REVISTA CARIBEÑA DE CIENCIAS SOCIALES

Julio 2019 - ISSN: 2254-7630

SEGURIDAD DE LA INFORMACIÓN PARA INSTITUCIONES EDUCATIVAS A TERCER NIVEL BASADO EN LA ISO/ IE27001

Carlos Bladimir Moreano Guerra

Facultad de Posgrados, Universidad Tecnologica Empresarial de Guayaquil, Dirección UTEG, Guayaqui, Ecuador
moreanocarlos@hotmail.com
moreanocarlos1@gmail.com

Para citar este artículo puede utilizar el siguiente formato:

Carlos Bladimir Moreano Guerra (2019): "Seguridad de la información para instituciones educativas a tercer nivel basado en la ISO/ IE27001", Revista Caribeña de Ciencias Sociales (julio 2019). En línea

https://www.eumed.net/rev/caribe/2019/07/seguridad-informacion.html

Resumen

Como es de conocimiento publico en el país la ley de comercio electronico y firmas electrónicas permiten establecer algunos parametros para implementar sistemas de gestion de seguridad de la información SGSI en distintos tipos de entidades. Es necesario aclarar que en la Constitucion de la República del Ecuadro se indica que la educacion es un derecho de las personas a lo largo de su vida y que es responsabilidad del estado garantizar la alfabetización digital y el uso de las tecnologias de informacion y comunicacion en el proceso educativo. El proyecto que se presenta consite en verificar como se esta llevando la seguridad de la informacion en las instituciones educativas a tercer nivel identificando los procesos con Cobit determinando los riesgos, consecuencias, impacto para posteriormente verificar si cumple la denominada norma ISO/IEC 27001.

Palabras claves

SGSI, Cobit, riesgos, procesos, instituciones educativas

Absatract

As it is public knowledge in the country the law of electronic commerce and electronic signatures allow to establish some parameters to implement

management systems of information security in different types of entities. It is necessary to clarify that in the Constitution of the Republic of the Equator it was stated that education is a right of people throughout their life and that it is the responsibility of the State to guarantee digital literacy and the use of information and communication technologies in the educational process. The project presented consists of verifying how information security is being carried out in educational institutions at a third level, identifying the processes with Cobit, determining the risks, consequences, and impact to subsequently verify if it meets the so-called ISO / IEC 27001 standard.

1 Introduccion

Todo se remonta desde hace muchos años atrás donde la seguridad nació con el objetivo de evitar problemas que se pueden generar en las organizaciones en sus diferentes áreas, es por esto que al hablar sobre seguridad se hace referencia a que el riesgo se reduzca a niveles aceptables es decir sea manejable en la organización. La innovación de la tecnología hoy en día es una necesidad en todos los ambientes organizacionales ya que desde hace años atrás se ve la carencia que se tiene en realizar inversiones para proteger la seguridad informática varias organizaciones no prestaban la atención a esto pero con el pasar de los años a los sistemas de información y los datos contenidos en ella se los puede denominar como activos de mucha valides por lo que se hace de suma necesidad brindarles la protección adecuada mediante un análisis y evaluación de los riegos con lo que se verifica la existencia de controles en la seguridad existente y también un monitoreo de los sistemas de información con lo que se puede determinar el estado actual de la organización teniendo en cuenta las posibles vulnerabilidades a la cual está expuesta, para determinar eso de manera acertada se debe iniciar procesos de diagnóstico los cuales van a lograr establecer como se encuentra el estado actual de la seguridad en la organización. Se debe tomar en cuenta que se está viviendo en la era donde la información es el recurso más importante en las organizaciones así como también la implementación de tecnología la misma que contiene la estructura para almacenar la misma es decir que hoy en día el éxito depende de la gestión de la tecnología informática, es por esto que se aconseja que existan procesos entre las áreas administrativas así como también con el área de tecnología para manejar los recursos de manera eficiente, es por esto que en el desarrollo de este documento se habla sobre los proceso que se debe aplicar en las organizaciones cuando se trata de seguridad de la información aplicando los marcos de referencia COBIT con los controles que establece la norma **ISO/ IE27001** la que nos manifiestan que se puede aplicar en cualquier tipo de organización donde se demande la gestión de múltiples políticas, procedimientos, personas, bienes donde se recoge información de los elementos dentro de un sistema de gestión de seguridad de la

