PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA UN CENTRO CULTURAL BINACIONAL

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

Nelson Kal Montoya Pachas

ASESOR: Moisés Antonio Villena Aguilar

Lima, Diciembre de 2012

Resumen

La seguridad de información es un tema que muchas organizaciones deben ser capaces de manejar, ya que esto asegura que la organización tenga la capacidad para minimizar los efectos negativos que puedan verse reflejados en sus activos de información, producto de los riesgos a los que están expuestos dichos activos.

Deberán definirse reglas para poder asegurar que la información que maneja la organización sea confidencial, íntegra, disponible y auditable en términos de seguridad. Caso contrario uno de los activos más importantes para una organización, como es la información, seguirá siendo vulnerable ante las amenazas, lo que podría provocar severas pérdidas para la empresa, así como también daños a la reputación de la misma por no manejar dichas reglas para el buen tratamiento de la información.

Esta situación no es ajena para un centro cultural binacional, ya que dichas organizaciones manejan información de todos los miembros que pertenecen a estas, así como también manejan información de sus procesos, la cual les vendría bien a pequeñas empresas que buscan emular las actividades brindadas por estos centros y así lograr ser más competitivas en el sector.

Esto motiva a que en el presente proyecto de fin de carrera se diseñe un Sistema de Gestión de Seguridad de Información según el estándar internacional ISO/IEC 27001:2005 para un centro cultural binacional, con el propósito de proteger sus activos de información ante las amenazas a las cuales están expuestos, y de esta manera dar un tratamiento a los riesgos de información presentes en los procesos de la institución.

Dedicatoria

A mi querida familia, en especial a mi madre, Margarita, por enseñarme con sus acciones a dar lo mejor de mí. A mi padre, Luis, por educarme de la mejor manera. A mi amiga, mi compañera, Natalia, por motivarme siempre.

Agradecimientos

Agradezco a mi asesor, el Ingeniero Moisés Villena, por el apoyo brindado. Quiero agradecer al Coordinador de la especialidad, el Doctor Manuel Tupia, por su perseverancia al difundir las diversas áreas de conocimiento de la especialidad en la universidad.

TABLA DE CONTENIDO

Anexos

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Introducción

Hoy en día la Seguridad de Información está tomando más participación en las organizaciones, ya sea por cultura propia o por diversas regulaciones a las cuales están obligadas. Con esta herramienta metodológica de TI se puede atender las necesidades para ejecutar un adecuado tratamiento a los riesgos que está expuesta la organización.

Por otro lado, en la mayoría de las organizaciones se lucha contra una gran resistencia al cambio y de esto se desprende la falta de compromiso a la hora de intentar generar cultura de Seguridad en las mismas. Por este motivo, se opta por agrupar todas las pequeñas medidas tomadas por la seguridad y hacer un gran esfuerzo para realizar actividades y trabajos conjuntos para poder establecer un Sistema de Gestión de Seguridad de Información (SGSI).

En el Perú no se tiene una gran presencia de Centros Culturales Binacionales, es por ello que se ve como oportunidad a este tipo de organización y se toma como base teórica para realizar el diseño de un SGSI con el cual se pueda elaborar el correcto tratamiento para los riesgos presentes en el día a día de esta organización.

A lo largo de este proyecto se entenderán los aspectos necesarios a considerar para poder establecer el diseño de un Sistema de Gestión de Seguridad de Información para un Centro Cultural Binacional. Se abarcarán actividades desde los primeros pasos a realizar como la contextualización de la empresa elegida, teniendo en cuenta la definición de una serie de criterios y análisis de la organización, así como también se realizara la idónea evaluación y tratamiento de riesgos para la organización.

Con este conjunto de actividades y análisis a realizar se busca presentar la manera de poder brindar el camino adecuado para asegurar los activos de información de un Centro Cultural Binacional.

1. Generalidades

En el presente capítulo se presenta:

- La problemática del proyecto.
- El objetivo general del proyecto.
- Los objetivos específicos que se desprenden del objetivo general.
- Los resultados esperados que se tendrán al cumplir con cada objetivo específico.
- El alcance y las limitaciones para el proyecto.
- Los métodos y procedimientos que se usarán para obtener los resultados esperados como desarrollo de los objetivos específicos.
- La justificación del proyecto.
- La planificación del proyecto.
- El marco conceptual para que brinde definiciones para el correcto entendimiento del proyecto.
- El estado del arte para proyectos similares y la discusión del mismo.

1.1. Definición de la problemática

Hoy en día, la información se ha convertido en un activo que al igual que otros activos importantes del negocio, representa un valor significativo para toda organización. En consecuencia, requiere de un tratamiento que asegure su adecuada protección. Esto es muy importante en un creciente ambiente interconectado de negocios, ya que producto de esto la información está expuesta a un mayor rango de amenazas, y encara un mayor número de vulnerabilidades propias del entorno organizacional, que se generan debido a las diversas formas que puede adoptar la información (impresa, escrita en papel, almacenada electrónicamente, transmitida por correo electrónico o por medios electrónicos, mostrada en un video o hablada en una conversación). Independientemente de la forma que tome la información o el medio por el que se distribuya, debe protegerse. [ISO 27002]

La seguridad de información se logra implementando un conjunto de controles, que pueden tomar la forma de políticas, prácticas, procedimientos, estructuras organizativas y funciones de software y hardware. Estos controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados donde sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad y negocios de la organización. [ISO 27002]

Por otro lado, algo que pone en riesgo de pérdida de información, reputacional y económica, es la poca importancia que se le da al área de tecnología de información (TI) en las organizaciones, la misma que es vista como un área de Soporte y no como una parte importante de la organización que genera valor y que maneja todos los procesos de la organización de manera que estén siempre a disposición y puedan brindar facilidades generando herramientas tecnológicas para el día a día de la organización. [TUPIA 2010]

A lo anterior debemos agregar que la cultura organizacional en el Perú no es abundante en el ámbito de seguridad de información, y mucho menos en el caso de los Centros Culturales Binacionales, tal es así que tampoco toman en cuenta aspectos administrativos como la propia modelación de sus procesos (lo cual es importante para

la realización de sus actividades), ya que al tratarse de labores que realizan siempre, no lo ven como algo que pueda servirles, presentándose situaciones en las que dejan pasar los años y no logran evolucionar en ese aspecto.

A partir de lo expuesto previamente, en el presente proyecto de fin de carrera se tiene como propósito elaborar un Sistema de Gestión de Seguridad de Información (SGSI) según el estándar internacional ISO/IEC 27001:2005 para un Centro Cultural Binacional, con el fin de proteger sus activos de información ante las amenazas a las cuales están expuestos, y de esta manera dar un tratamiento adecuado a los riesgos de información presentes en los procesos más importantes del Centro Cultural.

1.2. Objetivo general

Diseñar un Sistema de Gestión de Seguridad de Información (SGSI) para un Centro Cultural Binacional siguiendo las normas internacionales ISO/IEC 27001:2005 e ISO/IEC 27002:2005.

1.3. Objetivos específicos

Tabla 1.1 Objetivos específicos

ID	OBJETIVO ESPECÍFICO
OB1	Modelar los procesos de negocio del Centro Cultural Binacional que forman el alcance del SGSI.
OB2	Identificar y realizar la valorización de los activos de información de los procesos de negocio que conforman el alcance.
OB3	Identificar, analizar y evaluar los riesgos a los cuales están expuestos los activos identificados en el punto anterior.

ID	OBJETIVO ESPECÍFICO
OB4	Seleccionar objetivos de control y controles para el tratamiento de los riesgos identificados en los procesos principales.
OB5	Elaborar la Declaración de Aplicabilidad.
OB6	Elaborar la documentación requerida por las normas adoptadas para el SGSI.

1.4. Resultados esperados

Tabla 1.2 Resultados esperados

ID	RESULTADOS ESPERADOS
RE1	Modelo de los procesos de negocio del Centro Cultural Binacional que forman el alcance del SGSI [OB1].
RE2	Inventario de los activos de información críticos presentes en los procesos de negocio que conforman el alcance [OB2].
RE3	Reporte de análisis del riesgo [OB3].
RE4	Plan de tratamiento del riesgo [OB4].
RE5	Enunciado de Aplicabilidad [OB5].
RE6	Documentación completa para el SGSI solicitada por el estándar ISO/IEC 27001:2005 según el alcance del proyecto [OB6].

1.5. Alcance y limitaciones

El presente proyecto pretende elaborar el diseño de un Sistema de Gestión de Seguridad de Información para un Centro Cultural Binacional, que le permita a dicha

organización, gestionar la seguridad de sus activos, con el objetivo de darles un tratamiento adecuado frente a los riesgos a los que se encuentran expuestos.

La elección del tipo de organización está basada en el hecho que dicha institución maneja información de un negocio no muy común y que por ende depende de su confidencialidad como fuente de su ventaja competitiva. Y también al promocionar la cultura manejan información personal de sus miembros.

Para el caso de este proyecto el sector se circunscribe a un Centro Cultural Binacional de tamaño mediano con sede en Lima, debido a la facilidad que se quiere tener para el levantamiento de información, y basado en que Lima es la ciudad capital del país (motivo por el cual es una de las ciudades más activas en cuanto a turismo).

Los procesos del Centro Cultural Binacional abarcan una serie de temas que van desde lo cultural, ya sean exposiciones de arte, teatro y danza; hasta aspectos como el aprendizaje de la lengua nativa y certificaciones en la misma.

Es por ese motivo que en acuerdo con el Centro se incluyen los siguientes procesos como parte del alcance para la realización del diseño del SGSI:

- Proceso de Matrícula.
- Proceso de exámenes de cursos.
- Proceso de Programación académica.
- Proceso para el servicio de actividades culturales
- Proceso para el servicio de exámenes internacionales.
- Proceso para el servicio de traducciones.

Siendo todos del tipo “operativo” dentro de un mapa de procesos.

Durante el levantamiento de información se llevarán a cabo entrevistas con la empresa perteneciente al sector descrito previamente, con el objetivo de recolectar los aspectos necesarios que se deberán tenerse en cuenta para el modelamiento de los procesos con los que se identificarán activos para el presente proyecto.

Para el desarrollo de este proyecto se seguirán los lineamientos propuestos en las normas internacionales ISO/IEC 27001:2005 e ISO/IEC 27002:2005. Esta decisión se toma debido a que dichas normas son reconocidas a nivel mundial y que se puede realizar una certificación con la norma ISO/IEC 27001:2005 como trabajo futuro.

El desarrollo de este proyecto demanda a su autor la necesidad de conocer a fondo los procesos mencionados previamente, de manera que será necesario hacer visitas a la organización donde se adquirirá la información sobre la cual se basará el modelamiento de los procesos pertenecientes al alcance de este proyecto. Por esta razón se crea una dependencia hacia los representantes de la organización, de los cuales se obtendrá la información, quedando el proyecto supeditado a la disposición que brinden dichos representantes, de manera que de no contarse con el apoyo de estos, el proyecto se verá afectado debido al retraso en el desarrollo de sus actividades. Y esto podrá mermar en la posible reprogramación de fechas de entregas.

Otra particularidad similar a la anterior es que los representantes de la empresa se nieguen a brindar información sobre los subprocesos que ellos manejan, debido a un posible recelo por esta información, siendo este influenciado por el miedo de que está información caiga en manos de organizaciones del mismo rubro que son parte de la competencia que existe en el sector.

Como se mencionó previamente, este proyecto está limitado a tratar sólo los aspectos de Diseño ya que para una posible implementación sería necesaria una inversión en recursos de tiempo, monetarios y de personas por parte de la empresa, situación algo difícil para el autor del proyecto. También es motivo de esta acotación el hecho que no se dispone del tiempo necesario para poder realizar un proyecto más ambicioso como lo mencionado previamente.

1.6. Métodos y procedimientos

En esta sección del capítulo se presentarán los distintos métodos y procedimientos que se deberán llevar a cabo para cumplir con los objetivos específicos planteados en este proyecto.

Primero se presenta la metodología que se seguirá para la conducción del presente proyecto de fin de carrera. Luego de esto, se presentarán los métodos y procedimientos a realizarse con motivo ya mencionado.

1.6.1. Metodología para el proyecto

Como lo indica el objetivo general del proyecto, la conducción del proyecto será realizado siguiendo lo propuesto en la norma internacional ISO/IEC 27001:2005 para elaborar el diseño de un SGSI donde se establezcan una política, objetivos, procesos y procedimientos para el SGSI, relevantes para manejar el riesgo y mejorar la seguridad de la información, para entregar resultados en concordancia con las políticas y objetivos generales de la organización.

1.6.2. Métodos a realizarse en las distintas actividades para el cumplimiento de los objetivos específicos

Se presenta como un primer objetivo el modelamiento de los procesos que intervienen en el alcance, para esta labor se realizarán entrevistas con los representantes de la empresa, para poder definir las entradas, salidas y tareas para dichos procesos. Luego de esto, se procesará la información recopilada y se procederá a realizar el modelamiento utilizando la notación BPMN 2.0.

