado peruano en un 91,66% del Dominio 5 y un 83.33% del Dominio 7 de la NTP-ISO/IEC 17799:2007 como parte del proceso de implementación de la NTP-ISO/IEC 27001:2008 (Sistema de Gestión de Seguridad de Información).

Se pudo evidencias que la empresa del estado en revisión, tiene un nivel intermedio de seguridad de la información que se ve reflejada en los diversos documentos e

implementación que ha realizado y que se ha podido constatar en la revisión. Es importante poder cubrir dichos falencias detectadas para que se pueda resguardar la confidencialidad, disponibilidad e integridad de la información que se administra.

Se recomienda la implementación de establecimiento de las Responsabilidades y la Comunicación de incidencias. Para ello se podrían tomar como referencias marcos internacionales como COBIT 5.0 (desarrollado en este proyecto de fin de carrera, refiérase a los Sub-dominios DSS02-Gestiónar requerimientos de Servicio e Incidentes y DSS03-Gestionar Problemas) así como también ITIL v3 (refiérase al libro de Operación de Servicio, sección de Gestión de Incidencias).

Además se sugiere poder desarrollar y aprobar por parte de la Alta Gerencias los siguientes documentos:

- ✓ Política de Uso de Información obtenida de los sistemas: donde se indique cómo debería de utilizarse y las medidas de seguridad a considerar en la administración de la información que se ha obtenido desde los sistemas de información de la empresa estatal.
- ✓ Acuerdos de información compartida: Acuerdos de confidencialidad en el que el colaborador de la empresa estatal se comprometa a tener un celo riguroso en la divulgación y administración de la información que requiere y utiliza en la ejecución de sus funciones.

CAPÍTULO 5:
CONCLUSIONES Y RECOMENDACIONES

Por la efectividad de las pruebas realizadas el presente proyecto de fin de carrera se presenta como una herramienta muy útil en el proceso de evaluación en el cumplimiento de las Normas Técnicas Peruanas NTP-ISO/IEC 17799 y NTP-ISO/IEC 27001 que se quiera realizar a las empresas del estado que estén regidas por la regulación pertinente que las obliga a tenerlas implementadas.

La presentación de estos procedimientos de auditoría de cumplimiento son resultado de la motivación generada por las capacidades obtenidas al llevar los cursos del área de Tecnologías de Información del plan de estudios de la especialidad Ingeniería Informática de la Pontificia Universidad Católica del Perú. Esto es una llamada a poder tener más atención en esta área ya que se necesitan cubrir estos vacíos que se presentan en el escenario informático nacional, pues se declara la obligatoriedad de las NTP tener los mecanismos de poder verificar su cumplimiento. [ONGEI 2010b]

Es vital reconocer que estos procedimientos están enfocados únicamente para escenarios de empresas del estado, por lo que se recomienda poder trasladarlo a empresas del sector privado, para ocasionar una mejor calidad en Seguridad de Información en ambos grupos (público y privado) dónde el mayor beneficiario serán los ciudadanos y por consiguiente las empresas y/u organizaciones.

La actualización de las normas ISO 27001 e ISO 27002 en su versión del año 2013 no afectan a la aplicabilidad de los procedimientos presentados en este proyecto ya que éstos se basan en las NTP que son equivalentes a las normas ISO 27001 e ISO 27002 en su versión del año 2005.

REFERENCIAS

BIBLIOGRAFÍA

ALLEN, Julia

2005 Governing for Enterprise Security. Technical Note. CMU/SEI-2005-TN-023. Estados Unidos: Software Engineering Institute

BOSWORTH, Seymour, M.E. KABAY y Eric WHYNE

2002 Computer security handbook. 5ª edición. Estados Unidos: John Wiley & Sons.

HUBER, George

1990 A theory of effects of advanced information technologies on organizational design, intelligence and decision making.

INDECOPI - Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual

2006 TECNOLOGÍA DE LA INFORMACIÓN Procesos del Ciclo de Vida del Software (2nd ed.). Lima: Comité de Reglamentos Técnicos y Comerciales de INDECOPI.

ISACA - Information Systems Audit and Control Association

2011 Manual de preparación para el examen de certificación CISA (Certification Information System Auditor) USA: ISACA Publishing

2012 COBIT 5.0 ® for Information Security USA: ISACA Publishing

ISO - International Organization for Standardization

2002 ISO 19011:2002 Directrices para la auditoría de los sistemas de gestión de calidad y/o ambiental. Suiza: ISO.

2004 ISO/IEC 13335-1:2004 Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management. Suiza: ISO.

2005 ISO/IEC 27002:2008 Information technology - Security techniques – Information security risk management. Suiza: ISO.

2008 ISO/IEC 27005:2008 Information technology - Security techniques – Information security risk management. Suiza: ISO.

2009 Information technology - Security techniques - Information security management systems - Overview and vocabulary. Suiza: ISO.

ITGI – Informatic Technology Governance Institute

2003 IT Governance Executive Summary.

ITGI - IT Governance Institute

2008 The Val IT Framework 2.0 Extract. USA: IT Governance Institute.

MORTON, Michael

1988 Information Technology and Corporate Strategy.

ONGEI – Oficina Nacional de Gobierno Electrónico e Informática

2010a Encuesta de Seguridad 2010. Consulta: 27 de mayo 2012. <http://www.pcm.gob.pe/Transparencia/Resol_ministeriales/2010/RM-187-2010-PCM.pdf>

2010b Resumen de los Resultados de la Encuesta de Seguridad 2010, pp. 44-57. Consulta: 27 de mayo de 2012. <http://www.ongei.gob.pe/eventos/Programas_docu/57/Programa_417.pdf>

PAULK, Mark y otros

1993 Key Practices of the Capability Maturity Model Version 1.1Software Engineering Institute. Paper 171. Consulta: 13 de abril de 2012 <http://repository.cmu.edu/sei/171/>

PIATTINI, Mario y Emilio DEL PESO

2001 Auditoría Informática: un enfoque práctico. 2ª edición. España: Alfaomega.

TUPIA, Manuel

2010 Administración de la seguridad de información. Tupia Consultores y Auditores S.A.C. Perú: Graficar

2011 Gobierno de las tecnologías de información bajo la óptica de COBIT 4.1. Tupia Consultores y Auditores S.A.C. Perú.

SA - Standards Australia

2004 AS/NZS 4360:2004 Administración de riesgos. Australia: SA.