información con lo que la organización mejorara el cumplimiento de requerimientos legales, obtener una ventaja comercial, mejores costos y una mejor organización. En este proyecto se realizara un diagnóstico de la seguridad de la información en las instituciones educativas a tercer nivel basados en la ISO / IE 27001 puesto que cuentan con sistemas de información e infraestructuras tecnológicas que se encuentran expuestos a varios problemas que se pueden generar y no cuentan con precauciones necesarias lo que deriva las falta de control, la inseguridad, el mal uso de los recursos y la mala administración de los mismos lo que afecta el buen funcionamiento de los recursos informáticos.

2 Fundamento Teórico

2.1 Educación Superior

Como es de conocimiento en Ecuador las instituciones a tercer nivel se encuentran reguladas por las LOES (Ley Orgánica de Educación Superior) la misma que establece que la educación es un derecho de las personas a lo largo de su vida y un deber del Estado, es así como también se determina que el Sistema de Educación a tercer nivel tiene como finalidad la formación académica y profesional de las personas y donde es de mucha importancia el conocer que es derecho de las instituciones el uso y aplicación de las tecnologías de información en cualquier campo que este sea como administrativo o educativo[1] para su mejor entendimiento punto fundamental que se debe tener en cuenta en el transcurso de este documento puesto que de aquí nace el lugar de donde se origina toda la información que se desea analizar.

2.2 Tecnología de la Información (TI)

La Tecnología Informática (TI) ha penetrado todos los sectores del mundo actual, desde el punto de vista personal hasta los negocios. Hoy en día las empresas almacenan información de sus clientes, usuarios y proveedores en bases de datos, se comunican con ellos a través del correo electrónico, videoconferencias en vivo. La TI ha cumplido un rol determinante en el éxito de las organizaciones, ya que ha pasado de ser un área ignorada por los accionistas a ser un componente clave en los procesos de negocio, así como en la creación de nuevas oportunidades como un factor diferencial para obtener una ventaja competitiva. Teniendo esto en mente, la TI no solamente soporta las estrategias de negocio existentes de una compañía, sino que genera nuevas estrategias, agregando valor a los productos y servicios que la organización ofrece[2]. Las TIC han cambiado el soporte primordial del

conocimiento, que producirá cambios en los modos de conocer y pensar de los seres humanos. El nuevo modo de acceso al conocimiento se produce a través de los hiperdocumentos, que presentan tres características fundamentales como son información multimedia, un alto grado de interactividad y una estructura no lineal. [3]

2.3 Seguridad de Información

La seguridad de la información es más que un problema de seguridad de datos en los computadores debe estar básicamente orientada a proteger la propiedad intelectual y la información importante de las organizaciones así como también de las personas, los riesgos de la información se presentan cuando se manejan dos elementos amenazas y vulnerabilidades las mismas que se encuentran ligadas, y no puede haber ninguna consecuencia sin la presencia conjunta de éstas. [4] Las amenazas deben tomar ventaja de las vulnerabilidades y pueden venir de cualquier parte, interna o externa, relacionada con el entorno de las organizaciones. La seguridad de la información es un conjunto de técnicas y medidas para controlar todos los datos que se manejan dentro de una organización la misma que se encarga que la información no salga de la empresa, este tipo de sistemas se basan en las nuevas tecnologías, por tanto la seguridad de la información resguardará los datos que están disponibles en dicho sistema y a los que solo tendrán acceso usuarios autorizados los mismos que podrán hacer modificaciones en la información[5]. Es por todo lo presentado que se puede definir que la Seguridad de la Información es el conjunto de medidas preventivas y correctivas de las organizaciones que permiten resguardar y proteger la información buscando mantener la confidencialidad, disponibilidad e integridad de la misma. [6]
La confidencialidad impide la divulgación a personas no autorizadas, la disponibilidad es la condición de la información de encontrarse de manera rápida, la integridad es mantener la información tal y cual fue generada. Al hablar de seguridad de la información se debe tener muy en cuenta el siguiente gráfico y se debe manejar de forma clara cada una de las palabras indicadas