Acorde a lo anterior, también se realizará la identificación de los activos involucrados en dichos procesos, para lograr este objetivo se utilizarán los diagramas obtenidos en el punto anterior y se utilizará la norma ISO/IEC 27005:2008 para poder realizar una correcta identificación y valoración de dichos activos.

Se deberá definir una metodología para identificar, analizar y evaluar los riesgos de información presentes en los procesos pertenecientes al alcance. Una vez definida la metodología se deberá realizar un análisis de los riesgos para cada uno de los procesos utilizando dicha metodología.

Se dará un tratamiento a los riesgos encontrados utilizando los controles propuestos en la norma ISO/IEC 27002:2005. El marco COBIT se empleará como contenedor de las normas ISO de seguridad.

Finalmente se elaborará la declaración de aplicabilidad según lo indicado en la norma ISO/IEC 27001:2005 y se concluirá la documentación requerida para la etapa de diseño de un SGSI según esta norma.

1.7. Justificación y viabilidad

Este proyecto tiene como objetivo elaborar el diseño de un SGSI para un Centro Cultural Binacional. Este SGSI permitirá, a dicha organización, gestionar la seguridad de la información que maneja, de manera que se pueda cumplir con la preservación de la confidencialidad, integridad y disponibilidad de la información.

En cuanto a las implicaciones prácticas, este proyecto pretende ofrecer una herramienta que gestione la seguridad, y de los activos de información presentes en los principales procesos de un Centro Cultural Binacional, tales como los mencionados en el alcance del presente proyecto. Por esto, el presente proyecto se circunscribe a un Centro Cultural Binacional que satisfaga dicho alcance. Se realizará el correspondiente levantamiento de información de esta organización, y se adoptará la lógica de negocio manejada en ella para los procesos incluidos en el alcance.

En cuanto al valor teórico, se puede desprender el aporte generado en este proyecto para lo que se refiere al diseño de un SGSI para este tipo de organizaciones, quedando documentado todo el procedimiento necesario para tal ejecución en el

presente documento. Esto es importante ya que en el país no existe precedente para este tipo de diseño con este tipo de organizaciones.

La viabilidad en el aspecto técnico para el proyecto está asegurada ya que se usarán herramientas para su desarrollo que no incurrirá en gastos extras para el ejecutante. Así mismo, hay que agregarle el uso de estándares internacionales para la ejecución de las actividades necesarias en el del proyecto, lo que dará una pauta segura y comprobada para seguir en este proyecto lo que garantiza un correcto desarrollo de las actividades requeridas y buen uso de los recursos y herramientas con las que se cuentan.

En términos económicos también se rescata la viabilidad del proyecto. Como se mencionó, el ejecutante ya cuenta con ciertas herramientas que le permitirán desarrollar el proyecto sin problema alguno; debido a que se trata de un proyecto de fin de carrera, el ejecutante dispone de ciertos beneficios por parte de la institución académica a la cual presentará el proyecto a su finalización, siendo esta institución un apoyo en cuanto a la obtención de herramientas para el desarrollo se refiere, tales como los estándares, normas o marcos necesarios para la elaboración del diseño.

La institución académica que exige el desarrollo de un proyecto como parte de su malla de cursos, otorga un periodo de 4 meses para la ejecución de este, lo cual, teniendo en cuenta el alcance del proyecto, se puede asegurar la viabilidad en términos temporales. Vale mencionar, que el alumno asume su responsabilidad como único ejecutante y asegura contar con el tiempo y la dedicación necesaria para el desarrollo del proyecto, ya sea liberándose de otras cargas o por el contrario haciendo una no asunción de las mismas.

1.8. Plan de proyecto

A continuación se presenta el cronograma de actividades en diagrama de Gantt.

EDT	Nombre de tarea	Duración	Comienzo	Fin
1	**Diseño de SGSI para Centro Cultural Binacional**	**66 días**	**lun 20/08/12**	**lun 19/11/12**
1.1	**Elaboración de Anteproyecto**	**5.5 días**	**lun 20/08/12**	**lun 27/08/12**
1.1.1	Definición del problema	0.5 días	lun 20/08/12	lun 20/08/12
1.1.2	Objetivo general	0.5 días	lun 20/08/12	lun 20/08/12
1.1.3	Objetivos específicos	0.5 días	mar 21/08/12	mar 21/08/12
1.1.4	Resultados Esperados	0.5 días	mar 21/08/12	mar 21/08/12
1.1.5	Alcance y Limitaciones	0.5 días	mié 22/08/12	mié 22/08/12
1.1.6	Métodos y procedimientos	0.5 días	mié 22/08/12	mié 22/08/12
1.1.7	Justificación y Viabilidad	0.5 días	jue 23/08/12	jue 23/08/12
1.1.8	Marco conceptual	1 día	jue 23/08/12	vie 24/08/12
1.1.9	Estado del arte y revisón	1 día	vie 24/08/12	lun 27/08/12
1.2	**Características de un Centro Cultural Binacional**	**18.5 días**	**lun 27/08/12**	**jue 20/09/12**
1.2.1	Modelado de los procesos	13.5 días	lun 27/08/12	jue 13/09/12
1.2.2	Identificación de activos	2 días	vie 14/09/12	lun 17/09/12
1.2.3	Valoración de activos	4 días	lun 17/09/12	jue 20/09/12
1.3	**Diseño del SGSI**	**42 días**	**vie 21/09/12**	**lun 19/11/12**
1.3.1	Definir metodología de riesgos	5 días	vie 21/09/12	jue 27/09/12
1.3.2	Identificar los riesgos	6 días	vie 28/09/12	vie 05/10/12
1.3.3	Analizar y evaluar los riesgos	8 días	lun 08/10/12	mié 17/10/12
1.3.4	Identificar y evaluar tratamiento de los riesgos	3 días	jue 18/10/12	lun 22/10/12
1.3.5	Seleccionar controles	10 días	mar 23/10/12	lun 05/11/12
1.3.6	Elaborar documento de aplicabilidad	4 días	mar 06/11/12	vie 09/11/12
1.3.7	Mapeo con COBIT	4 días	lun 12/11/12	jue 15/11/12
1.3.8	Conclusiones y recomendaciones	2 días	vie 16/11/12	lun 19/11/12

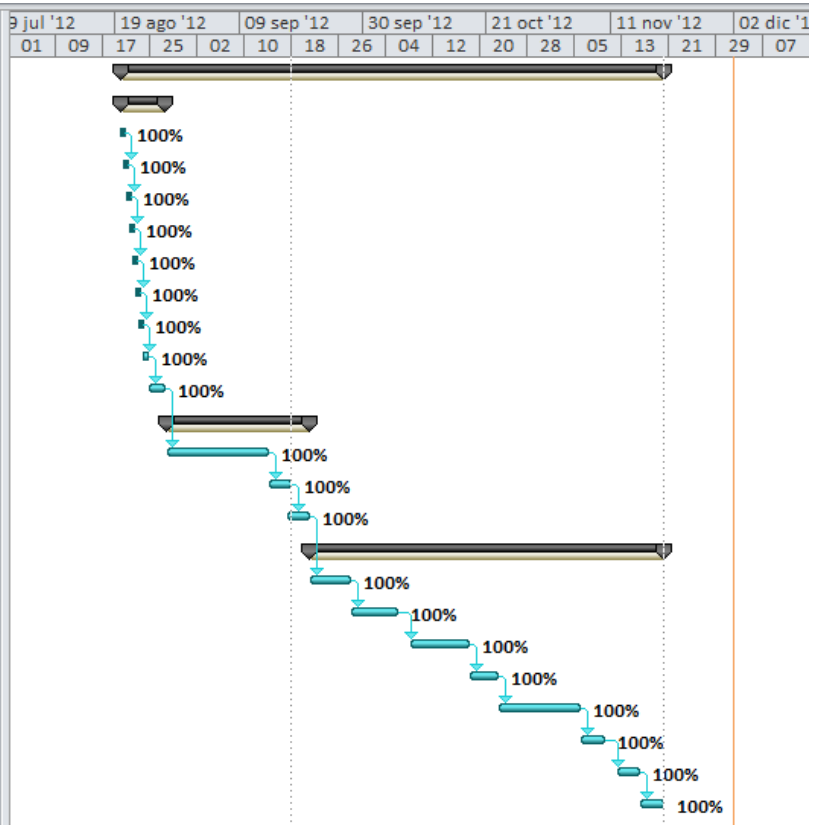

Figura 1.1 Plan de proyecto

A continuación se muestra el EDT obtenido.

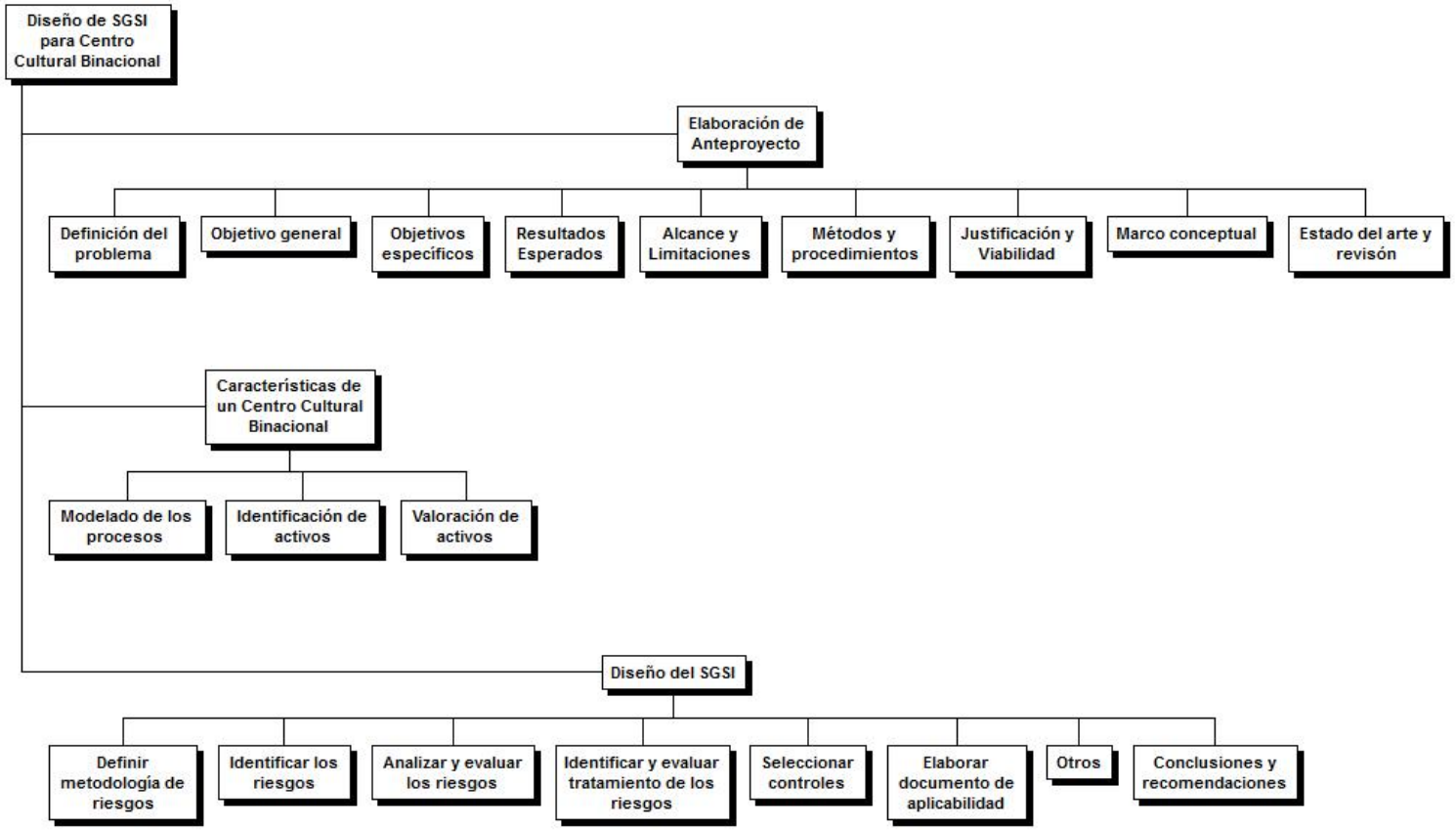

Figura 1.2 EDT del proyecto

1.9. Marco conceptual

A continuación se presentarán conceptos que enmarcan un mejor contexto para lo tratado en el presente proyecto:

1.9.1. Definiciones

Activo

Algo que tenga valor para lo organización. [ISO 13335]

Control

Herramienta de la gestión del riesgo, incluido: políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal. [ISO 27002]

Pauta

Descripción que aclara que es lo que se debe hacer y cómo se hace, con el fin de alcanzar los objetivos planteados en las políticas. [ISO 13335]

Instalaciones de proceso de información

Sistemas de información, servicio o infraestructura, o locaciones físicas que los almacena. [ISO 27002]

Seguridad de la información

Preservación de la confidencialidad, integridad y disponibilidad de la información, así mismo, otras propiedades como la autenticidad, no rechazo, contabilidad y confiabilidad también pueden ser consideradas. [ISO 27002]