Fig 1. Aspectos importantes de los Sistemas de Información

Amenaza.- es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño sobre los elementos de Información.
Riesgo.- es la probabilidad de que ocurra un hecho el cual puede producir un efecto
Vulnerabilidad.- esta se relaciona completamente con el riesgo y la amenaza ya que se lo puede determinar como una debilidad del sistema

2.4 COBIT 5

Sus siglas significan Objetivos de Control para Tecnología de Información y Tecnologías relacionadas es un modelo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad TI y que abarca controles específicos de TI desde una perspectiva de negocios. La estructura del modelo COBIT propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización.[7]

Fig 2. Estructura de COBIT

Cobit tiene diferentes versiones las mismas que pretenden a travez del tiempo mejorar sus productos para beneficio de la organizacion y de esta manera asegurar las tareas y actividades qu hacen parte de la estructura de las tecnologias de informacion.[8]

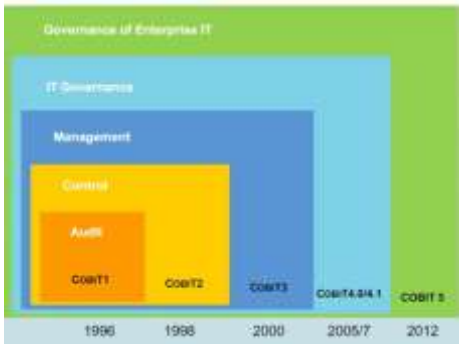

Fig 3. Versiones de COBIT

De las versiones presentadas en la figura anterior se puede indicar que la versión COBIT 5permite que las tecnologías de la información y relacionadas se gobiernen y administren de una manera holística a nivel de toda la Organización, incluyendo el alcance completo de todas las áreas de responsabilidad funcionales y de negocios, considerando los intereses relacionados con la TI de las partes interesadas internas y externas.[9] Con lo indicado se debe mencionar que los principios de COBIT son satisfacer las necesidades de las partes interesadas, cubrir la organización de forma integral, aplicar un solo marco integrado, habilitar un enfoque holístico, separar el gobierno de la administración.

2.5 ISO/ IE27001

Las normas ISO son una red de organismos nacionales de estandarización de más de 160 países donde los resultados finales de los trabajos realizados por ISO son publicados como normas internacionales.[10] Un SGSI (Sistema de Gestión de Seguridad de la Información) proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la protección de los activos de información para lograr objetivos de negocio. En este caso se hace referencia a la norma ISO 27001 que es de la que se tratara este trabajo la misma que indica que al ser certificada una organización puede solicitar una auditoría siempre y cuando cuente con un SGSI.[11]

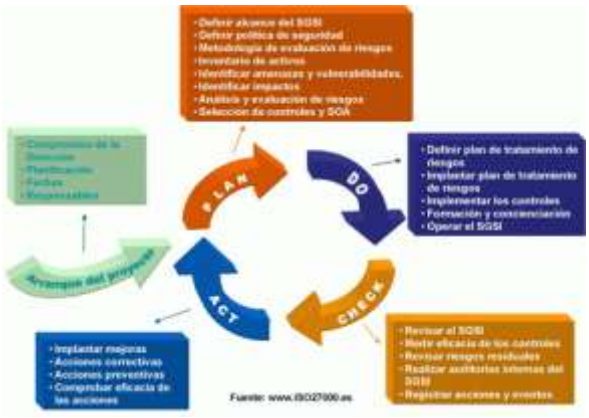

Fig 4. Puntos y etapas de la norma ISO 27001

Esta estructura de norma ISO 27001 se adapta a una estructura de alto nivel que siguen las normas de sistema de gestión lo que indica que es fácilmente integrable es por esto que incluye los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información, es decir es un sistema activo, integrado en la organización, orientado a los objetivos empresariales y con una proyección de futuro es por esto que al incorpora un nueva herramienta en la organización se debe actualizar el análisis de riesgos para poder mitigar de forma responsable los riesgos y por supuesto considerando la regla básica de riesgo es decir, minimizar los riesgos con medidas de control ajustadas y considerando los costos del control. Esta norma propone un marco de gestión de la seguridad de toda la información de la empresa, incluso si es información perteneciente al propio conocimiento y experiencia de las personas o sea tratada en reuniones. Es de suma importancia[12][13].

Como es de conocimiento la norma ISO 27001 para establecer un control más adecuado dentro de la organización se puede relacionar con otras normas como Cobit e Itil las cuales presentan procesos comunes y se basan en el ciclo de vida de las aplicaciones, servicios y sistemas de TI, es por esto que al aplicar Cobit e ISO 27001 se enfocan específicamente en la seguridad de la información.

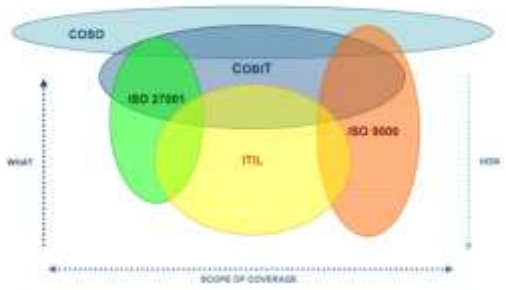

Fig 5. ISO 27001 y relación con otras normas

3 Metodologia

La metodología utilizada es la ISO 27001:2013 que no solo establece cambios en el contenido sino también en la estructura lo que verá reflejado en otros documentos que forman parte de la familia ISO 27000. La norma ISO 27001:2013 ha sido desarrollada con base al Anexo SL, en la que se proporciona un formato y un conjunto de alineamiento que siguen el desarrollo documental de un Sistema de Gestión sin que le importe el enfoque empresarial, se alinean bajo la misma estructura todos los documentos que se relacionan con el Sistema de Gestión de Seguridad de la Información y así se evitan problemas de integración con otros marcos de referencia. En la norma ISO 27001:2013 el cambio más significativo es la eliminación de la sección “Enfoque del proceso” que sí contenía la versión 2005, donde se describía el modelo PHVA, considerándose el corazón del Sistema de Gestión de Seguridad de la Información**.** La norma ISO 27001:2013 se convierte en una referencia normativa obligatoria y única, ya que contiene todos los nuevos términos y definiciones. Los términos y las definiciones que se encontraban en la ISO 27001:2005 los trasladaron y fueron agrupados en la sección 3 de la norma ISO 27001:2013 “Fundamento y vocabulario”, con el fin de contar con una sola guía de términos y definiciones que sea consistente. Dentro del contexto de la organización esta norma identifica los problemas externo e internos que rodena a la empresa donde se intuyen todos los requisitos para definir el contexto del SGSI sin importar el tipo de empresa que sea y el alcance que tenga. El liderazgo se realiza un ajuste de la relación y las responsabilidades de la gerencia de la organización con respecto al SGSI, destacando como se deberá demostrar el compromiso. La Planeación aquí la **norma** ISO 27001:2013 se enfoca a la definición de los objetivos de seguridad como un todo, los cuales deben estar claros y se deben contar con planes específicos para conseguirlos, teniendo en cuenta que se puede presentar grandes cambios en el proceso de evaluación de riesgos. Dentro del soporte se cuenta con recursos, personal competente, conciencia y comunicación

Al establecer la metodología que se utiliza se puede determinar una tabla donde se establecen los tipos, activos, nombre de activo, clasificación de la información, impacto, probabilidad y riesgo.