Evento de seguridad de información

Es una ocurrencia identificada de un sistema, servicio, o red el cual indica una posible brecha de la política de seguridad de información o fallas de las salvaguardias o una situación desconocida que puede ser relevante para la seguridad. [ISO 18044]

Incidente de seguridad de información

Es indicado por una o varias series de eventos inesperados y no deseados que tienen una gran probabilidad de comprometer las operaciones de negocios y de amenazar la seguridad de información. [ISO 18044]

Política

Dirección general y formal expresada por la gerencia. [ISO 73]

Terceros

Persona que es reconocida por ser independiente de las partes involucradas concerniente al tema en cuestión. [ISO 73]

Amenaza

Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización. [ISO 13335]

Vulnerabilidad

Debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas. [ISO 13335]

Riesgo

Combinación de la probabilidad de un evento y sus consecuencias. [ISO 73]

Análisis del riesgo

Uso sistemático de la información para identificar fuentes y estimar el riesgo. [ISO 73]

Valoración del riesgo

Proceso de comparación del riesgo estimado contra el criterio del riesgo dado para determinar el significado de este. [ISO 73]

Gestión del riesgo

Actividades coordinadas para dirigir y controlar una organización considerando el riesgo. Gestión del riesgo incluye típicamente evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo y comunicación del riesgo. [ISO 73]

Tratamiento del riesgo

Proceso de selección e implementación de medidas para modificar el riesgo. [ISO 73]

Evaluación del riesgo

Proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo. [ISO 73]

Riesgo residual

El riesgo remanente después del tratamiento del riesgo. [ISO 73]

Aceptación de riesgo

Decisión de aceptar el riesgo. [ISO 73]

Disponibilidad

La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada. [ISO 13335]

Confidencialidad

La propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no-autorizados. [ISO 13335]

Integridad

La integridad es la garantía de que los datos sean correctos y de la completitud de la información. [TUPIA 2010]

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. [TUPIA 2010]

Enunciado de aplicabilidad

Enunciado documentado que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI de la organización. [ISO 27001]

1.9.2. Normas y prácticas

Familia de normas ISO/IEC 27000:2005

La adecuada gestión de la seguridad de la información hace necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

La familia de normas ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Dentro de dichos estándares se tienen:

- ISO/IEC 27001:2005

  Es el estándar principal de la serie y contiene los requisitos para el desarrollo de un sistema de gestión de seguridad de la información. Se basó en la BS 7799-

2:2002 (no vigente). Los SGSI se certifican actualmente contra este estándar por auditores externos a las organizaciones.

Este estándar internacional promueve la adopción de un enfoque del proceso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización. [ISO 27001]

Este estándar internacional fomenta que sus usuarios enfaticen la importancia de [ISO 27001]:

- ✓ Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información.
- ✓ Implementar y operar controles para manejar los riesgos de la seguridad de la información.
- ✓ Monitorear y revisar el desempeño y la efectividad del SGSI.
- ✓ Mejoramiento continuo en base a la medición del objetivo.

El estándar adopta el modelo PDCA o también conocido como el “Ciclo de Deming” (Figura 1.3).

Presenta lo siguiente para cada etapa [ISO 27001]:

- ✓ Planear (establecer el SGSI): Establecer la política, objetivos, procesos y procedimientos para el SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información, para entregar resultados en concordancia con las políticas y objetivos generales de la organización.
- ✓ Hacer (implementar y operar el SGSI): Implementar y operar la política, controles, procesos y procedimientos para el SGSI.
- ✓ Chequear (monitorear y revisar el SGSI): Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas del SGSI y reportar los resultados a la gerencia para su revisión.

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

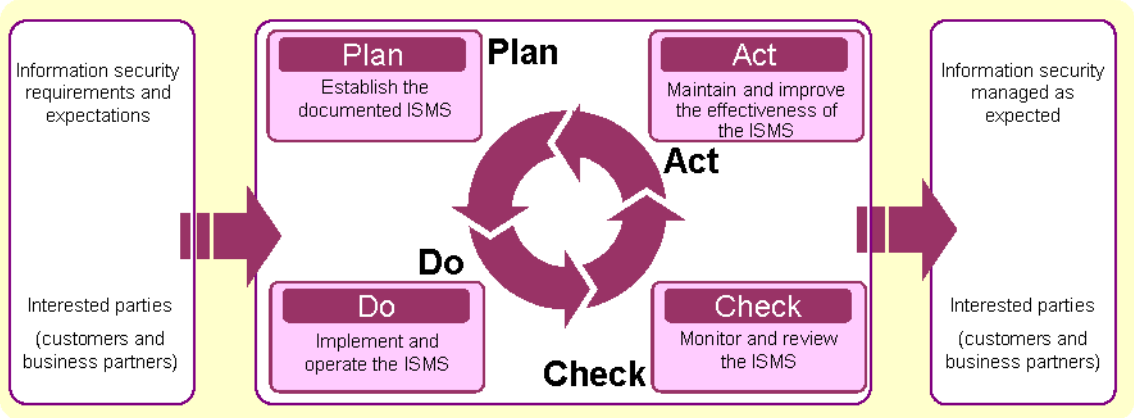

Figura 1.3Ciclo de Deming [ISO 27001]

- ISO/IEC 27002:2005

  Es una guía de prácticas que describe los objetivos de control y los controles recomendables en cuanto a seguridad de la información. Desde el año 2007 es la nueva denominación de la norma ISO/IEC 17799 y por lo tanto, no es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. La norma ISO 27001 contiene un anexo que resume los controles de ISO/IEC 27002:2005. [ISO 27002]

  Esta norma ofrece recomendaciones para realizar la gestión de la seguridad de la información que pueden utilizarse por los responsables de iniciar, implantar o mantener y mejorar la seguridad en una organización. Persigue proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad. [ISO 27002]

La norma puede servir como una guía práctica para desarrollar estándares organizacionales de seguridad y practicas efectivas de la gestión de seguridad. Igualmente, permite proporcionar confianza en las relaciones entre organizaciones. Las recomendaciones que se establecen en esta norma deberían elegirse y utilizarse de acuerdo con la legislación aplicable en la materia. [ISO 27002]

Presenta la siguiente estructura [ISO 27002]:

- ✓ Política de seguridad.
- ✓ Organizando la seguridad de información.
- ✓ Gestión de activos.
- ✓ Seguridad en recursos humanos.
- ✓ Seguridad física y ambiental.
- ✓ Gestión de comunicaciones y operaciones.
- ✓ Control de acceso.
- ✓ Adquisición, desarrollo y mantenimiento de sistemas de información.
- ✓ Gestión de incidentes de los sistemas de información.
- ✓ Gestión de la continuidad del negocio.
- ✓ Cumplimiento.

Figura 1.4. Dominios de la norma ISO/IEC 27002 [ISO 27002]

- ISO/IEC 27003:2010

  Este Estándar Internacional se enfoca en los aspectos críticos que se necesitan para lograr el diseño e implementación satisfactoria de un SGSI según la ISO/IEC 27001:2005. Describe el proceso de especificación y diseño de un SGSI desde la concepción hasta la elaboración de los planes de implementación. Este estándar describe el proceso para la obtención del apoyo de la alta gerencia de la organización para la implementación del SGSI, provee una guía sobre como planificar el SGSI, obteniendo como resultado un plan de implementación para el SGSI. [ISO 27003]

Este estándar internacional propone recomendaciones y aclaraciones, no especifica ningún requerimiento. Está hecho para trabajar en conjunto con la ISO/IEC 27001:2005 e ISO/IEC 27002:2005, pero no para modificar y/o reducir los requerimientos especificados en la norma ISO/IEC 27001:2005 o las recomendaciones propuestas en ISO/IEC 27002:2005. [ISO 27003]

Presenta las siguientes clausulas [ISO 27003]:

- ✓ Obtención de la aprobación de la alta gerencia para iniciar el SGSI.
- ✓ Definir el alcance y la política para el SGSI.
- ✓ Conducción del análisis de la organización.
- ✓ Conducción de la valorización y el plan de tratamiento de riesgos.
- ✓ Diseñar el SGSI.

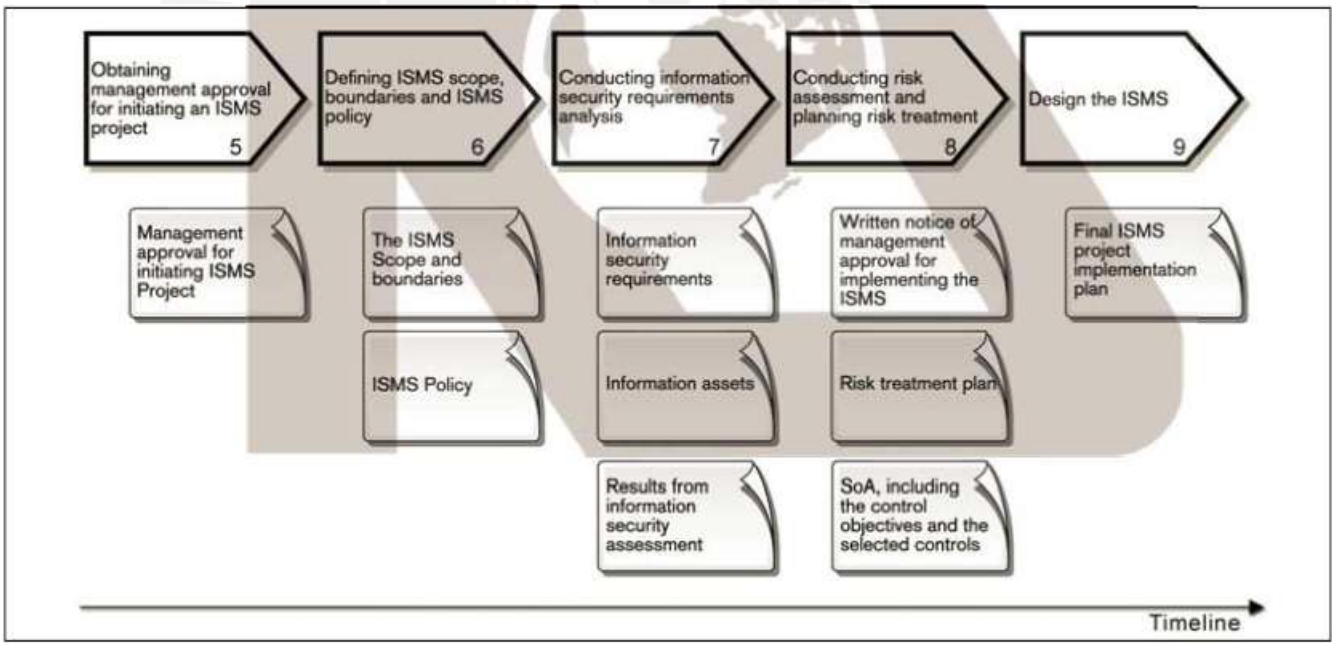

Figura 1.5. Cláusulas de la norma ISO/IEC 27003 [ISO 27003]

- ISO/IEC 27005:2008

Este estándar internacional provee lineamientos para la gestión del riesgo de la la seguridad de información apoyando los conceptos generales especificados en el ISO/IEC 27001:2005 y está diseñado para asistir la implementación adecuada de la seguridad basada en un enfoque del riesgo. Proporciona directrices para la gestión del riesgo, sin embargo, no proporciona ninguna metodología específica para el análisis del mismo. [ISO 27005]

El estándar presenta la siguiente estructura de cláusulas [ISO 27005]:

- ✓ Alcance.
- ✓ Normativa asociada.
- ✓ Términos y definiciones.
- ✓ Estructura del estándar.
- ✓ Background.

- ✓ Generalidades sobre el proceso de gestión de riesgos de seguridad de información.
- ✓ Estableciendo el contexto.
- ✓ Ciclo de vida de la gestión de riesgos.
- ✓ Tratamiento del riesgo de seguridad de información.
- ✓ Aceptación del riesgo de seguridad de información.
- ✓ Comunicación del riesgo de seguridad de información.
- ✓ Monitoreo y revisión de la gestión de riesgos de seguridad de información.

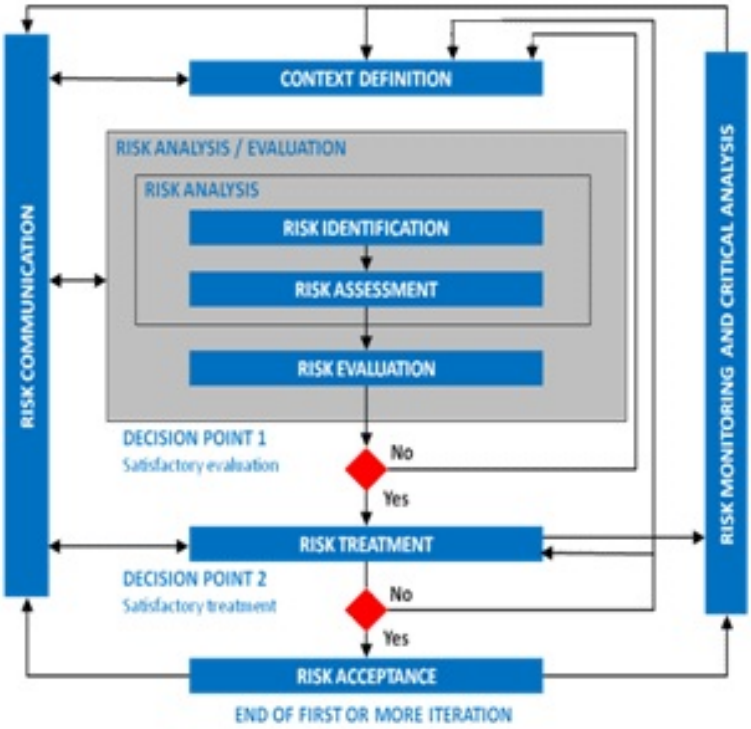

Figura 1.6. Ciclo de vida del Riesgo [ISO 27005]

Ley 29733 - Protección a los datos personales

La Ley 29733 se promulgó con el objetivo de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, el cual señala que toda persona tiene derecho: “A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar”. Esta protección se pretende lograr a través de un adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en la Constitución Política del Perú se reconocen.

El ámbito de aplicación de la Ley es hacia los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional. Son objeto de especial protección los datos sensibles. [CRP 2011]

La ley presenta la siguiente estructura [CRP 2011]:

- ✓ Título I: Principios rectores.
- ✓ Título II: Tratamiento de datos personales.
- ✓ Título III: Derechos del titular de datos personales.
- ✓ Título IV: Obligaciones del titular y del encargado del banco de datos personales.
- ✓ Título V: Bancos de datos personales.
- ✓ Título VI: Autoridad Nacional de Protección de Datos Personales.
- ✓ Título VII: Infracciones y sanciones administrativas.

COBIT 5

Es la última edición de este marco mundialmente aceptado, el cual proporciona una visión empresarial del Gobierno de TI que tiene a la tecnología y a la información como protagonistas en la creación de valor para las empresas. ISACA® lanzó el 10 de abril de 2012 la nueva versión de este marco de referencia.

El marco empieza su introducción indicando que la información es un recurso clave para todas las empresas, y desde el momento en que la información se ha creado hasta el momento en que se destruye, la tecnología juega un papel importante. Por otro lado increpa que la Tecnología de la Información es cada vez más avanzada y se ha extendido en las empresas y en entornos públicos, sociales y de negocios.

Se presenta a COBIT 5 como un marco integral que facilita la labor de las empresas para que de esta manera sean capaces de alcanzar sus objetivos de gobierno y de gestión de las TI. Dicho de otra manera, ayuda a las empresas a crear valor óptimo de

las TI manteniendo un balance entre la obtención de beneficios y la optimización de los niveles de riesgo y el uso de los recursos. [ISACA 2012]

Este marco permite que las TI se rijan y administren de manera integral para toda la empresa, tomando a la empresa de extremo a extremo y a las áreas funcionales de responsabilidad de TI, teniendo en cuenta los intereses que tienen en las TI, los grupos de interés externos e internos. [ISACA 2012]

COBIT se basa en cinco (5) principios (Figura 1.7) para el gobierno y la administración de las TI en las empresas [ISACA 2012]:

- ✓ Identificar las necesidades de los grupos de interés: COBIT provee todos los procesos necesarios para dar soporte a la creación de valor en la empresa a través del uso de las TI. Este marco puede ser aterrizado al contexto en el que se encuentra la empresa de manera que los objetivos del negocio se puedan trasladar a objetivos específicos y manejables para las TI y se utilicen los procesos propuestos en él.
- ✓ Cubrir y conocer al negocio: Se trata de integrar el Gobierno de TI con el Gobierno de la empresa. De esta manera se acerca al área de TI con todos los procesos de la empresa.
- ✓ Aplicar un marco integrado simple (se sugiere COBIT).
- ✓ Habilitar un enfoque holístico: Se trata de ver a las TI como un todo y no como entidades separadas una de las otras.
- ✓ Separa Gobierno de Gestión: COBIT hace una clara distinción entre gobierno y administración. Estas disciplinas enmarcan distintos tipos de actividades, requieren distintas estructuras organizacionales y sirven a distintos propósitos.

Estos cinco (5) principios permiten que la empresa pueda elaborar un marco de gobierno y administración efectivo que optimice la inversión y el uso en TI para el beneficio de los grupos de interés.

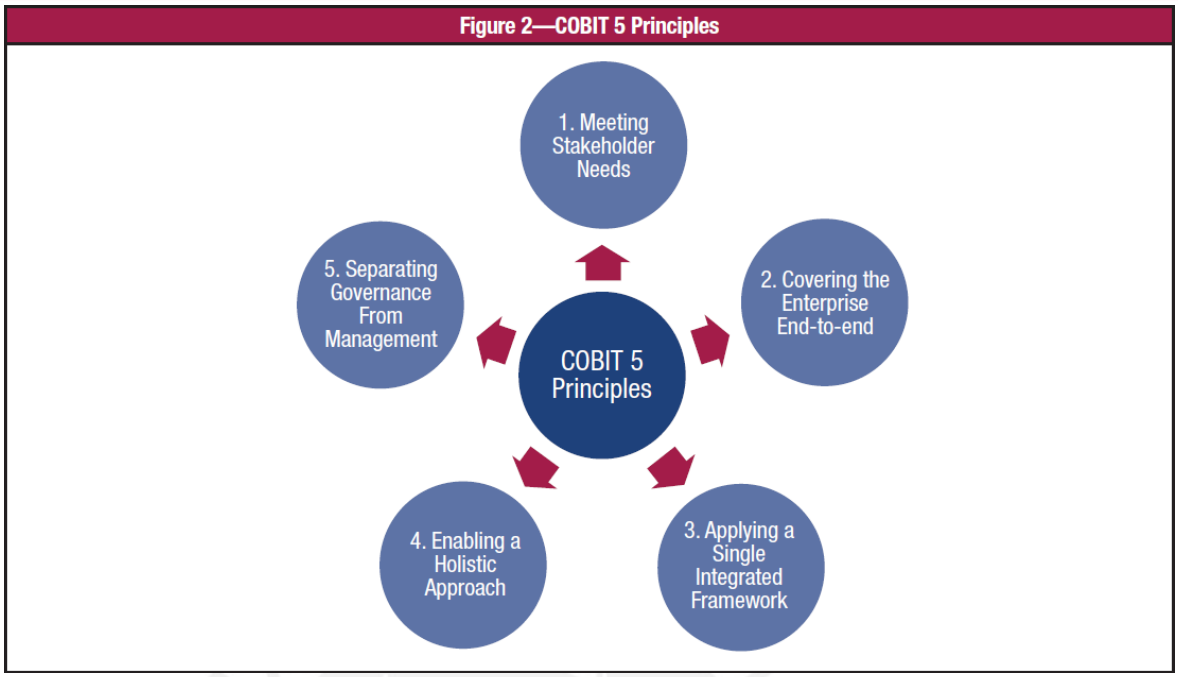

Figura 1.7. Principios de COBIT [ISACA 2012]

COBIT, tomando como base cada uno de estos principios, y a la vez la inclusión de procesos de los marcos "Risk IT" y "Val IT", propone distintos procesos de gobierno y administración, agrupados en los siguientes dominios (Figura 1.8):

- ✓ Evaluar, Dirigir y Monitorear (EDM).
- ✓ Alinear, Planificar y Organizar (APO).
- ✓ Construir, Adquirir e Implementar (BAI).
- ✓ Difundir, Servir e Soportar (DSS).
- ✓ Monitorear, evaluar y valorar (MEA).

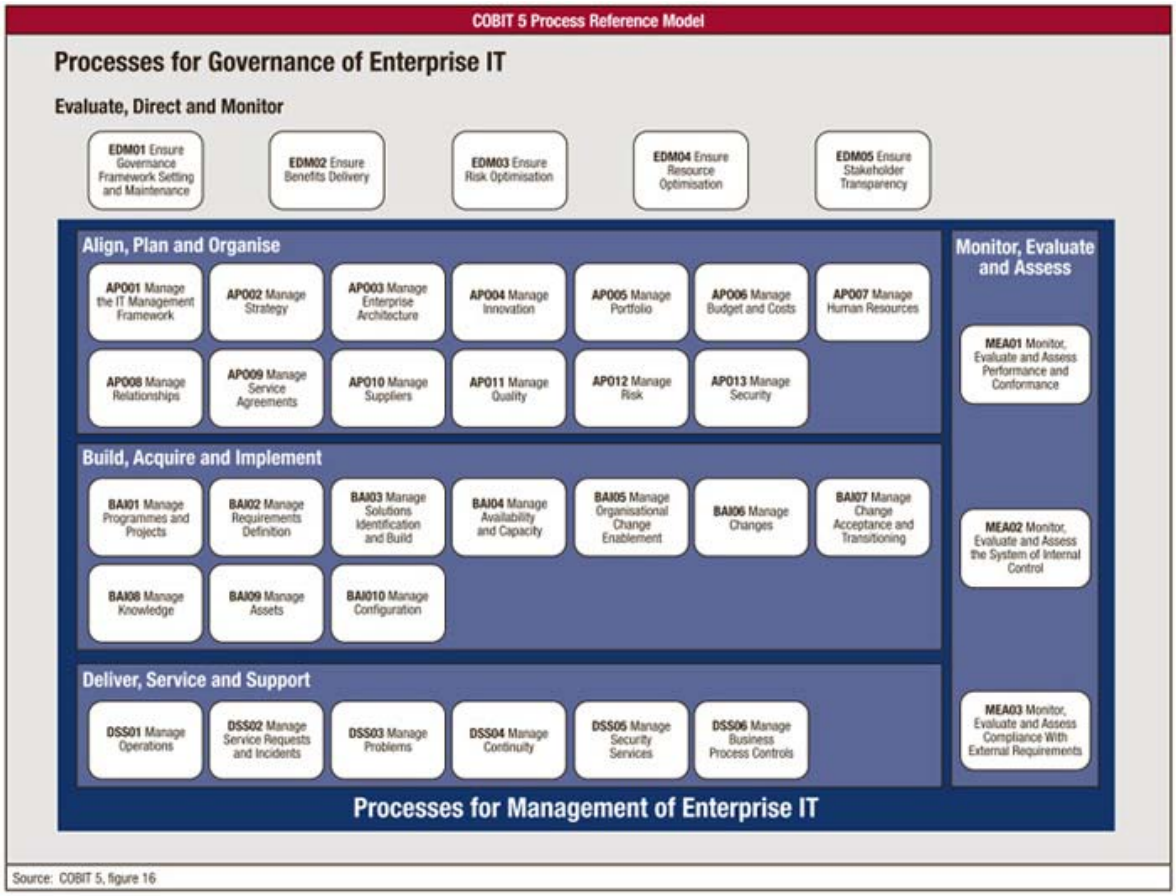

Figura 1.8. Modelo de referencia de los procesos de COBIT [ISACA 2012]

1.10. Revisión del estado del arte

Para el proyecto bastará con la realización del diseño de un SGSI basándonos en la norma ISO/IEC 27001:2005. Pero se presentará a continuación la situación mundial en cuanto a certificaciones sobre dicha norma, es decir casos completos con implementación del SGSI en la organización.

A la fecha existen 7940 organizaciones certificadas con la norma ISO/IEC 27001:2005, siguen la distribución mostrada en la Figura 1.9.

Japan	4152	Netherlands	24	Belgium	3
UK	573	Saudi Arabia	24	Gibraltar	3
India	546	UAE	19	Lithuania	3
Taiwan	461	Bulgaria	18	Macau	3
China	393	Iran	18	Albania	3
Germany	228	Portugal	18	Bosnia Herzegovina	2
Czech Republic	112	Argentina	17	Cyprus	2
Korea	107	Philippines	16	Ecuador	2
USA	105	Indonesia	15	Jersey	2
Italy	82	Pakistan	15	Kazakhstan	2
Spain	72	Colombia	14	Luxembourg	2
Hungary	71	Russian Federation	14	Macedonia	2
Malaysia	66	Vietnam	14	Malta	2
Poland	61	Iceland	13	Mauritius	2
Thailand	59	Kuwait	11	Ukraine	2
Greece	50	Canada	10	Armenia	1
Ireland	48	Norway	10	Bangladesh	1
Austria	42	Sweden	10	Belarus	1
Turkey	35	Switzerland	9	Bolivia	1
Turkey	35	Bahrain	8	Denmark	1
France	34	Peru	7	Estonia	1
Hong Kong	32	Chile	5	Kyrgyzstan	1
Australia	30	Egypt	5	Lebanon	1
Singapore	29	Oman	5	Moldova	1
Croatia	27	Qatar	5	New Zealand	1
Slovenia	26	Sri Lanka	5	Sudan	1
Mexico	25	South Africa	5	Uruguay	1
Slovakia	25	Dominican Republic	4	Yemen	1
Brazil	24	Morocco	4	**Total**	**7940**

Figura 1.9. Distribución de organizaciones certificadas a nivel mundial [IIUG 2012]

De las 7940 organizaciones certificadas a nivel mundial se puede apreciar que el nombre de Perú figura con 7 certificaciones en su haber (al 13 de Septiembre de 2012), siendo dichas organizaciones las mostradas en la Figura 1.10.