TIPO	ACTIVO	NOMBRE ACTIVO	CLASIFICACION DE LA INFORMACION	IMPACTO	PROBABILIDAD	RIESGO
DATOS INFORMACION	COPIAS RESPALDOS	ARCHIVOS DE NOTAS	CONFIDENCIAL	MUY ALTA	PRACTICAMENTE SEGURO	CRITICO
		ARCHIVOS DE CONTABILIDAD	USO INTERNO	MUY ALTA	PRACTICAMENTE SEGURO	CRITICO
		ARCHIVOS DE ACTAS Y RESOLUCIONES	PUBLICO	MUY ALTA	PRACTICAMENTE SEGURO	CRITICO
		COPIAS DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO	SECRETA	MUY ALTA	PRACTICAMENTE SEGURO	CRITICO
	DATOS DE CONFIGURACIO	DATOS DE CONFIGURACION DE COMPUTADORAS Y SERVIDORES	CONFIDENCIAL	MUY ALTA	PRACTICAMENTE SEGURO	CRITICO
	CONTRASEÑAS	CONTRASEÑAS DE COMPUTADORES	RESERVADO USO INTERNO	MUY ALTA	PRACTICAMENTE SEGURO	CRITICO
SERVICIOS	PAGINA WEB	SERVICIO QUE OFRECEN LOS INSTITUTOS A LA COMUNIDAD EDUCATIVA	PUBLICA	MUY ALTA	PRACTICAMENTE SEGURO	CRITICO
	INTERCAMBIO DE DATOS	INTERCAMBIO DE DATOS QUE OFRECEN LOS INSTITUTOS	PUBLICA	MUY ALTA	PRACTICAMENTE SEGURO	CRITICO
SOFTWARE APLICACIONES INFORMATICAS	SISTEMAS OPERATIVOS	VERSIONES DE WINDOWS	PUBLICA	BAJO	POCO PROBABLE	BAJO
	SERVIDOR DE CORREO	SERVIDOR DE CORREO ELECTRONICO	CONFIDENCIAL	MEDIO	POSIBLE	APRECIABLE

	SIGBD	GBD ALMACENA DATOS DE ESTUDIANTES	CONFIDENCIAL	MEDIO	POSIBLE	APRECIABLE
	GESTOR DE MAQUINAS VIRTUALES	VIRTUAL BOX	PUBLICA	BAJO	POCO PROBABLE	BAJO
	SERVIDOR DE APLICACIONES	XAMPP APACHE	PUBLICA	BAJO	POCO PROBABLE	BAJO
EQUIPAMIENTO INFORMATICO	PC PORTATILES	EQUIPOS DE COMPUTO	PUBLICA	MEDIO	POSIBLE	APRECIABLE
REDES	WIFI	RED INALAMBRICA	RESERVADO USO INTERNO	BAJO	POCO PROBABLE	BAJO
	INTERNET	INTERNET	RESERVADO USO INTERNO	BAJO	POCO PROBABLE	BAJO

Tabla #1

A continuación se definen los controles para contrarrestar el impacto cuando se materialice una amenaza en los activos encontrados en la institución educativa de educación media indicando si cumplen o no los mismos.