Name of the Organization	Country	Certificate Number	Certification Body	Standard BS 7799-2:2002 or ISO/IEC 27001:2005
GMD	Peru	SAC 0705104	LRQA	ISO/IEC 27001:2005
HERMES TRANSPORTES BLINDADOS S.A.	Peru	GB12/85495	SGS United Kingdom Ltd	ISO/IEC 27001:2005
Hochschild Minning PLC	Peru	IS 525891		ISO/IEC 27001:2005
Oficina de Normalisacación Previsonal (ONP)	Peru	01 153 04012	TÜV Rheinland	ISO/IEC 27001:2005
Telefonica del Peru	Peru	179684	Bureau Veritas Certification	ISO/IEC 27001:2005
Telefonica Empresas	Peru	179684	Bureau Veritas Certification	ISO/IEC 27001:2005
TELEFONICA GESTION DE SERVICIOS COMPARTIDOS PERU S.A.C.	Peru	GB10/79313	SGS United Kingdom Ltd	ISO/IEC 27001:2005

Figura 1.10.Organizaciones certificadas en el Perú [IIUG 2012]

1.11. Discusión sobre los resultados del estado del arte

En los acápites anteriores, se ha observado definiciones, descripciones de normas y marcos de las cuales se puede entender que existe numerosa información en cuanto a temas de seguridad de la información y la gestión de los riesgos. También se ha vislumbrado el hecho que una cantidad considerable de empresas están certificadas con la norma ISO/IEC 27001:2005 a nivel mundial.

Pero en contraposición a esto, el Perú no es uno de los países que presenta alto número de organizaciones certificadas, por el contrario sólo 7 organizaciones a nivel nacional están certificas, de las cuales ninguna es un Centro Cultural Binacional o

afín. Situación que se da por diversos factores tales como la cultura o estructura organizacional que tienen las empresas en el país, lo que no permite el acoplamiento de diversos marcos de gobierno y por ende no se aplican o se logra con dificultad.

Podemos desprender de lo expuesto la novedad que representa realizar el diseño de un Sistema de Gestión de Seguridad de Información para un Centro Cultural Binacional en este país como tema de este proyecto de fin de carrera.

2. Características de un Centro Cultural Binacional para el SGSI

En el presente capítulo se hará la presentación oficial de los procesos indicados en el alcance, para tal labor se hará una descripción de los mismos, así como también se presentará su moldeamiento con la notación BPMN 2.0. Posterior a esto, se elaborará la identificación y valoración de los activos de información presentes en dichos procesos.

2.1. Modelamiento de los procesos del Centro Cultural Binacional

Como se entiende el primer paso para el diseño del SGSI es realizar el moldeamiento de los procesos incluidos en el alcance, pertenecientes al Centro Cultural binacional. Para los procesos que se mencionarán, se tiene como dueño del proceso al Director General de la organización, ya que este es quien determina los resultados para estos, así como también las actividades que se deberán realizar para lograr dichos resultados. Los procesos son los siguientes:

- Proceso de Matrícula

  Es uno de los principales procesos que generan casi la totalidad de los ingresos para la organización. El objetivo de este proceso es realizar las actividades necesarias para lograr concretar la matrícula de un alumno en uno de los cursos que ofrece la organización. El gerente de este proceso es el Supervisor de Servicios Administrativos.

  Este proceso inicia con la intención de un cliente (alumno) de participar en uno de los cursos pertenecientes a los programas ofrecidos por la organización. En él se debe asignar una reserva de horario para realizar un pago posterior y así concretar la matrícula. Para dicha reserva es necesario que el alumno tenga un nivel de cursos asociado, en caso de no tener un nivel asociado, el alumno podrá rendir un examen de clasificación para de esta manera asociarle un nivel o registrar sus datos y empezar desde el nivel más básico.

  Existe también la posibilidad de hacer una modificación en dicha matrícula dentro de un periodo establecido por la organización para así poder brindar las facilidades necesarias al alumno de manera que pueda vivir una mejor experiencia en la organización.

  El modelamiento de este proceso se encuentra en el **Anexo H**.

- Proceso de exámenes de cursos

  El objetivo de este proceso es administrar las evaluaciones para los cursos que se dictan en la organización de manera que se logre satisfacer la demanda de estas. El gerente de este proceso es el Supervisor de Servicios Administrativos.

  Este proceso inicia con el abastecimiento de nuevas evaluaciones y hojas de respuestas por parte de las sedes, es decir con la solicitud que se realiza a

Imprenta, abarca actividades de actualización de plantillas y exámenes, así como también el almacenamiento de los mismos por parte de las sedes.

Como se indica, también se presentan actividades para distribución de las evaluaciones y el retorno de los mismos, así como el registro de notas obtenidas por parte del alumnado.

El modelamiento de este proceso se encuentra en el **Anexo I**.

- Proceso de Programación académica

El objetivo de este proceso es satisfacer la demanda mensual de cursos que se presenta en la organización. El gerente de este proceso es el Supervisor de Servicios Administrativos.

En este proceso se vislumbra la manera en la que la organización dictará los cursos mes a mes.

El proceso inicia con la elaboración de la lista de los cursos que se dictarán, a su vez se ven actividades para la asignación de profesores y aulas según los criterios que la organización maneja.

Se ejecutan también actividades de actualización debido a la demanda real que se vive en la organización, ya que este proceso está ligado al proceso de matrícula.

El modelamiento de este proceso se encuentra en el **Anexo J**.

- Proceso para el servicio de actividades culturales

El objetivo de este proceso es preparar una agenda cultural anual para la promoción de actividades culturales que se llevarán a cabo en las sedes

pertenecientes a la organización, así como la gestión necesaria para la realización de dichas actividades. El gerente de este proceso es el Director Cultural.

El proceso inicia con la preparación de la agenda cultural anual, para lo cual se definen una serie de eventos en acuerdos con distintos artistas. Posterior a esto se debe definir la forma en la cual se dará el servicio de entradas a los eventos ya que la organización puede tomar la decisión de trabajar en acuerdo con una empresa dedicada a la venta de entradas. Finalmente se evalúa la recaudación lograda y se definen los pagos que se realizarán a los artistas por concepto de los servicios brindados en los eventos.

El modelamiento de este proceso se encuentra en el **Anexo K**.

- Proceso para el servicio de exámenes internacionales

El objetivo de este proceso es brindar el servicio de certificación en el manejo de otro idioma a distintos clientes o grupos de clientes, como pueden ser organizaciones o colegios. Este servicio también es necesario para aquellos que quieren ser profesores de los cursos que brinda el Centro Cultural. El gerente de este proceso es el Director Académico.

El proceso inicia con la inscripción de un participante para las evaluaciones programadas. Como se mencionó este servicio puede prestarse también a grupos o colegios para lo cual será necesario realizar un acuerdo con la Dirección de Exámenes Internacionales de la organización.

Se ven también las actividades que se realizarán para la calificación de dichas evaluaciones ya que se emitirán certificados a nombre de instituciones internacionales.

El modelamiento de este proceso se encuentra en el **Anexo L**.

- Proceso para el servicio de traducciones

  El objetivo de este proceso es brindar un servicio de traducción de documentos al público en general. Se traducen documentos especiales o documentos generales como partidas de nacimiento, diplomas, etc. El gerente de este proceso es el Director Académico.

  Este servicio se puede realizar también por Internet, sin necesidad que el cliente se aproxime a las inmediaciones de la organización. Inicia con la solicitud de traducción de algún documento, abarca actividades que se realizan para la elaboración de la cotización de dichos documentos, así como también el proceso de traducción en sí.

  En la empresa existen 2 formas de ofrecer este servicio, motivo por el cual el modelamiento se realizará en 2 diagramas distintos.

  El modelamiento de este proceso se encuentra en los **Anexos M** y **N**.

Para todos los procesos presentados se entiende que los operativos del proceso (personas encargadas de llevar a cabo las actividades del proceso) serán las que aparezcan en los diagramas del modelamiento.

2.2. Identificación de los activos de información

“No se puede proteger lo que no se conoce” está simple pero muy importante frase, que menciona [TUPIA 2010], nos incita a repasar el por qué se realizó el modelamiento de los procesos en el acápite anterior. Pues bien, la respuesta a ello es poder determinar en cada proceso los activos involucrados, esto permitirá poder realizar una

buena gestión de riesgos asociados a los procesos de negocio del Centro Cultural Binacional.

En el **Anexo A** se presenta el inventario de activos realizado en el Centro Cultural a manera de tabla conteniendo las siguientes columnas:

- ID: Será el identificador del activo.
- Activo: Es el nombre del activo o la manera en la que se le identifica en el Centro Cultural.
- Proceso: Proceso al cual pertenece el activo o en el que participa.
- Tarea: Tarea del proceso en la que está presente el activo.
- Descripción: Descripción del activo
- Tipo: Indica si el activo es primario o secundario.
- Tangible: Indica si el activo es tangible o no.

2.3. Valoración de los activos de información

Posterior a la identificación de activos se debe establecer la escala a utilizar y los criterios para la asignación de un lugar determinado en dicha escala a cada activo, sobre la base de la valoración.

Debido a la diversidad de activos que se encuentren dentro de la mayoría de las organizaciones es probable que algunos activos que tienen un valor monetario conocido se valoren monetariamente, mientras que otros que tienen un valor más cualitativo se les puede asignar un valor en dicha escala que vaya, de "muy bajo" a "muy alto".

La decisión de utilizar una escala cuantitativa versus una escala cualitativa es realmente una cuestión de preferencia organizacional. Ambos tipos de valoración podrían ser utilizados para el mismo activo. [ISO 27005]

Para realizar la valoración de los activos de información debemos primero definir una escala para cada criterio que tendremos en cuenta. Los criterios serán: disponibilidad, integridad, confidencialidad.

La escala cualitativa se puede apreciar en la Tabla 2.1.

Tabla 2.1 Criterios de escala cualitativa

Criterio	Valor del Activo Según el Criterio	Clase	Descripción
Disponibilidad	0	No aplica/ No es relevante	Se puede tolerar que el activo no esté disponible
	1	Baja disponibilidad	Se puede tolerar que el activo no esté disponible por más de un día
	2	Disponibilidad mediana	Se puede tolerar que el activo no esté disponible por máximo medio o un día
	3	Alta disponibilidad	No se puede tolerar que el activo no esté disponible por unos horas o inclusive menos
Integridad	0	No aplica/ No es relevante	El daño o modificación no autorizada no genera impacto negativo en la empresa
	1	Baja integridad	El daño o modificación no autorizada genera un impacto insignificante o menor en la empresa
	2	Integridad mediana	El daño o modificación no autorizada genera un impacto significativo en la empresa
	3	Integridad alta	El daño o modificación no autorizada genera un impacto importante en la empresa y podría conllevar a falla grave o total de empresa
Confidencialidad	0	No aplica/ No es relevante	Activo de “vox pópuli”
	1	Disponible al público	Activo disponible para el público en general
	2	Para uso interno solamente	Activo disponible dentro de la organización con restricciones variadas con base en las necesidades de la empresa

Criterio	Valor del Activo Según el Criterio	Clase	Descripción
	3	Estrictamente confidencial	Activo disponible sólo sobre la base de la necesidad estricta del conocimiento

Para finalizar la valoración se obtendrá como valor del activo la suma de los valores por criterio que obtenga cada uno. Los activos que se tendrán en cuenta para la realización del proyecto serán los que obtengan un valor mayor o igual a 5 de acuerdo al apetito de riesgo del Centro Cultural.

En el **Anexo B** se vuelven a presentar los activos a manera de tabla pero esta vez se mostrará su valor según los criterios previamente definidos, esta tabla presentará las siguientes columnas:

- ID: Identificador de activo.
- Activo: Nombre del activo o como se le denomina en el Centro Cultural.
- Disponibilidad: Valor del criterio de disponibilidad del activo.
- Integridad: Valor del criterio de integridad del activo.
- Confidencialidad: Valor del criterio de confidencialidad del activo.
- Valor: Valor cualitativo estimado del activo.

3. Identificación y evaluación de Riesgos

En el presente capítulo se elaborará el mapa de riesgos adecuado a los activos seleccionados para ser tratados en el presente proyecto, para esto se deberán definir previamente la metodología de riesgos a utilizar. De igual manera una vez definida la metodología se realizará el análisis de riesgo pertinente. Posteriormente, una vez realizado el análisis se determinarán controles para el tratamiento tomando como base los indicados en la ISO/IEC 27002. Finalmente se realizará un mapeo entre los controles seleccionados para el tratamiento y los procesos del marco COBIT 5, para mostrar la relación entre la norma y el marco.

3.1. Mapa de riesgos

Como se indica en la introducción de este capítulo, el primer paso será definir una metodología para la gestión de los riesgos. Dentro de las posibilidades existentes se ha

rescatado el uso de la norma ISO/IEC 27005. Esta norma proporciona directrices para la gestión del riesgo en la seguridad de la información en una organización, dando soporte particular a los requisitos de un sistema de gestión de seguridad de la información (SGSI) de acuerdo con la norma ISO/IEC 27001 (usada como guía para la elaboración de este proyecto), y es por este motivo el que se cree conveniente el uso de la misma como metodología de riesgos. Sin embargo, esta norma no brinda ninguna metodología específica para la gestión del riesgo en la seguridad de la información, pero proporciona en sus cláusulas un proceso para la gestión de riesgos, es por ello que la norma puede utilizarse como metodología en sí. [ISO 27005]

Una vez aceptada la norma como metodología, se procede a realizar el análisis de la misma para ejecutar las indicaciones que en ella encontramos. Como primera instancia la norma menciona que se debe establecer el contexto para la gestión de riesgo. Este contexto determina los criterios básicos para la gestión del riesgo. Dentro de estos criterios se encuentran los criterios de impacto y probabilidad.

Como marco inicial para estos conceptos de criterios se debe entender el significado de un “escenario de incidente”, es la descripción de una amenaza que explota una vulnerabilidad determinada o un conjunto de vulnerabilidades en un incidente de seguridad de información. Los conceptos de impacto y probabilidad están asociados a este de escenario de incidente, de manera tal que se ve a la probabilidad de ocurrencia como una amenaza que explota una vulnerabilidad con una probabilidad determinada, y al impacto como el impacto que afecta en el negocio en caso de produjese dicho escenario de incidente. [ISO 27005]

Para ambos conceptos se presenta una escala desde un nivel llamado “Muy bajo/a” hasta el denominado “Muy alto/a”, y para cada uno se ha tomado en cuenta lo que pretende expresar el Centro Cultural con cada una de estas denominaciones, tal y como lo indica la norma, acerca de la contextualización de los criterios.

A continuación se presenta el significado de tales denominaciones para cada criterio, en la Tabla 3.1 y en la Tabla 3.2.

Tabla 3.1 Criterios de impacto

Impacto producido por el escenario		
ID	**Valor**	**Descripción**
1	Muy Bajo	Los procesos relacionados no se verían afectados y se podrían continuar normalmente con su desarrollo.
2	Bajo	Los procesos relacionados se verían afectados y se requeriría de poco menos de una hora para poder continuar con su desarrollo.
3	Medio	Los procesos relacionados se verían afectados y se requeriría de pocas horas para poder continuar con su desarrollo.
4	Alto	Los procesos relacionados se verían afectados y se requeriría de pocos días para poder continuar con su desarrollo.
5	Muy Alto	Los procesos relacionados se verían afectados por tiempo indefinido superior a una semana para poder continuar con su desarrollo.

Tabla 3.2 Criterios de probabilidad

Probabilidad de ocurrencia del escenario		
ID	**Valor**	**Descripción**
1	Muy Baja	El escenario en mención ocurre rara vez en la empresa. En el aspecto temporal se puede decir que sucede una vez cada cinco años.
2	Baja	El escenario en mención ocurre ocasionalmente en la empresa. En el aspecto temporal se puede decir que sucede una vez al año.
3	Media	El escenario en mención ocurre eventualmente en la empresa. En el aspecto temporal se puede decir que sucede una vez al mes.
4	Alta	El escenario en mención ocurre con frecuencia en la empresa. En el aspecto temporal se puede decir que sucede una vez a la semana.

5	Muy Alta	El escenario en mención ocurre con notable continuidad en la empresa. En el aspecto temporal se puede decir que sucede más de una vez a la semana.

La norma indica, como siguiente paso, que se realice la valoración del riesgo de seguridad de información. Remarca que los riesgos se deberían identificar, describir cuantitativa o cualitativamente y priorizar frente a los criterios de evaluación del riesgo y los objetivos relevantes para la organización. [ISO 27005]

Un riesgo es una combinación de consecuencias que se presentarían después de la ocurrencia de un evento indeseado y de su probabilidad de ocurrencia. La valoración del riesgo cuantifica o describe cualitativamente el riesgo y permite a los directores priorizar los riesgos de acuerdo con su gravedad percibida u otros criterios establecidos. El propósito de la identificación del riesgo es determinar qué podría suceder que cause una pérdida potencial, y llegar a comprender el cómo, dónde y por qué podría ocurrir esta pérdida.[ISO 27005]

En base ello, el siguiente paso es realizar la identificación de los riesgos, para lo cual previamente se deberán identificar los eventos que podrían desencadenar el riesgo y por ende se deben detallar las amenazas y vulnerabilidades que conforman los escenarios de estos eventos.

Una amenaza puede causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a las organizaciones. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas. Es recomendable identificar tanto los orígenes de las amenazas accidentales como de las deliberadas. Una amenaza puede tener su origen dentro o fuera de la organización y algunas pueden afectar a más de un activo, generando distintos impactos en cada escenario. [ISO 27005]

Se presenta en la norma una lista de posibles amenazas a encontrarse en las organizaciones, la cual será tomada como lista de posibles amenazas para el Centro Cultural.

La siguiente lista, reflejada en la Tabla 3.3, muestra para cada tipo de amenaza donde D (deliberado), A (accidental), E (ambiental) es relevante. D se utiliza para todas las acciones deliberadas dirigidas a los activos de información, A se utiliza para todas las acciones humanas que pueden dañar accidentalmente los activos de información, y E se utiliza para todas las incidencias que no se basan en las acciones humanas.

Tabla 3.3 Lista de amenazas

Tipo	Amenaza	Origen
Daño Físico	Fuego	A, D, E
	Daños por agua	A, D, E
	Contaminación del medio ambiente	A, D, E
	Accidente grave	A, D, E
	Destrucción de los equipos o medios de comunicación	A, D, E
	Polvo, corrosión, congelación	A, D, E
Eventos naturales	Fenómeno climático	E
	Fenómeno sísmico	E
	Fenómeno volcánico	E
	Fenómeno meteorológico	E
	Inundación	E
Pérdida de servicios esenciales	Fallo del sistema de suministro de aire acondicionado o de agua	A, D
	Pérdida del suministro de energía	A, D, E
	Falla de equipos de telecomunicaciones	A, D
Perturbación debido a radiación	Radiación electromagnética	A, D, E
	Radiación térmica	A, D, E
	Pulsos electromagnéticos	A, D, E
Compromiso de información	Interceptación de señales	D
	Espionaje remoto	D
	Escucha ilegal	D
	Robo de multimedia o documentos	D
	Robo de equipos	D
	Recuperación de multimedia reciclados o desechados	D
	Divulgación	A, D
	Datos procedentes de fuentes no confiables	A, D

Tipo	Amenaza	Origen
	Manipulación de hardware	D
	Manipulación de software	A, D
	Detección de posición	D
Fallas técnicas	Fallo de equipo	A
	Mal funcionamiento de equipo	A
	Saturación del sistema de información	A, D
	Mal funcionamiento de software	A
	Incumplimiento de mantenimiento del sistema de información	A, D
Acciones no autorizadas	Uso de equipo sin autorización	D
	Copia fraudulenta de software	D
	Uso de software falsificado o copiado	A, D
	Datos corruptos	D
	Tratamiento ilegal de datos	D
Compromiso de funciones	Error en el uso	A
	Abuso de los derechos	A, D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento de la disponibilidad de personal	A, D, E

También se presenta una lista de amenazas con fuente de causas humana, se puede ver en la Tabla 3.4.

Tabla 3.4 Lista de amenazas de causa humana

Origen de la amenaza	Amenaza
Hacker, cracker	Hacking
	Ingeniería social
	Intrusión, accesos forzados al sistema
	Acceso no autorizado al sistema
Criminal de computación	Crimen computacional
	Actos fraudulentos
	Información corrupta
	Suplantación de identidad
	Intrusiones en el sistema

Origen de la amenaza	Amenaza
Terrorista	Bomba
	Guerra de información
	Ataques al sistema
	Penetración al sistema
	Manipulación del sistema
Espionaje industrial	Ventaja de defensa
	Ventaja política
	Explotación económica
	Robo de información
	Intrusión a información personal
	Ingeniería social
	Penetración al sistema
	Acceso no autorizado al sistema
Intrusos	Asalto a empleado
	Chantaje
	Intromisión a información personal
	Abuso del ordenador
	Fraude y robo
	Información corrupta
	Ingreso de datos corruptos o falsos
	Intercepción
	Código malicioso
	Venta de información personal
	Errores en el sistema
	Intromisión al sistema
	Sabotaje al sistema

Una vulnerabilidad no causa daño por sí misma, dado que es necesario que haya una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza correspondiente puede no requerir de la implementación de un control, pero es recomendable reconocerla y monitorearla para determinar los cambios. [ISO 27005]

De la misma forma realizada para las amenazas, se debe hacer una identificación de las vulnerabilidades existentes para cada activo. En la Tabla 3.5 se muestra una lista de estas.

Tabla 3.5 Lista de vulnerabilidades

Tipos	Ejemplos de vulnerabilidades
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.
	Falta de esquemas de reemplazo periódico
	Susceptibilidad a la humedad, el polvo y la suciedad
	Sensibilidad a la radiación electromagnética
	Falta de control de cambio con configuración eficiente
	Susceptibilidad a las variaciones de tensión
	Susceptibilidad a las variaciones de temperatura
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Falta o insuficiencia de la prueba del software
	Defectos bien conocidos en el software
	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado
	Falta de pruebas de auditoría
	Distribución errada de los derechos de acceso
	Software de distribución amplia
	Utilización de los programas de aplicación a los datos errados en términos de tiempo
	Interfaz de usuario complicada
	Falta de documentación
	Configuración incorrecta de parámetros
	Fechas incorrectas
	Falta de mecanismos de identificación y autentificación, como la autentificación de usuario
	Tablas de contraseñas sin protección
	Gestión deficiente de las contraseñas
	Habilitación de servicios innecesarios
	Software nuevo o inmaduro
	Especificaciones incompletas o no claras para los desarrolladores

Tipos	Ejemplos de vulnerabilidades
	Falta de control eficaz del cambio
	Descarga y uso no controlados de software
	Falta de copias de respaldo
	Falta de protección física de las puertas y ventanas de la edificación
	Falla en la producción de informes de gestión
Red	Falta de prueba del envío o la recepción de mensajes
	Líneas de comunicación sin protección
	Tráfico sensible sin protección
	Conexión deficiente de los cables.
	Punto único de falla
	Falta de identificación y autentificación de emisor y receptor
	Arquitectura insegura de la red
	Transferencia de contraseñas autorizadas
	Gestión inadecuada de la red (capacidad de recuperación del enrutamiento)
	Conexiones de red pública sin protección
Personal	Ausencia del personal
	Procedimientos inadecuados de contratación
	Entrenamiento insuficiente en seguridad
	Uso incorrecto de software y hardware
	Falta de conciencia acerca de la seguridad
	Falta de mecanismos de monitoreo
	Trabajo no supervisado del personal externo o de limpieza
	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos
	Ubicación en un área susceptible de inundación
	Red energética inestable
	Falta de protección física de las puertas y ventanas de la edificación
Organización	Falta de procedimiento formal para el registro y retiro del registro de usuario
	Falta de proceso formal para la revisión (supervisión) de los derechos de acceso
	Falta o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes

Tipos	Ejemplos de vulnerabilidades
	Falta de procedimiento de monitoreo de los recursos de procesamiento información
	Falta de auditorías (supervisiones) regulares
	Falta de procedimientos de identificación y evaluación de riesgos
	Falta de reportes sobre fallas incluidos en los registros de administradores y operador
	Respuesta inadecuada de mantenimiento del servicio
	Falta o insuficiencia en el acuerdo a nivel de servicio
	Falta de procedimiento de control de cambios
	Falta de procedimiento formal para el control de la documentación del SGSI
	Falta de procedimiento formal para la supervisión del registro del SGSI
	Falta de procedimiento formal para la autorización de la información disponible al público
	Falta de asignación adecuada de responsabilidades en la seguridad de la información
	Falta de planes de continuidad
	Falta de políticas sobre el uso del correo electrónico
	Falta de procedimientos para la introducción del software en los sistemas operativos
	Falta de registros en los logs de administrador y operario.
	Falta de procedimientos para el manejo de información clasificada
	Falta de responsabilidades en la seguridad de la información en la descripción de los cargos
	Falta o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados
	Falta de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información
	Falta de política formal sobre la utilización de computadores portátiles
	Falta de control de los activos que se encuentran fuera de las instalaciones
	Falta o insuficiencia de política sobre limpieza de escritorio y de pantalla
	Falta de autorización de los recursos de procesamiento de la información
	Falta de mecanismos de monitoreo establecidos para las brechas en la seguridad
	Falta de revisiones regulares por parte de la gerencia

Tipos	Ejemplos de vulnerabilidades
	Falta de procedimientos para la presentación de informes sobre las debilidades en la seguridad
	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales

Para esto se tomarán los activos valorizados que satisfacen el apetito de riesgo del Centro Cultural y se realizarán para ellos una identificación de las amenazas y vulnerabilidades correspondientes para dichos activos. Esta asignación se apreciará en la tabla del **Anexo C** que cuenta con las columnas:

- IDV: identificación de activo en la valorización.
- Proceso: Proceso al cual pertenece el activo.
- Activo: Activo de información que satisface exigencias de la valorización de activos.
- Vulnerabilidad: Posible vulnerabilidad del activo.
- Amenaza: Amenaza a la cual está expuesta el activo.