CONTROL ISO	CONTROLES	CUMPLE		CONTROL DESCRIPCION
		SI	NO	
5.1	5.1.1 Políticas para la seguridad de la información		X	Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes

	5.1.2 Revisión de la política de seguridad de la información		X	Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.
6.1	6.1.1 Roles y responsabili-dades para la seguridad de información		X	Se deberían definir y asignar todas las responsabilidades de la seguridad de la información
7.1	7.1.1 Investigación de antecedentes	X		Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos
	7.2.1 Responsabilidades de la dirección		X	La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
8.2	8.2.1. Clasificación de la información	X		La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
	8.2.3 Manejo de activos		X	Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización
9.1	9.1.1 Política de control de acceso		X	Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información
	.9.1.2 Política sobre el uso de los servicios de red		X	Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente

	9.2.3 Gestión de derechos de acceso privilegiado		X	Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado
9.4	9.4.1 Restricción de acceso Información	X		El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.
	9.4.2 Procedimiento de ingreso seguro		X	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
	9.4.3 Sistema de gestión de contraseñas		X	Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
	9.4.4 Uso de programas utilitarios privilegiados		X	Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones
11	11.1.3. Seguridad de oficinas, recintos e instalaciones	X		Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
	11.1.4. Protección contra amenazas externas y ambientales	X		Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
	11.2.2 Servicios de suministro	X		Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro
	11..2.4 Mantenimiento de equipos	X		Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.
12	12.2.1 Controles contra códigos maliciosos		X	Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos
	12.3.1 Respaldo de información	X		Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias

				de respaldo aceptada.
	12.4.1 Registro de eventos		X	Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
	12.4.2 Protección de la información de registro	X		Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado
	12.5.1 Instalación de software en sistemas operativos		X	Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos
	12.6.2 Restricciones sobre la instalación de software		X	Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios
13	13.1.1 Controles de redes	X		Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.
	13.2.3 Mensajería electrónica	X		Se debería proteger adecuadamente la información incluida en la mensajería electrónica
16	16.1.3 Reporte de debilidades de seguridad de la información	X		Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios
17	17.1.2 Implementación de la continuidad de la seguridad de la información	X		La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa
18	18.2.2 Cumplimiento con las políticas y normas de seguridad		X	Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y

				cualquier otro requisito de seguridad.

Tabla #2

Como se cuenta con los controles ISO 27001-2013 se integra con los procesos Cobits 5 indicados a continuación

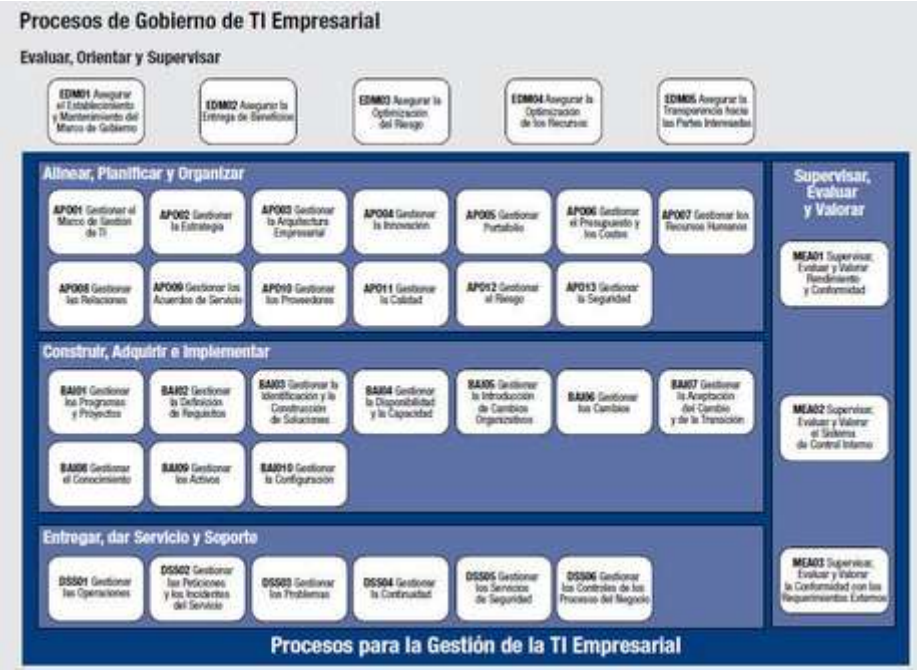

Fig 6. Procesos Cobit 5

4 Discusion

A partir de este punto y mediante una matriz que se presenta en la tabla#1 se ha logrado identificar el impacto la probabilidad y el riesgo de los activos de las instituciones educativas a tercer nivel, con esto se puede detectar las partes donde existen algunas anomalias en las cuales al aplicar la metodología ISO 27001:2013 con los respectivos controles que se muestra el la tabla#2 se puede deteminar objetivos, aplicabilidad, directrices, confidencialidad, integridad, disponibilidad tomando en cuenta que esto nos brinda una gran oportunidad de mejora en las instituciones educativas de tercer nivel. Mediante la metodologia utilizada se puede identificar el Què del

problema que se genera mientras que con Cobit 5 y sus controles se complementan y se da el como resolver por definitivo los problemas generados.

5 Conclusiones

En el diagnóstico realizado a los activos de información aplicando la metodología ISO 27001:2013 se pudo verificar con que activos cuenta la institución educativa, los activos fueron clasificados de acuerdo a los criterios de la información. En la institución educativa no cuenta con unas políticas de seguridad adecuadas para la salvaguardar la información. Las políticas de seguridad propuestas se tratan de mejorar la seguridad de la información, en función de la productividad en procesos, se puede concluir indicando que al interactuar la metodología utilizada y Cobit 5 se puede establecer los controles y procesos indicados y de esta manera lograr implementar en las instituciones educativas de tercer nivel una buena política de seguridad en el manejo de la información.

Referencias

[1] R. O. S. De, H. Enrique, and D. Pozo, “LEY ORGANICA DE EDUCACION SUPERIOR , LOES,” pp. 1–92, 2018.

[2] C. Belloch, “Las Tecnologías de la Información y la Comunicación,” vol. 16, no. 29, p. 1, 2012.

[3] L. A. S. Tecnologías, D. E. L. A. Información, Y. C. T. I. C. En, C. T. I. C. En, and E. L. Aprendizaje, “Las tecnologías de la información y comunicación (t.i.c.) en el aprendizaje,” no. October, 2014.

[4] A. Generales, “AMENAZAS INFORMÁTICAS Y,” pp. 137–146.

[5] J. A. Monsalve Pulido, F. A. Aponte Novoa, and D. F. Chaves-Tamayo, “Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia),” *Fac. Ing.*, vol. 23, no. 37, pp. 65–72, 2014.

[6] L. A. Disponibilidad and Y. L. A. Integridad, “DE LOS DATOS Y SISTEMAS INFORMÁTICOS INTEGRITY AND AVAILABILITY OF DATA AND information SYSTEMS . The Spanish Normativity,” pp. 27–53.

[7] E. Cobit, E. Cobit, C. Objectives, I. Systems, and I. S. Audit, “COBIT : MODELO PARA AUDITORIA Y,” 2007.

[8] D. Nathaly and L. Armendáriz, “información basado en COBIT , ITIL e ISO / IEC 27000,” vol. 30, no. Mayo, pp. 51–69, 2017.

[9] T. Velásquez, A. M. Puentes, and Y. M. Pérez, “Model for implementation of IT corporate governance,” *Tecnura*, no. c, pp. 159–169, 2015.

[10] A. S. Del Castillo and N. Sardi, “ISO standards and the quality concept applied to anesthesia services,” *Colomb. J. Anesthesiol.*, vol. 40, no. 1,

pp. 14–16, 2012.
[11] A. Ladino *et al.*, “FUNDAMENTOS DE ISO 27001 Y SU APLICACIÓN EN LAS EMPRESAS Fundamentals of ISO 27001 and its application in enterprises,” 2011.
[12] M. La *et al.*, “No Title,” 2015.
[13] Asociación Española para la Calidad, “La norma ISO 27001 del Sistema de Gestión de la Garantía de confidencialidad, integridad,” *Aenor*, p. 5, 2012.