Posteriormente, con las vulnerabilidades y amenazas identificadas, se puede realizar la identificación de las consecuencias. Una consecuencia puede ser la pérdida de la eficacia, condiciones adversas de operación, pérdida del negocio, reputación, daño, etc. [ISO 27005]

Cabe definir previamente la manera en la que se estimarán los riesgos. Una metodología de estimación puede ser cualitativa o cuantitativa, o una combinación de ellas, dependiendo de las circunstancias. En la práctica, con frecuencia se utiliza la estimación cualitativa en primer lugar para obtener una indicación general del nivel del riesgo y revelar los riesgos más importantes. La forma del análisis debería ser consistente con los criterios de evaluación del riesgo desarrollados como parte del establecimiento del contexto.

La estimación cualitativa utiliza una escala de atributos calificativos para describir la magnitud de las consecuencias potenciales (para el caso del presente proyecto se utilizarán los definidos previamente) y la probabilidad de que ocurran dichas

consecuencias. Una ventaja de la estimación cualitativa es su facilidad de comprensión por parte de todo el personal pertinente, mientras que una desventaja es la dependencia en la selección subjetiva de la escala. [ISO 27005]

Para realizar esta estimación se tomará como base un enfoque proporcionado en la norma, el cual enfrenta al impacto de un escenario contra la probabilidad de ocurrencia de dicho escenario, para de esta manera lograr otorgarle un valor al riesgo asociado a dichos grados de impacto y probabilidad. Se obtiene una tabla de nivel de riesgo.

Tabla 3.6 Nivel de riesgo

	Probabilidad de un escenario de incidente	Muy Baja (1)	Baja (2)	Media (3)	Alta (4)	Muy Alta (5)
Impacto en el negocio	Muy Bajo (1)	1	2	3	4	5
	Bajo (2)	2	3	4	5	6
	Medio (3)	3	4	5	6	7
	Alto (4)	4	5	6	7	8
	Muy Alto (5)	5	6	7	8	9

En la Tabla 3.7, se muestran 4 niveles de riesgo que serán claves para la evaluación, dentro de los cuales tenemos: Bajo, medio, alto y crítico. Estos niveles se obtienen determinando primero un nivel de probabilidad de ocurrencia de un escenario de incidente (desde muy baja hasta muy alta) y por otro lado determinando un nivel de impacto en el negocio (desde muy bajo hasta muy alto) con lo que se logra ubicar el escenario de incidente en uno de los 4 niveles de riesgo mencionados. A manera de ejemplo se asume que se tiene un escenario con probabilidad de ocurrencia media (3)

y un impacto alto (4), eso nos daría in nivel de riesgo 6 para lo que se obtiene que el nivel de riesgo sea alto, como se muestra en la siguiente tabla de nivel de riesgo.

Tabla 3.8 Descripción de nivel de riesgo

	Nivel de riesgo
1,2,3	Bajo
4,5	Medio
6,7	Alto
8,9	Crítico

Para poder realizar el análisis de riesgo se tomarán en cuenta los activos de información que están dentro de lo especificado por el Centro Cultural, es decir los que obtuvieron un valor igual o superior a 5 en dicha valorización.

Para todos y cada uno de ellos se determinarán posibles escenarios de incidentes, con los cuales se obtendrá una estimación de nivel de riesgo y de esa manera poder determinar los riesgos más peligrosos para el Centro Cultural y con ellos poder elaborar un plan de tratamiento de riesgos.

Para evaluar los riesgos se utilizará una escala numérica del “1” al “5” donde el menor valor representa al riesgo con mayor prioridad (esto se verá representado para la parte de tratamiento de riesgos), en el caso de coincidir con el nivel encontrado se tomará la decisión de priorizar los riesgos que presenten un mayor impacto en el negocio.

El paso siguiente es elaborar la matriz de riesgos correspondiente para dichos activos seleccionados como parte del análisis.

3.1.1. Matriz de riesgos

En este apartado se elaborará la matriz de riesgos utilizando los criterios antes definidos para la probabilidad de ocurrencia de un escenario de incidente y el impacto que este tendría en la organización, así como también se toman en cuenta las listas de amenazas y vulnerabilidades sugerida por la ISO/IEC 27005 para elaborar dicho análisis.

Esta tabla utilizará las siguientes columnas:

- IDV: identificación de activo en la valorización.
- Proceso: Proceso al cual pertenece el activo.
- Activo: Activo de información que satisface exigencias de la valorización de activos.
- Vulnerabilidad: Posible vulnerabilidad del activo.
- Amenaza: Amenaza a la cual está expuesta el activo.
- IDR: Identificación del posible escenario de incidente.
- Riesgo: Consecuencia del escenario.
- Impacto: Valor cualitativo del impacto del escenario de incidente.
- Probabilidad: Probabilidad de ocurrencia del escenario de incidente.
- Valor: Es el valor cualitativo del escenario de incidente obtenido utilizando el enfoque de la norma ISO/IEC 27005.

En el **Anexo D** se muestra la tabla con el análisis.

Este análisis permitirá determinar el nivel de riesgo que se incluirá en el tratamiento de riesgos, estos serán los riesgos con un nivel crítico o alto.

3.2. Plan de tratamiento de riesgos

Luego de haber obtenido el nivel de riesgo se deberá seleccionar controles para reducir, retener, evitar o transferir los riesgos (que obtuvieron un nivel crítico o alto) y se deberá definir un plan para el tratamiento del riesgo.

Las opciones para este tratamiento se deberían seleccionar con base en el resultado de la evaluación del riesgo, ya que con esta se priorizarán los riesgos, el costo esperado para implementar estas opciones y los beneficios esperados como resultado de tales opciones. Cuando se pueden obtener reducciones grandes en los riesgos con un costo relativamente bajo, se deberían implementar esas opciones. Las opciones adicionales para las mejoras pueden no ser económicas y es necesario estudiarlas para determinar si se justifican o no. [ISO 27005]

Por los motivos anteriores es necesario realizar la labor de asignación de controles en conjunto con el Centro Cultural para poder plasmar sus expectativas en cuanto a reducción del riesgo.

En general, los controles pueden brindar uno o más de los siguientes tipos de protección: corrección, eliminación, prevención, minimización del impacto, disuasión, detección, recuperación, monitoreo y concienciación. Durante la selección del control es importante ponderar el costo de adquisición, implementación, administración, operación, monitoreo y mantenimiento de los controles en comparación con el valor de los activos que se protegen; además, el retorno de la inversión en términos de reducción del riesgo y el potencial para explotar nuevas oportunidades de ejecución que brindan algunos controles también se deberían tomar en consideración. También conviene considerar las habilidades especializadas que pueden ser necesarias para definir e implementar nuevos controles o modificar los existentes. [ISO 27005]

Para la selección de controles se utilizarán los propuestos en la norma ISO/IEC 27002 ya que esta norma proporciona información detallada de los mismos y son adecuados para el trabajo que se viene realizando con la norma ISO/IEC 27001.

En el **Anexo E**se presenta una tabla con los controles que serían convenientes aplicar para la reducción de riesgos asociándolos con dichos riesgos. Dicha tabla cuenta con las siguientes columnas:

- IDR: Identificador del riesgo identificado.
- Riesgo: Riesgo identificado y estimado.
- Evaluación: Priorización del riesgo según los criterios de evaluación.
- Control: Control de la norma ISO/IEC 27002.
- Detalle: Detalle del control de la norma ISO/IEC 27002.

3.3. Mapeo de los controles de la norma ISO/IEC 27002 y el marco COBIT 5

En esta sección se analizará el marco COBIT para realizar un alineamiento de los controles de la norma ISO/IEC 27002, seleccionados en el apartado anterior como parte del tratamiento de los riesgos, hacia los procesos de dicho marco.

Se realiza este alineamiento ya que los controles propuestos en el tratamiento cubren áreas específicas y pueden ser mapeados al marco de referencia COBIT, proporcionando así una jerarquía de materiales de orientación en TI para el Centro Cultural, ya que los controles de dicho marco son modelos de procesos de TI. [ISACA 2008]

Tal cual se presentó en la sección de estado del arte, el marco COBIT presenta procesos para el gobierno de TI agrupados en los siguientes dominios:

- Evaluar, Dirigir y Monitorear (EDM).
- Alinear, Planificar y Organizar (APO).
- Construir, Adquirir e Implementar (BAI).
- Difundir, Servir e Soportar (DSS).

- Monitorear, evaluar y valorar (MEA).

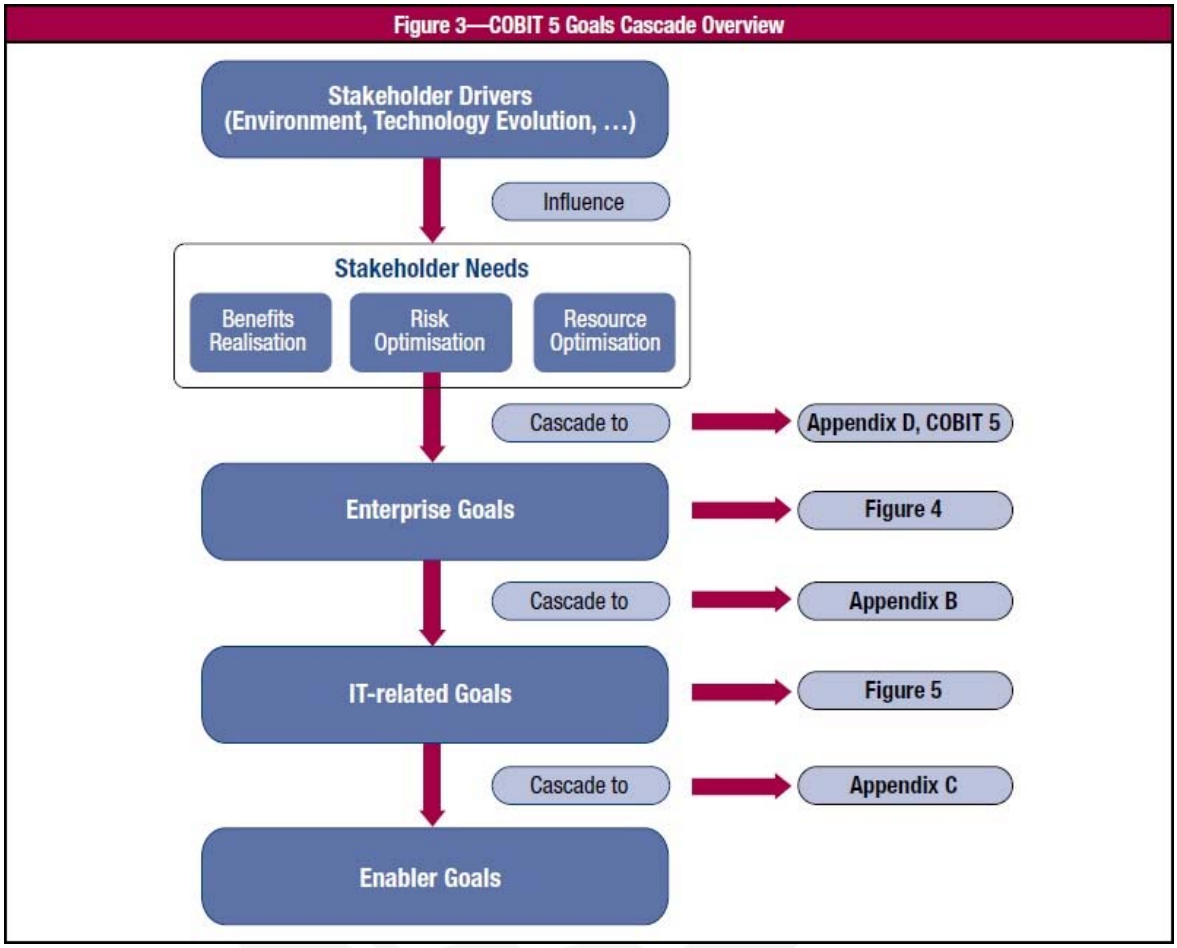

Figura 3.1. Cascada de objetivos de COBIT 5

Para poder realizar el mapeo usaremos la manera de descender hacía los procesos habilitadores que se muestra en la cascada de objetivos del marco, la cual se muestra en la Figura 3.1. La manera de realizar este proceso será identificando primero los objetivos de gobierno propuestos por el marco que apliquen al Centro Cultural.

El marco COBIT propone 17 objetivos de gobierno, como se muestra en la Figura 12. De estos objetivos se han seleccionado los siguientes como aplicables al caso del Centro Cultural:

- Riesgos empresariales gestionados.
- Continuidad y disponibilidad de los servicios de negocio.
- Cumplimiento de políticas internas.

Figure 4—COBIT 5 Enterprise Goals				
BSC Dimension	Enterprise Goal	Relation to Governance Objectives		
		Benefits Realisation	Risk Optimisation	Resource Optimisation
Financial	1. Stakeholder value of business investments	P		S
	2. Portfolio of competitive products and services	P	P	S
	3. Managed business risk (safeguarding of assets)		P	S
	4. Compliance with external laws and regulations		P	
	5. Financial transparency	P	S	S
Customer	6. Customer-oriented service culture	P		S
	7. Business service continuity and availability		P	
	8. Agile responses to a changing business environment	P		S
	9. Information-based strategic decision making	P	P	P
	10. Optimisation of service delivery costs	P		P
Internal	11. Optimisation of business process functionality	P		P
	12. Optimisation of business process costs	P		P
	13. Managed business change programmes	P	P	S
	14. Operational and staff productivity	P		P
	15. Compliance with internal policies		P	
Learning and Growth	16. Skilled and motivated people	S	P	P
	17. Product and business innovation culture	P		

Figura 3.2. Objetivos de gobierno de COBIT 5

El marco cuenta con unos anexos para lograr el descenso donde proporciona unas tablas en las que se relacionan los objetivos de gobierno con los objetivos relacionados a TI (también 17) que propone.

Utilizando esta tabla se logró obtener los objetivos relacionados a TI que se pueden desprender de los objetivos de gobierno seleccionados previamente para el caso del Centro Cultural. Esta relación se muestra en la Tabla 3.8.

Tabla 3.9 Relación de Objetivos de Gobierno y TI

ID	Objetivo Empresarial	ID	Objetivo relacionado a TI
3	Riesgos empresariales gestionados	4	Riesgos empresariales relacionados a TI gestionados
		10	Seguridad de información, infraestructura de procesamiento y aplicaciones
		16	Personal de negocio y TI motivado y competente
7	Continuidad y disponibilidad de los servicios de negocio	4	Riesgos empresariales relacionados a TI gestionados
		10	Seguridad de información, infraestructura de procesamiento y aplicaciones
		14	Disponibilidad de información confiable y útil para la toma de decisiones
15	Cumplimiento de políticas internas	2	Cumplimiento y apoyo de TI para el cumplimiento empresarial de las leyes y reglamentos externos
		10	Seguridad de información, infraestructura de procesamiento y aplicaciones
		15	Cumplimiento de TI con políticas internas

Según la cascada de objetivos de COBIT 5, una vez identificados los objetivos relacionados a TI, se podrá hacer uso de otros de los anexos el cual nos muestra la relación entre los objetivos relacionados a TI y los procesos habilitadores (agrupados por dominios) que satisfacen el logro de dichos objetivos, de ser implantados.

Para tal relación el marco COBIT muestra una escala con dos niveles “P” y “S”.

“P” representa la relación primaria, cuando existe una relación importante, es decir, el proceso de COBIT 5 es un soporte principal para la consecución del objetivo relacionado con a TI.

“S” representa la relación secundaria, cuando todavía hay una fuerte, pero menos importante, relación, es decir, el proceso de COBIT 5 es un soporte secundario para el objetivo relacionado con a TI.

A continuación se muestran 2 tablas en las cuales se muestran los procesos de cada dominio, representados por el número que se les ha otorgado como identificador en el dominio del marco. Los dominios aparecen como columnas y los objetivos relacionados a TI obtenidos previamente, aparecen como filas de cada tabla.

En la Tabla 3.9 se muestran los procesos que satisfacen la relación con el nivel “P”.

Tabla 3.10 Procesos con relación primaria

	CONDICIÓN: "P"	Dominio COBIT				
ID	Objetivo de TI	EDM	APO	BAI	DSS	MEA
2	Cumplimiento y apoyo de TI para el cumplimiento empresarial de las leyes y reglamentos externos	-	1,12,13	10	5	2,3
4	Riesgos empresariales relacionados a TI gestionados	3	10,12,13	1,6	1,2,3,4 ,5,6	1,2,3
10	Seguridad de información, infraestructura de procesamiento y aplicaciones	3	12,13	6	5	-
14	Disponibilidad de información confiable y útil para la toma de decisiones	-	9,13	4,10	3,4	-
15	Cumplimiento de TI con políticas internas	3	1	-	-	1,2
16	Personal de negocio y TI motivado y competente	4	1,7	-	-	1,2
	Compilado	3,4	1,7,9,10, 12,13	1,4,6,10	1,2,3,4 ,5,6	1,2,3

En la Tabla 3.10 se muestran los procesos que satisfacen la relación con nivel “S”.

Tabla 3.11 Procesos con relación secundaria

	CONDICIÓN: "S"	Dominio COBIT				
ID	Objetivo de TI	EDM	APO	BAI	DSS	MEA
2	Cumplimiento y apoyo de TI para el cumplimiento empresarial de las leyes y reglamentos externos	1,3,5	7,10,11	2,9	1,3,4,6	1
4	Riesgos empresariales relacionados a TI gestionados	1,4	1,2,3,4,5,6,7,8,9,11	2,3,4,7,9,10	-	-
10	Seguridad de información, infraestructura de procesamiento y aplicaciones	1	1,3,7,9,10	2,8,9,10	1,2,4,6	1,2,3
14	Disponibilidad de información confiable y útil para la toma de decisiones	1,2,3,5	1,2,3,4,10,11,12	2,3,6,7,8,9	1,2,5,6	1,2
15	Cumplimiento de TI con políticas internas	1,5	2,7,8,9,10,11,12	6,7,9,10	1,2,3,4,5,6	3
16	Personal de negocio y TI motivado y competente	1,2,3	2,8,11,12	1,8	1,4,6	1
	Compilado	1,2,3,4,5	1,2,3,4,5,6,7,8,9,10,11,12	1,2,3,4,6,7,8,9,10	1,2,3,4,5,6	1,2,3

Finalmente se logró obtener los procesos del marco que podrían satisfacer el cumplimiento de los objetivos de gobierno del Centro Cultural (los seleccionados de entre los propuestos por el marco) y de esta manera será más fácil identificar cuáles son los procesos que cubren lo detallado por los controles de la norma ISO/IEC 27002 que forman parte del tratamiento de riesgos del proyecto.

Para el mapeo en sí se mostrará el tipo de cobertura del proceso del marco COBIT, se identificará con la letra “A” (algunos aspectos) a aquellos controles del marco que cubren de manera abierta y general al control de la norma, y con la letra “C” (cubierto) a aquellos que por el contrario cubren gran parte del control de la norma.

En el **Anexo F** se muestra una tabla en la cual se detalla el mapeo a manera de tabla y para cada control se identifica el proceso que lo abarca y la manera de la cobertura.

4. Entregables de un SGSI

En el presente capítulo se presentarán los entregables de un SGSI correspondientes al diseño y que estén considerados dentro del alcance.

4.1. Declaración de aplicabilidad

Corresponde hacer una declaración de aplicabilidad tal como lo exige la norma ISO/IEC 27001, este documento describe los controles relevantes y aplicables al alcance del SGSI del Centro Cultural. En ella se entenderá el porqué de la aplicabilidad de cada control dando primero una adaptación del control de la norma ISO/IEC 27002 al caso del Centro Cultural y posteriormente explicando que tan factible sería su implementación. Se presentará a manera de tabla en el **Anexo G** para cada control:

- El control propiamente dicho, que viene a ser la cláusula de la norma en la cual se hace referencia al tema relacionado al riesgo que se quiere tratar.

- El detalle del control, que es la descripción del control, a manera de indicaciones, las cuales pueden ser aplicadas a la empresa, dependiendo de la situación de esta.
- La adaptación al caso del Centro Cultural, que es la “contextualización” del control a la organización, con la cual se podrá tomar la decisión sobre si es o no factible la implementación de dicho control como medida de seguridad en la empresa.
- La aplicabilidad, se indica si el control aplica o no.
- La justificación, es el porqué de la aplicabilidad de control.

5. Observaciones, Conclusiones y Recomendaciones

En este capítulo se presentarán las observaciones, conclusiones, recomendaciones y trabajos futuros correspondientes al diseño de un SGSI para un Centro Cultural.

5.1. Observaciones

Se encontró una primera gran dificultad al no contar con la documentación correspondiente a los procesos que forman parte del alcance del proyecto, lo que obligó al autor a indagar sobre temas de modelamiento de procesos con la notación BPMN 2.0.Esta situación que fue resarcida gracias a algunas consultas bibliográficas y al apoyo del asesor del presente proyecto, quien es un conocedor del tema de modelamiento de procesos.

La falta de documentos sobre los procesos también obligó al autor a acordar muchas reuniones con la institución para el levantamiento de información sobre los procesos, que de haber contado con la documentación, hubieran sido innecesarias.

Otro aspecto fundamental fue el conjunto de reuniones que se tuvieron con la empresa para concretar la definición de los distintos criterios usados en el proyecto, como también para las valorizaciones que se realizaron en el mismo.

5.2. Conclusiones

Tal como se presenta en este proyecto, la gestión de la seguridad de información no es un tema de mediana envergadura, sino que por el contrario es algo que debe estar ya incluido en la cultura organizacional de las empresas (en este caso el Centro Cultural), lo cual no se podrá lograr sin el apoyo de la alta gerencia como promotor activo de la seguridad en la empresa.

Del mismo modo, se debe establecer que los dueños de los procesos que fueron incluidos en este proyecto, miren de manera diferente la seguridad de la información, y que velen para que de alguna manera se pueda levantar los riesgos encontrados dentro de sus actividades ya que no es seguro que este diseño se logre implementar, y por ello debería ser labor de ellos el tratar de eliminar dichos riesgos.

Debe tenerse en cuenta que el diseño de SGSI presentado se adapta a los objetivos actuales del Centro Cultural en el cual se ha basado el proyecto, y que este podría (y es probable que lo haga) variar ya que los objetivos de gobierno cambiarán y por ello algunos procesos que forman parte del alcance del proyecto, también lo harán.

Se concluye así que el Centro Cultural, y las organizaciones en general deben tomar en cuenta la seguridad de la información de la empresa, y de esta forma proteger su activo más importante, la información, ante las amenazas que están presentes en todos los ambientes organizacionales, es con este activo con el que lograrán alcanzar sus objetivo y también es irrecuperable en algunas ocasiones, en caso de pérdida o robo.

5.3. Recomendaciones y trabajos futuros

En primera instancia se recomienda al Centro Cultural que en base al diseño presentado en este proyecto, se preocupe en concientizar a todas las personas que forman parte de dicha empresa, sobre la seguridad de la información y su importancia. Luego, se recomienda la búsqueda para lograr realizar la implementación de este diseño y que en el futuro se pueda gestionar la seguridad de información de tal manera que se pueda aspirar a una certificación, ya que el diseño ha sido realizado con la norma ISO/IEC 27001, la cual es certificable.

Como trabajos futuros se pueden realizar diseños similares para el centro cultural en los cuales se utilicen otras metodologías para la gestión de riesgos. De manera similar sería interesante que se elabore un plan de continuidad de negocio para un Centro Cultural, lo que permitirá reforzar la seguridad en la empresa. Otra opción, si se contará con la disposición y apoyo total de la alta gerencia, sería la de lograr realizar la implementación de un SGSI para un Centro Cultural y poder alcanzar la certificación de dicho sistema.

Referencias Bibliográficas

[IIUG 2012] ISMS International User Group.
2012 International Register of ISMS Certificates. Consulta: 13 de Septiembre de 2012.
<http://www.iso27001certificates.com/>

[ISO 73] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
2002 ISO/IEC Guide 73:2002. Risk management - Vocabulary - Guidelines for use in standards.

[ISO 13335] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
2004 ISO/IEC 13335-1:2004. Information technology -- Security technique - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management.

[ISO 18044] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
2004 ISO/IEC TR 18044:2004. Information technology - Security techniques - Information security incident management.

[ISO 27001] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
2005 ISO/IEC 27001:2005. Information technology - Security techniques - Information security management systems - Requirements.

[ISO 27002] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION

2005 ISO/IEC 27002:2005. Information technology - Security techniques - Code of practice for information security management.

[ISO 27003] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
2010 ISO/IEC 27003:2010.Information technology - Security techniques - Information security management systems implementation guidance.

[ISO 27005] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
2008 ISO/IEC 27005:2008. Information technology - Security techniques - Information security risk management.

[TUPIA 2010] TUPIA, Manuel
2010 Administración de la Seguridad de Información. Primera edición. Lima: Tupia Consultores y Auditores S.A.C.

[ISACA 2012] Information Systems Audit and Control Association
2012 COBIT 5.Control Objectives for Information and Related Technologies. 10 de Abril.

[CRP 2011] CONGRESO DE LA REPÚBLICA DEL PERÚ
2011 Ley 29733. Ley de protección de datos personales. 03 de Julio.

[ISACA 2008] Information Systems Audit and Control Association
2008 Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa.