ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA TECNOLÓGICA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

PROGRAMA DE MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER

TEMA: PLAN DE SEGURIDAD INFORMÁTICA DE LA ESPE SEDE SANTO DOMINGO

AUTORAS: BORJA LÓPEZ, YOLANDA AZUCENA
SÁNCHEZ CALI, FANNY GUADALUPE

DIRECTOR: ING. QUINTANA, MARCO MSc.

SANGOLQUÍ, MAYO 2015

CERTIFICADO

Certifico que el presente trabajo titulado “Plan de Seguridad Informática de la ESPE Sede Santo Domingo” fue desarrollado en su totalidad por Yolanda Azucena Borja López y Fanny Guadalupe Sánchez Cali, bajo mi supervisión.

Atentamente.-

.....

Ing. Marco Vinicio Quintana MSc.
DOCENTE DIRECTOR

AUTORÍA DE RESPONSABILIDAD

El presente trabajo titulado "Plan de Seguridad Informática de la ESPE Sede Santo Domingo", ha sido elaborado considerando el derecho intelectual de otros autores especificando en citas de pie de página, fuentes bibliográficas e investigaciones sobre el tema.

Nosotras, Fanny Guadalupe Sánchez Cali y Yolanda Azucena Borja López, declaramos que el trabajo aquí detallado es de nuestra autoría.

AUTORIZACIÓN

Nosotras, Fanny Guadalupe Sánchez Cali y Yolanda Azucena Borja López, autorizamos la publicación del presente trabajo titulado "Plan de Seguridad Informática de la ESPE Sede Santo Domingo" en la Biblioteca Virtual Institucional.

DEDICATORIA

A mi familia en especial a mi Madre Laura y amigos quienes de alguna manera nos apoyaron incondicionalmente para la culminación de este trabajo.

Fanny Sánchez

A mis padres Vicente y Yolanda, a mis hijos Sebastián, Johann, Joseph y Julliette por su apoyo incondicional, por su comprensión y acompañamiento en todo momento.

Yolanda Borja

AGRADECIMIENTO

A Dios por la vida, salud y la oportunidad de servir a la humanidad a través del conocimiento adquirido y luego pueda ser impartido a quien lo requiera en bien de la sociedad.

Fanny Sánchez

Agradezco a Dios por darme vida y salud, a mis padres Vicente y Yolanda quienes han sido mi apoyo incondicional en todas mis metas propuestas, a mis hijos Sebastián, Johann y Joseph por su apoyo, paciencia y a mi hermosa hija Juliette quien ha sido mi compañera de estudios. Un agradecimiento especial a mi amiga del alma Fanny por toda su comprensión y apoyo para finalizar con este trabajo.

Yolanda Borja

CONTENIDO

INDICE DE TABLAS

ÍNDICE DE FIGURAS

ANEXOS

RESUMEN

Los sistemas de gestión de la información están relacionados con los procesos organizacionales e instituciones públicos o privados, en virtud de esto y sabiendo en lo importante que se ha convertido hoy en día la seguridad de la información se aplica lo determinado por el Acuerdo No 166 de la Secretaria Nacional de la Administración Pública del Ecuador, donde se establece la elaboración de un Sistema de Gestión de Seguridad de la Información conocido PLAN DE SEGURIDAD DE LA INFORMACIÓN, estableciendo los lineamientos y políticas para proteger la información. Para el desarrollo del proyecto se aplica un marco integrado de estándares internacionales, como COBIT 5 Security Information, serie de las normas ISO 27000 para seguridad de la información y para gestión de riesgos ISO 31000. Sabiendo que la metodología COBIT 5 abarca la institución de extremo a extremo, integrando marcos de estándares y una vez determinadas las herramientas que se utilizaran en el proyecto, se levanta información de la Unidad de Tecnologías de la Información y Comunicación de la ESPE matriz y sus aplicaciones para la Sede Santo Domingo, para el análisis de riesgos utilizando normas ISO 31000 y 27005, posterior con la identificación de procesos y eventos con mayor probabilidad de ocurrencia y que afecte a la seguridad de la información y además relacionando los procesos COBIT se diseña el Plan de seguridad de la información estableciendo controles para los riesgos encontrados.

PALABRAS CLAVES:

- **SEGURIDAD DE LA INFORMACIÓN**
- **ISO/IEC 27000**
- **COBIT 5 SECURITY INFORMATION**
- **ISO 31000**
- **GESTIÓN DE SEGURIDAD**

ABSTRACT

The management of information system it´s related processes organizational public or private institutions, honoring this and knowing how important it has become security information nowadays it´s determined in the Agreement No. 166. The National Secretary of Public Administration of Ecuador, where is established a system known Information Security ISMS, following guidelines and politics in order to protect important information. For developing this project it´s applied an integrated international framework standard, such as COBIT 5 Security Information, ISO 27000 for security information and for danger management it´s applied ISO 31000. Knowing that the COBIT 5 methodology involves the context institution, integrated frameworks to established standards and tools to be used in the project, the Information from the Technology and Communication Unit ESPE and its applications are Transferred to the Headquarters Santo Domingo, to analyze high danger using ISO 31000 and 27005, before the identification processes and events most likely to occur and affecting the security information standards and also linking COBIT information processes security Plan control to establish any dangers found.

Keywords:

- **SECURITY INFORMATION**
- **ISO/IEC 27000**
- **COBIT 5 SECURITY INFORMATION**
- **ISO 31000**
- **SECURITY MANAGEMENT**

CAPÍTULO I

INTRODUCCIÓN

1.1. Antecedentes

La información es un recurso que tiene un valor muy importante dentro de toda institución, por ende debe ser debidamente protegida, con el fin de garantizar la continuidad en los sistemas de información y comunicación y minimizar los riesgos para mejorar la gestión dentro de una institución.

La Universidad de las Fuerzas Armadas ESPE como institución de educación superior también requiere proteger su información física y digital, tanto de la matriz como de cada una de las sedes que la conforman, el propósito del presente trabajo es establecer un plan de políticas de seguridad de información basadas en marcos y estándares referenciales internacionales y nacionales, de la misma manera se basará en acuerdos gubernamentales sobre el resguardo de la información siendo hoy en día uno de los temas más relevantes dentro de las tecnologías de la información.

El objetivo de creación de políticas de seguridad de información direccionada a la Universidad de las Fuerzas Armadas ESPE es especificar normativas institucionales de la seguridad de la información, describiendo acciones necesarias para el análisis de riesgos de acuerdo a la normativa vigente, además se determinara los ámbitos donde se requiere la implementación de las políticas de seguridad.

Para que los principios de la política de seguridad de la información sean efectivos es necesario crear una cultura organizacional de seguridad y compromiso por parte de funcionarios y todas aquellas personas involucradas en la gestión de la información para contribuir a la difusión, consolidación y cumplimiento de la misma.

La propuesta se sustenta en el Acuerdo N° 166 que trata sobre un Esquema Gubernamental de Seguridad de la Información (EGSI) de la Secretaria Nacional de Administración Pública, suscrito por el Secretario de Administración Público Cristian Castillo Peña herrera, de fecha 19 de septiembre del 2013, el acuerdo a su

vez se regirá a lo que establece el Estándar Internacional ISO/IEC 27001 además se fundamentará en lo que indica COBIT Security Information y 31000.

1.2. Entorno organizacional de la Universidad de las Fuerzas Armadas ESPE

1.2.1. Organización Institucional

La Universidad de las Fuerzas Armadas - ESPE, como parte del Sistema de Educación Superior, es una institución con personería jurídica, autonomía administrativa y patrimonio propio, de derecho público, con domicilio en la ciudad de Quito y sede matriz en la ciudad de Sangolquí; se rige por la Constitución de la República del Ecuador, la Ley Orgánica de Educación Superior y su reglamento; otras leyes conexas; su Estatuto aprobado por el Consejo de Educación Superior – CES, mediante resolución RPC-S0-24-No.248-2013 emitida el 26 de Julio del 2013; los reglamentos internos expedidos de acuerdo con la ley y por normas emitidas por sus órganos de administración y autoridades.

1.2.2. Misión

Formar académicos y profesionales de excelencia; generar, aplicar y difundir el conocimiento y, proponer e implementar alternativas de solución a problemas de interés público en sus zonas de influencia.

1.2.3. Visión

Ser líder en la gestión del conocimiento y de la tecnología en el Sistema de Educación Superior, con prestigio Internacional y referente de práctica de valores éticos, cívicos y de servicio a la sociedad.

1.2.4. Estructura Organizacional

Según el Art. 17 Organigrama Estructural del Reglamento Orgánico de Gestión Organizacional por Procesos, representa la estructura organizacional de la Universidad de las Fuerzas Armadas ESPE, en el **Anexo 1** se indica los procesos organizacionales con sus respectivas Unidades Administrativas.

- **Organigrama estructural ESPE sede Santo Domingo**

En el **Anexo 2** se indica la estructura organizacional de la Sede Santo Domingo, tanto en área Administrativa, Hacienda Zoila Luz Km. 24 Vía Santo Domingo – Quevedo y el área Académica, Km. 35 Vía Santo Domingo – Quevedo.

1.2.5. Plan estratégico (2014-2017)

El Plan Estratégico traza el rumbo para el desarrollo de la Universidad; posibilita el alineamiento de esfuerzos para alcanzar los objetivos y metas en él planteados y orienta las acciones hacia el logro de una visión de futuro compartido. El éxito de su ejecución requiere del compromiso y disciplina de toca la comunidad universitaria ESPE.

Los principales objetivos contemplados en el plan estratégico son los siguientes según (Armadas, 2015):

- Incrementar el reconocimiento de la Universidad de las Fuerzas Armadas - ESPE como una institución referente a educación superior.
- Incrementar la calidad de los profesionales y postgraduados.
- Incrementar la producción científica, tecnológica y su calidad.
- Incrementar el impacto social de los programas de vinculación.
- Incrementar la eficiencia y eficacia del sistema formativo de grado y pregrado.
- Incrementar la capacidad del sistema de investigación integrándolo con el modelo formativo.
- Incrementar la capacidad y calidad del sistema de vinculación integrándolo con el sistema de investigación y con el modelo formativo.
- Incrementar las capacidades de sustentación institucional. Talento humano-Finanzas-Recursos Físicos y Tecnológicos.

El Plan Estratégico Institucional de la ESPE (2014-2017) presentado en el **Anexo 3,** sirve de base para la sede Santo Domingo en caso de requerir estrategias de aplicabilidad en la parte administrativa y en la parte académica**.**

1.2.6. Unidad de Tecnologías de la Información y las Comunicaciones

La UTIC se encarga de garantizar el óptimo funcionamiento de todos los servicios relacionados con la informática, tanto de hardware como de software, así como el mantenimiento de las redes de comunicación. Además la UTIC realiza fundamentalmente tareas de mantenimiento, tanto correctivo como preventivo, de los equipos y servicios informáticos de la Universidad, sin olvidar otras tareas tan importantes como son la seguridad y las comunicaciones.

- Actualmente la ESPE sede Santo Domingo **no cuenta** con una Dirección de Tecnologías de la Información por lo que depende totalmente de la administración de la UTIC en las áreas: técnica y administrativa.

1.2.6.1. Misión de la UTIC MATRIZ

Administra y provee de forma eficiente y segura los recursos y servicios de tecnologías de información y comunicaciones, de acuerdo a las necesidades institucionales y tendencias globales, cumpliendo normas y estándares internacionales.

1.2.6.2. Visión UTIC MATRIZ

Ser reconocida como unidad estratégica de la Institución, contribuyendo al desarrollo, innovación y transferencia de Tecnologías de Información y Comunicaciones, cumpliendo normas y estándares internacionales, con responsabilidad social y del medio ambiente.

1.2.6.3. Departamento de Soporte Técnico

Brinda el soporte y mantiene en óptimas condiciones los equipos informáticos y recursos informáticos básicos, que garanticen una mejor ejecución de las funciones administrativas y operacionales de las distintas unidades de la Universidad.

1.2.6.4. Departamento de Desarrollo de Sistemas de Información

Este departamento desarrolla, implementa y mantiene los sistemas de información de la Institución, como el que se indica en la **Figura1**.

Figura 1 Servicios virtuales ESPE

Fuente (ESPE, 2015)

1.2.6.5. Departamento de Redes y Telecomunicaciones

Implementar y administrar la infraestructura de las redes de comunicación de la Universidad y los servicios relacionados con la misma.

1.2.7. Sede Santo Domingo

La Sede Santo Domingo cuenta con la Carrera de Ingeniería en Ciencias Agropecuarias Santo Domingo, aprobada el 16 de agosto del 2000 en la ciudad de Quito, por el Consejo Nacional de Universidades y Escuelas Politécnicas (CONUEP).

Servicios de la ESPE Sede Santo Domingo

La Carrera ofrece los siguientes servicios:

- Aulas de clases equipadas con equipos de última tecnología
- Internado con servicio de alojamiento y alimentación
- Biblioteca
- Bar – comedor.
- Laboratorios de uso general y técnicos.
- Laboratorio de computación.
- Parcelas de investigación agropecuaria.
- Ganadería de carne y leche.

- Auditórium.
- Sala de descanso.
- Canchas deportivas.
- Policlínico.
- Transporte interno.
- Seguridad.
- Sitio web: iasa2.espe.ec/inicio/

El presente proyecto se realizará en la Universidad de las Fuerzas Armadas ESPE, sede Sto. Domingo, Ubicada en la Provincia de Santo Domingo de los Tsáchilas, Cantón Sto. Domingo, Ha. Zoila Luz, Vía Santo Domingo - Quevedo Km. 24, teléfono: (593) 02-2722246 – 48, fax: (593) 02-2722247, correo:santodomingo@espe.edu.ec, horarios de atención**:** 07H00 - 15H30, detalle de mapa de ubicación en **Figura2**.

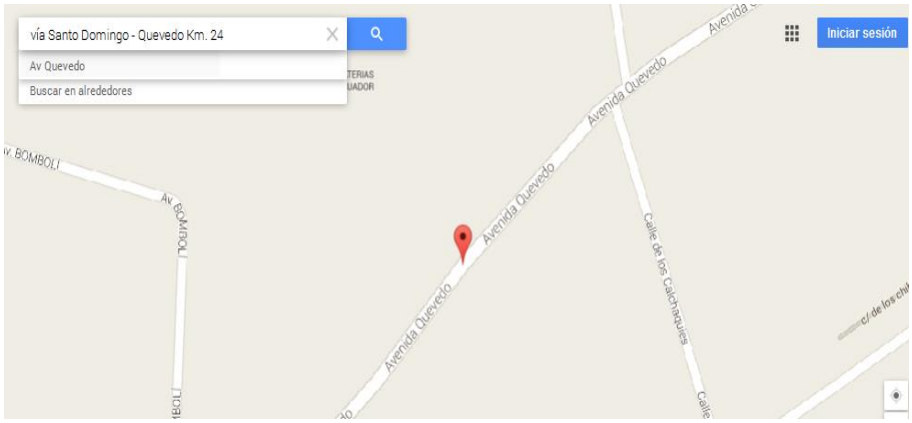

Figura 2 Ubicación geográfica de la Universidad de las Fuerzas Armadas sede Santo Domingo
Fuente: (Google maps, 2014)

1.3. Justificación e Importancia

El Internet ha brindado ventajas de comunicación e interconexión de información en el mundo, a través de sistemas en línea, redes sociales y comerciales diversas Empresas utilizan esta red para facilitar sus transacciones como las Instituciones Bancarias y Comercio Electrónico, pero a la vez ha generado desventajas y nuevos

desafíos que amenazan la seguridad de la información por medio de los delitos informáticos.

La Seguridad Informática entonces se ha convertido en un tema de gran importancia en el Ecuador y el Mundo, la gestión incorrecta de datos puede generar notables pérdidas económicas, afectar el prestigio de los negocios, ocasionar problemas legales entre otros problemas. Entonces no se puede aseverar que un sistema de información es al 100% seguro, ni aun contando con una infraestructura tecnológica de Software y Hardware apropiado, siempre está presente la vulnerabilidad y las amenazas que pueden aparecer en cualquier momento y provocar daños irreparables.

En la actualidad los ataques contra la información se han convertido en un negocio rentable y en la mayoría de casos interviene el crimen organizado creando sus propias empresas dedicadas al desarrollo de herramientas tecnológicas para crear ataques en la red y también para evolucionar sus crímenes informáticos.

Por esta razón los usuarios de la información a nivel mundial nos encontramos preocupados por la seguridad de los datos que subimos y bajamos de lo que en tecnología se conoce como información en la nube, pero los ataques no se realizan solo a través del Internet, muchas veces la infraestructura tecnológica de Hardware y Software de cualquier Organización en el Mundo puede ser víctima de los intrusos.

En nuestro país, la gestión actual ha creado un Esquema Gubernamental de Seguridad de la Información (EGSI) de la Secretaria Nacional de Administración Pública, en el que indica los principios y políticas basados en la Norma ISO/IEC 27001 de seguridad de la información, este material puede ser utilizado por empresas, organizaciones, universidades y demás entes públicos y privados para que puedan implementar y resguardar su información valiosa.

1.4. Planteamiento del problema

La Universidad de las Fuerzas Armadas ESPE sede Santo Domingo presenta los siguientes problemas respecto a la seguridad informática:

- No cuenta con políticas de seguridad informática definidas.
- Falta de cultura y responsabilidad en seguridad informática.
- Vulnerabilidad en la manipulación de la información.
- Fácil acceso de personas externas a la Institución a las áreas tecnológicas.
- Desactualización de las base de datos del antivirus.

1.5. Formulación del problema

¿Cómo afecta en los procesos tecnológicos la falta de un Plan de Seguridad Informática en la Universidad de las Fuerzas Armadas ESPE sede Santo Domingo?

1.6. Objetivo general

Diseñar el Plan de Seguridad Informática de la ESPE sede Santo Domingo aplicando normas seguridad y análisis de riesgos fundamentados en el COBIT Security con el fin de promover una política institucional que sirva como referencia para la toma de decisiones acerca de las tecnologías emergentes y sus amenazas.

1.7. Objetivos específicos

- Fundamentar el estado del arte de seguridad informática a través de fuentes bibliográficas actuales.
- Recopilar información sobre la situación actual del manejo de seguridad informática utilizando Matriz de Riesgos y la entrevista-encuesta como técnica investigativa.
- Realizar el diagnóstico de la información recopilada y presentarla mediante gráficos estadísticos.
- Elaborar la propuesta de seguridad informática para que sea aplicada en la ESPE sede Santo Domingo aplicando la Norma 31000 de análisis de riesgos como metodología de análisis de riesgos, COBIT Security y el acuerdo Nro. 166 de la Secretaria Nacional de la Administración Pública.

CAPÍTULO II

FUNDAMENTACIÓN TEÓRICA

2.1. Marco teórico

2.1.1. Información

Según algunos autores, la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

Está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento (de, 2008).

2.1.2. Características de la información

- **Efectividad:** La información relevante y pertinente al proceso de negocio existe y es entregada a tiempo, correcta, consistente y de una manera usable.

- **Eficiencia:** Relativo a la entrega de información a través del óptimo (más productivo y económico) uso de los recursos.

- **Confidencialidad:** Relativo a la protección de información sensitiva de acceso y divulgación no autorizada.

- **Integridad:** Relativo a la exactitud y completitud de la información así como a su validez de acuerdo con el conjunto de valores y expectativas del negocio (Armadas, 2015).

- **Disponibilidad:** Relativo a que la información debe estar disponible cuando es requerida por el proceso de negocio y por lo tanto también relativo a la salvaguarda de recursos.
- **Cumplimiento:** Relativo al cumplimiento de leyes, regulaciones y acuerdos contractuales los cuales el proceso de negocio debe cumplir.

- **Confiabilidad:** Relativo a que los sistemas proveen a: la gerencia con la información apropiada para ser usada en la operación de la empresa; reportes a los usuarios de la información financiera e información a los organismos reguladores en cumplimiento de leyes y regulaciones ISACA (2008).

2.1.3. Seguridad

(AGUILERA, 2010) Define a la seguridad como: "Conjunto de medidas técnicas, educacionales, médicas y psicológicas empleadas para prevenir accidentes, tendientes a eliminar las condiciones inseguras del ambiente y a instruir o convencer a las personas acerca de la necesidad de implementación de prácticas preventivas".

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios y no solo en medios informáticos.

2.1.4. Plan de seguridad de la información

Plan de seguridad de la información es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System. Es el concepto central sobre el que se construye ISO 27001.

El Plan de seguridad de la información ayuda a establecer estas políticas y procedimientos en relación a los objetivos de la sede Santo Domingo, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

2.1.4.1. Qué incluye un Plan de seguridad de la información

En el ámbito de la gestión de la calidad según ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles. Es posible trasladar ese modelo a un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 como se puede visualizar en la **Figura 3**.

Figura 3 Sistema de Gestión de Seguridad de Información
Fuente: (NORMAS ISO 27000, 2015)

Por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del Plan de seguridad de la información.

- **Procedimientos**

  Documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

- **Instrucciones, checklists y formularios**

  Documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

- **Registros**

  Documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del Plan de seguridad de la información; están asociados a documentos de los otros tres niveles como *output* que demuestra que se ha cumplido lo indicado en los mismos.

2.1.5. Normas ISO 27000

De acuerdo a definiciones de (CALDERON HONOFRE Diana, ESTRELLA OCHOA Martín y FLORES VILLAMARIN Manuel, 2011) las normas ISO/IEC 27000 son 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.

Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

Como menciona la Organización Internacional de Normalización ((ISO), 2014) en su apartado correspondiente, la norma ISO27001 contiene un anexo como se muestra en la **Figura 4**, donde resume la familia de las ISO 27002:2005. En España, aún no está traducida (previsiblemente, a lo largo de 2008). Desde 2006, sí está traducida en Colombia (como ISO 17799) y, desde 2007, en Perú (como ISO 17799; descarga gratuita). El original en inglés y su traducción al francés pueden adquirirse en ISO.org.

Los lineamientos metodológicos y los requerimientos de la norma ISO/IEC 27001 son propuestos bajo el enfoque metodológico del Ciclo de Deming: Planificar – Hacer – Verificar – Actuar (PHVA)(4) (Pallas, 2009).

Entre ellas existen normas que son básicamente una especificación de Requerimientos como la ISO/IEC 27001 e ISO/IEC 27006. Otras son guías de implementación o lineamientos guía que son soporte del ciclo PHVA para los sistemas de gestión de la seguridad de la información, como la ISO/IEC 27003 o ISO/IEC 27.005 (Pallas, 2009).

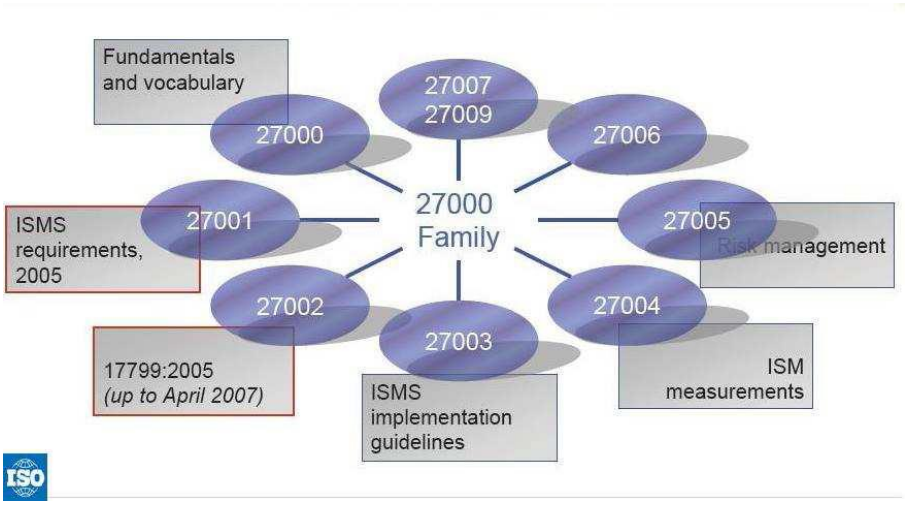

Figura 4 Contexto normativo de un Plan de seguridad de la información

Fuente: (NORMAS ISO 27000, 2015)

Según (Pallas, 2009), de las normas de la familia ISO 27000, destacan fundamentalmente la ISO/IEC 27001 e ISO/IEC 27.002 tienen como principales objetivos:

- Establecer un marco metodológico para un Plan de seguridad de la información (Pallas, 2009).
- La adopción de controles proporcionales a los riesgos percibidos (Pallas, 2009).

- La documentación de políticas, procedimientos, controles y tratamiento de riegos (Pallas, 2009).
- Identificación y asignación de responsabilidades al nivel adecuado (Pallas, 2009).
- Formalización, seguimiento y revisión de los controles y riesgos, de forma sistemática (periódica) y metodológica (Pallas, 2009).
- Generación y preservación de evidencias (Pallas, 2009).
- Tratamiento de los incidentes de seguridad (Pallas, 2009).
- Revisión y mejora continua del Plan de seguridad de la información (Pallas, 2009).
- Gestión de Riesgos (Pallas, 2009).
- Uso de métricas para evaluar efectividad y eficiencia de los controles y del propio Plan de seguridad de la información (Pallas, 2009).

A continuación, se describen brevemente los más relevantes para el desarrollo del proyecto:

- "ISO/IEC 27000: Provee información introductoria a seguridad de la información y a la gestión de la seguridad de la información, el estado y la relación de las normas de la familia de estándares para un Plan de seguridad de la información (Pallas, 2009).

- "ISO/IEC 27001:2005: Es una norma que admite certificación y especifica los requerimientos para la definición, implementación, implantación, mantenimiento y mejora de un Plan de seguridad de la información (Pallas, 2009).

- "ISO/IEC 27002:2005: Provee una guía de implementación de los controles aplicables a la seguridad de la información. Presenta once (11) cláusulas de control de la seguridad que contienen un total de treinta y nueve (39) categorías de seguridad y por lo tanto igual número de indicaciones de Objetivos de Control, con varios Controles por cada uno de ellos (Pallas, 2009).

- "ISO/IEC 27003: Provee información práctica y una guía de implementación de la norma ISO/IEC 27001 (Pallas, 2009).

- "ISO/IEC 27004: Provee una guía y consejos para el desarrollo y uso de métricas para evaluar la efectividad de un Plan de seguridad de la información, los objetivos de control y controles utilizados para implementar y gestionar la Seguridad de la Información, de acuerdo con la norma ISO/IEC27001 (Pallas, 2009).

- "ISO/IEC 27005: Provee una guía metodológica para la Gestión de Riesgos de una Organización, alineada con los requerimientos de la norma ISO/IEC 27001 (Pallas, 2009).

2.1.6. COBIT

Cobit es un acrónimo formado por las siglas derivadas de Control Objectives for Information and Related Technology (Objetivos de Control para Tecnología de Información y Tecnologías Relacionadas).

COBIT 5 es el marco de gestión y de negocio global para el gobierno y la gestión de las Tecnologías de Información de la empresa. Contiene cinco principios y define los 7 catalizadores que componen el marco.

2.1.6.1. Beneficios

COBIT 5 ayuda a empresas de todos los tamaños a:

- Optimizar los servicios el coste de las TI y la tecnología.
- Apoyar el cumplimiento de las leyes, reglamentos, acuerdos contractuales y las políticas.
- Gestión de nuevas tecnologías de información.

2.1.6.2. COBIT como metodología para seguridad de la información

En el mes de junio del 2012, ISACA lanzó "COBIT 5 para la seguridad de la información", actualizando la última versión de su marco a fin de proporcionar una guía práctica en la seguridad de la empresa, en todos sus niveles prácticos.

COBIT 5 para seguridad de la información puede ayudar a las empresas a reducir sus perfiles de riesgo a través de la adecuada administración de la seguridad. La información específica y las tecnologías relacionadas son cada vez más esenciales para las organizaciones, pero la seguridad de la información es esencial para la confianza de los accionistas.

2.1.6.3. Misión

En la Página de (PEÑA HERRERA José Angel, 2012) nenciona que la misión de COBIT es "investigar, desarrollar, publicar y promocionar un conjunto de objetivos de control generalmente aceptados para las tecnologías de la información que sean autorizados (dados por alguien con autoridad), actualizados, e internacionales para el uso del día a día de los gestores de negocios (también directivos) y auditores".

Gestores, auditores, y usuarios se benefician del desarrollo de COBIT porque les ayuda a entender sus Sistemas de Información (o tecnologías de la información) y decidir el nivel de seguridad y control que es necesario para proteger los activos de sus compañías mediante el desarrollo de un modelo de administración de las tecnologías de la información.

2.1.7. Metodología de Riesgos

2.1.7.1. Análisis y Gestión de riesgos

(CALDERON HONOFRE Diana, ESTRELLA OCHOA Martín y FLORES VILLAMARIN Manuel, 2011) Afirma que la Seguridad es la capacidad de las redes o de los sistemas de información para resistir los ataques de entes internos y externos, con un determinado nivel de confianza, los accidentes o acciones ilícitas o

malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles

2.1.7.2. Disponibilidad

Disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

2.1.7.3. Integridad

Mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

2.1.7.4. Confidencialidad

Que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

A estas dimensiones canónicas de la seguridad se pueden añadir otras derivadas que nos acerquen a la percepción de los usuarios de los sistemas de información:

2.1.7.5. Autenticidad

Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos. Contra la autenticidad de los usuarios de los servicios de acceso, podemos tener suplantación de identidad.

2.1.7.6. Trazabilidad

Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad.

Todas estas características pueden ser requeridas o no dependiendo de cada caso. Cuando se requieren, no es evidente que se disfruten sin más. Lo habitual que haya que poner medios y esfuerzo para conseguirlas. A racionalizar este esfuerzo se dedican las metodologías de análisis y gestión de riesgos que comienzan con una definición:

2.1.7.7. Riesgo

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema.

2.1.7.8. Análisis de riesgos

Proceso sistemático para estimar la magnitud de los riesgos que pueden afectar la seguridad de la información o que está expuesta en una Organización.

2.1.8. Acuerdo Nro. 166 Secretaria Nacional de la Administración Pública

Los avances de las Tecnologías de la Información y Comunicación han ocasionado que los gobiernos otorguen mayor atención a la protección de sus activos de información con el fin de generar confianza en la ciudadanía, en sus propias instituciones y minimizar riesgos derivados de vulnerabilidades informáticas.

La Secretaria Nacional de Administración Pública, considerando que las TIC son herramientas imprescindibles para el desempeño institucional e inter-institucional y como respuesta a la necesidad de gestiona de forma eficiente y eficaz la seguridad de

la información en las entidades públicas, emitió los Acuerdos Ministeriales Nro. 804 y Nro. 837 del 29 de julio y 19 de Agosto de 2011 respectivamente, mediante los cuales creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación.

2.1.9. Política de Seguridad

Las entidades de la administración Pública Central, Dependiente e Institucional que generan, utilizan, procesas, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema Gubernamental de Seguridad de la Información para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera.

La (SNAP Secretaria Nacional de la Administración Pública , 2013) indica que las entidades públicas podrán especificar una política de seguridad más amplia o específica en armonía con la Constitución, leyes y demás normativa legal propia o relacionada así como su misión y competencias.

2.2. Antecedentes del estado del arte

Existen diferentes enfoques para la implementación de un Sistema de Gestión de Seguridad de la Información. Uno de ellos la familia ISO/IEC 27.000, que contiene una serie de normas/estándares que sirven como base para la implementación del Sistema de Gestión de la Información.

Las mismas están alineadas con los Requerimientos especificados en la ISO/IEC 27.001, e incluyen, normativas sobre gestión de riesgos, métricas, auditoría, directrices / guías de implementación, etc.

Como evidencia y fundamentación de la información utilizada para la elaboración del presente proyecto se indica los siguientes documentos:

- Norma's ISO 27000

- COBIT-5-Information-Security_res_spa_1213
- COBIT-5-Risk_res_Spa_1114
- Gestión de la seguridad de la información, ISO/IEC 27000
- Principios y Directrices (ISO 31000:2009, IDT)
- Acuerdo 166 Esquema gubernamental de la seguridad de la información (EGSI)
- Plan Nacional del Buen Vivir

TGN Systems (2012) señala en su artículo que, las empresas se apoyan cada día más en las tecnologías para sus negocios y la mayoría desarrollan gran parte de su actividad conectadas a Internet o haciendo uso de servicios que utilizan Internet como pasarela de comunicaciones, factor que conduce a la implantación de medidas de seguridad cada vez son más exigentes dado el riesgo que ello implica.

Al igual que el uso de herramientas y sistemas de seguridad que nos protejan de amenazas externas, también debemos asegurar las amenazas internas o los usuarios. Son las personas que utilizan la estructura tecnológica y saben cómo es su funcionamiento, gestionan la información y las comunicaciones.

La seguridad debe establecerse mediante normas de funcionamiento y uso, perfiles de usuarios, perfiles de grupos o departamentos, restricciones, autorizaciones, denegaciones, protocolos y todo lo necesario para poder obtener un buen nivel de seguridad informática siempre evaluando antes el impacto en el desempeño diario por parte de los usuarios y de la misma empresa.

A través de la seguridad informática, garantizaremos la protección y disponibilidad de la información, de la infraestructura computacional y de los recursos informáticos. Se ´puede distinguir y diferenciar dos grupos de amenazas. Las amenazas internas**,** normalmente son amenazas más serias que las amenazas externas por varias razones:

Los trabajadores conocen perfectamente la red y saben cómo es el funcionamiento de la misma, tienen ciertos niveles de acceso a la red dadas las necesidades de su trabajo, normalmente tienen acceso a las comunicaciones y a Internet.

Amenazas externas son aquellas que se originan fuera de nuestra red, como por ejemplo un intruso que busca la manera de acceder a nuestros sistemas; para TGN-(Systems) La ventaja es que los administradores pueden prevenir parte de los ataques externos.

En la actualidad la tecnología de la información es sin lugar a dudas, lo que más rápidamente ha evolucionado en el mundo, siendo base importante en las operaciones administrativas y financieras de las empresas de hoy, cambiando los hábitos de las personas, lanzándolas a realizar transacciones en Internet de todo tipo, en forma automática, sin intermediarios y en cualquier lugar. Todo este nuevo mundo digital necesita que existan mecanismos que controlen la legitimidad de la información y que aseguren que la misma no ha sido cambiada o alterada.

Es por este motivo que la seguridad informática juega un rol muy importante dentro del mundo informático y es debido a esto que las empresas recientemente han comenzado a demandar especialistas con conocimientos del más alto nivel en el campo de la Seguridad Informática, razón por la cual la Escuela Superior Politécnica del Litoral (ESPOL) a través de su Facultad de Ingeniería en Electricidad y Computación (FIEC) presenta el programa de Maestría en Seguridad Informática Aplicada (MSIA).

2.3. Marco conceptual

2.3.1. Marco normativo para seguridad de la información

Entre los estándares de seguridad de la información aplicables al presente proyecto, tenemos Normas ISO 27000, COBIT 5 Security Information.

La integración de estas normas especifica requisitos para establecer, implantar, poner en ejecución, controlar, revisar, mantener y mejorar un Plan de seguridad de la información.

2.3.1.1. Familia de las normas ISO 27000

Son estándares de seguridad de la información publicados por la ISO (Organización Internacional para la Estandarización) y la IEC (Comisión Electrónica Internacional), la normativa contiene las mejores prácticas recomendadas para desarrollar, implementar y controlar un Plan de seguridad de la información.

A continuación se describirá las principales normas de esta familia que son aplicables al presente proyecto:

- Normas base: 27001, 27002
- Normas complementarias: 27003, 27004, 27005 entre otras.

Seguridad de la información según **ISO27001:** preserva la confidencialidad, integridad y disponibilidad, de los sistemas involucrados en su tratamiento de seguridad.

- **ISO/IEC 27000:**

  Define términos y conceptos utilizados en la familia 27000, contiene un conjunto de estándares desarrollados que proporcionan un marco referencial para la gestión de seguridad de la información, utilizable por cualquier tipo de organización.

- **ISO/IEC 27001:**

  Define los requisitos para implantar un Plan de seguridad de la información, así como la participación y responsabilidad del personal involucrado, se adapta al modelo PDCA (Plan-Do-Check-Act) más conocido como ciclo de Deming como se muestra en la **Figura 5**, el objetivo de esta norma es la mejora continua.

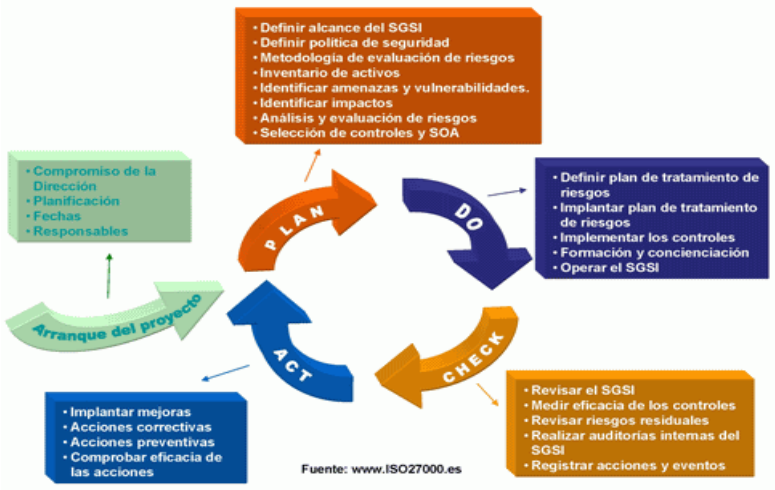

Figura 5 Mejora continua de un Plan de seguridad de la información

Fuente: (NORMAS ISO 27000, 2015)

- **Fase de planificación (Plan):**

  Establece objetivos, políticas, procesos y procedimientos relacionados con la gestión del riesgo y mejorar la seguridad de la información en una organización.

- **Fase de planificación (Do):**

  Define la implementación y gestión de un Plan de seguridad de la información, de acuerdo al establecimiento de políticas, controles, procesos y procedimientos.

- **Fase de planificación (Check):**

  Se establece monitoreo y revisión continua de las políticas, controles, procesos y procedimientos de un Plan de seguridad de la información.

- **Fase de planificación (Act):**

  Adopta acciones correctivas y preventivas basadas en auditorias y revisiones internas de la información relevante a la gestión de seguridad para alcanzar la mejora continua del Plan de seguridad de la información.

- **ISO/IEC 27002:**

  Define buena prácticas para la gestión de seguridad como, medidas y aspectos a analizar para garantizar la seguridad de la información, en la **Figura 6** muestra los aspectos y secciones que aplica la norma. El objetivo de esta fase es definir los aspectos prácticos y operativos de la implantación de un Plan de seguridad de la información.

  - **Áreas de actuación:**
    - ✓ Política de seguridad
    - ✓ Aspectos organizativos para la seguridad
    - ✓ Clasificación y control de activos
    - ✓ Seguridad ligada al personal
    - ✓ Seguridad física y del entorno
    - ✓ Gestión de comunicaciones y operaciones
    - ✓ Control de accesos
    - ✓ Desarrollo y mantenimiento de sistemas
    - ✓ Gestión de incidentes de seguridad de la información
    - ✓ Gestión de continuidad del negocio

Figura 6 Áreas y secciones para actuar frente al riesgo

Fuente: (NORMAS ISO 27000, 2015)

Se debe asegurar los objetivos de control dentro de cada área o sección. Respecto a los controles se define como mecanismos para asegurar los distintos objetivos de control (guía de buenas prácticas). Para cada control se incluye una guía para su implantación.

- **ISO/IEC 27003**

Describe la guía de implementación de un Plan de seguridad de la información, basado en el modelo PDCA y los requerimientos de sus diferentes fases, se trata de una norma adaptable para implantadores así como consultores de un Sistema de Gestión de Seguridad.

(SGSI, 2014) expone en su norma el siguiente contenido:

- Alcance.
- Referencias Normativas.
- Términos y Definiciones.
- Estructura de esta Norma.
- Obtención de la aprobación de la alta dirección para iniciar un Plan de seguridad de la información.
- Definición del alcance, límites y políticas.
- Evaluación de requerimientos de seguridad de la información.
- Evaluación de Riesgos y Plan de tratamiento de riesgos.
- Diseño del Plan de seguridad de la información.

- **ISO/IEC 27004**

Esta norma define la medición de seguridad de la información a través de métricas y técnicas aplicables para determinar la eficacia y aplicabilidad de un Plan de seguridad de la información, además los controles relacionados.

Las etapas propuestas por ISO 27004 con el objetivo de medir la eficacia de la seguridad de la información son:

- Selección procesos y objetos de medición.
- Definición de las líneas base.
- Recopilación de datos.
- Desarrollo de un método de medición.
- Interpretación de los valores medidos.
- Comunicación de los valores de medición.

Los resultados de medición del Plan de seguridad de la información se comunicarán a las partes interesadas. Además el Sistema de Gestión de Seguridad Informática (SGSI, 2014) explica que se puede hacer en forma de gráficos, cuadros de mando operacionales, informes o boletines de noticias

- **ISO/IEC 27005**

Define la gestión de riesgos en la seguridad de la información (métodos y técnicas para la evaluación de riesgos de la seguridad). La norma 27005 es aplicable a la gestión de riesgos que puedan complicar la seguridad de la información de cualquier organización pública o privada ya sea pequeña o grande.

Las secciones de este contenido son:

- Prefacio.
- Introducción.
- Referencias normativas.
- Términos y definiciones.
- Estructura.
- Fondo.
- Descripción del proceso de ISRM.
- Establecimiento Contexto.
- Información sobre la evaluación de riesgos de seguridad (ISRA).
- Tratamiento de Riesgos Seguridad de la Información.
- Admisión de Riesgos Seguridad de la información.
- Comunicación de riesgos de seguridad de información.

- Información de seguridad Seguimiento de Riesgos y Revisión.
- Definición del alcance del proceso.
- Valoración de activos y evaluación de impacto.
- Ejemplos de amenazas típicas.
- Las vulnerabilidades y métodos de evaluación de la vulnerabilidad.
- Enfoque ISRA

El Sistema de Gestión de Seguridad Informática (SGSI, 2014) trata de un estándar que cuenta con una parte principal concentrada en 24 páginas, también cuenta con anexos en los que se incluye ejemplos y más información de interés para los usuarios

2.3.1.2. COBIT 5 Security Information

COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde la tecnología de la información (TI) manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.

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

Para (PEÑA HERRERA José Angel, 2012), COBIT 5 para Seguridad de la Información, destacado en la **Figura7**, basado en el marco de COBIT 5, se enfoca en la seguridad de la información y proporciona una guía más detallada y práctica para los profesionales de seguridad de la información y otras partes interesadas a todos los niveles de la empresa.

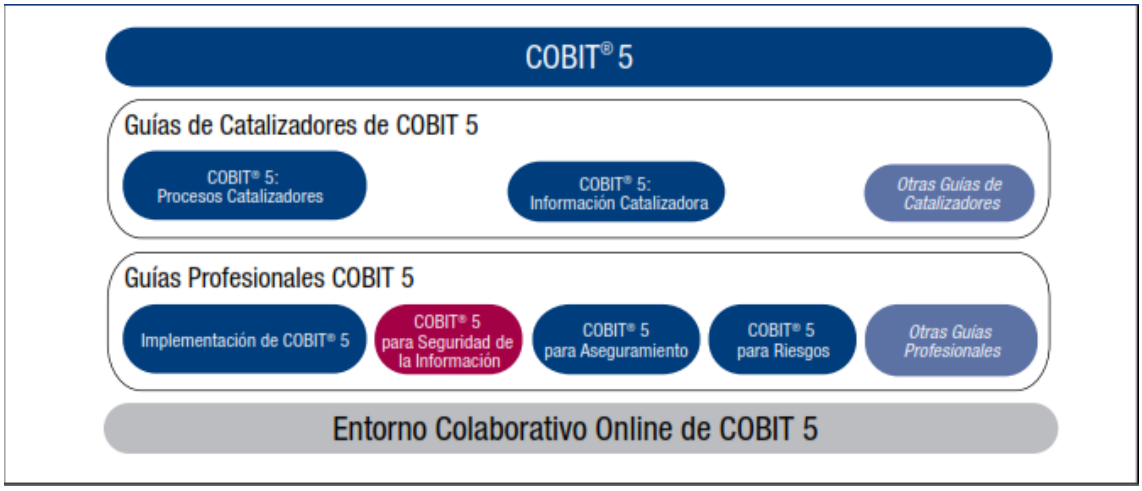

Figura 7 Familia de productos COBIT 5

Fuente: (ISACA –COBIT, 2015)

- **Motivos para aplicar COBIT 5 para Seguridad de la Información**

En (ISACA, 2015) COBIT 5, los procesos APO13 Gestionar la seguridad, DSS04 Gestionar la continuidad y DSS05 Gestionar los servicios de seguridad proporcionan una guía básica acerca de cómo definir, operar y monitorizar un sistema para la gestión general de seguridad. Por lo tanto, COBIT 5 para Seguridad de la Información proporciona la nueva guía de ISACA para el gobierno y la gestión corporativa de la seguridad de la información.

Los motivos más importantes para el desarrollo de COBIT 5 para Seguridad de la Información incluyen. La necesidad de describir la seguridad de la información en el contexto de una empresa incluyendo:

- Las responsabilidades funcionales de principio a fin de seguridad de la información para el negocio y TI.
- Todos los aspectos que llevan a un gobierno y gestión efectivos de la seguridad de la información, tales como estructuras organizativas, políticas y cultura.
- La relación y enlace de la seguridad de la información con los objetivos de la empresa.

Una necesidad creciente de la empresa de:

- Mantener el riesgo de información a un nivel aceptable y proteger la información contra divulgaciones no autorizadas, modificaciones involuntarias o no autorizadas y posibles intrusiones.
- Asegurar que los servicios y sistemas se encuentran disponibles continuamente para los grupos de interés internos y externos, con el objetivo de satisfacer a los usuarios en relación al compromiso y los servicios proporcionados por TI.

- **Beneficios de aplicar COBIT 5 para Seguridad de la Información**

(ISACA, 2015) afirma que al utilizar COBIT 5 para Seguridad de la Información proporciona a la empresa una serie de capacidades relacionadas con la seguridad de la información que pueden resultar en beneficios como:

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

- **Principios de COBIT 5 para Seguridad de la Información**

La **Figura 8,** muestra los principios de COBIT 5 Security Information, estos indican el contexto de aplicabilidad de COBIT en una organización,

proporcionado valor para las partes interesadas para lograr esto se requiere un Gobierno y Administración comprometido con la gestión de la norma.

Figura 8 Principios de COBIT 5 Security Information

Fuente: (ISACA –COBIT, 2015)

- **Satisfacer las necesidades de las partes interesadas**

Este principio de se basa en la cascada de objetivos de COBIT 5 permite definir prioridades de acuerdo a:

- Implementación
- Mejora
- Aseguramiento de gobernabilidad de las TI en la empresa

En la práctica, la cascada de objetivos:

- Define las metas y objetivos relevantes y tangibles en los diversos niveles de responsabilidad
- Filtra la base del conocimiento de COBIT 5, basado en las metas de la empresa para extraer la orientación relevante a incluir en la implementación, mejoras o proyectos de aseguramiento específicos.
- Identifica y comunica claramente cómo se usan los catalizadores para alcanzar los objetivos de la empresa

- **Cubrir la organización de forma integral**

  Este principio integra la gobernabilidad de las TI de la empresa dentro de la gobernabilidad empresarial y/o cubre todas las funciones y procesos necesarios para gobernar y administrar la información de la empresa y tecnologías relacionadas dondequiera que se procese la información.

- **Aplicar un solo marco integrado**

  Permite alinearse con los marcos de referencia y normas relevantes más recientes.

  - Es completo en cuanto a la cobertura de la empresa
  - Proporciona una base para integrar eficazmente otros marcos de referencia, normas y prácticas usados.
  - Integra todos los conocimientos anteriormente dispersos en diferentes marcos de referencia de ISACA.
  - Proporciona una arquitectura simple para estructurar materiales de orientación y elaborar un conjunto de productos coherentes.

- **Habilitar un enfoque holístico**

  (ISACA, 2015) COBIT 5 define un conjunto de catalizadores como muestra en la **Figura 9**, para apoyar la implementación de un sistema integral de gestión y gobierno de las TI empresariales.

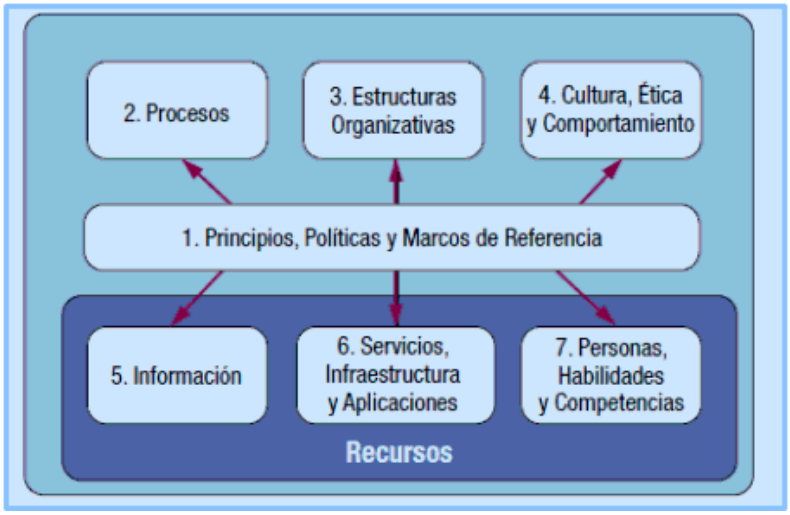

Figura 9 Catalizadores del COBIT 5

Fuente: (ISACA –COBIT, 2015)

- **Separar el Gobierno de la Administración**

El **Gobierno** asegura que las necesidades, condiciones y opciones de las partes interesadas:

- Sean evaluadas para determinar un equilibrio, en acuerdo con los objetivos que desea lograr la empresa.
- Ajuste por parte de la dirección a través de la priorización y toma de decisiones.
- Supervisar el rendimiento, cumplimiento y progreso frente a la dirección y los objetivos acordados (EDM).

La **Gerencia** planifica, desarrolla, ejecuta y supervisa:

- Actividades alineadas con la dirección establecida por el órgano de gobierno, para alcanzar los objetivos de la empresa.

En la **Figura 10**se indica el modelo de referencia de procesos aplicados por COBIT 5 Security Information.

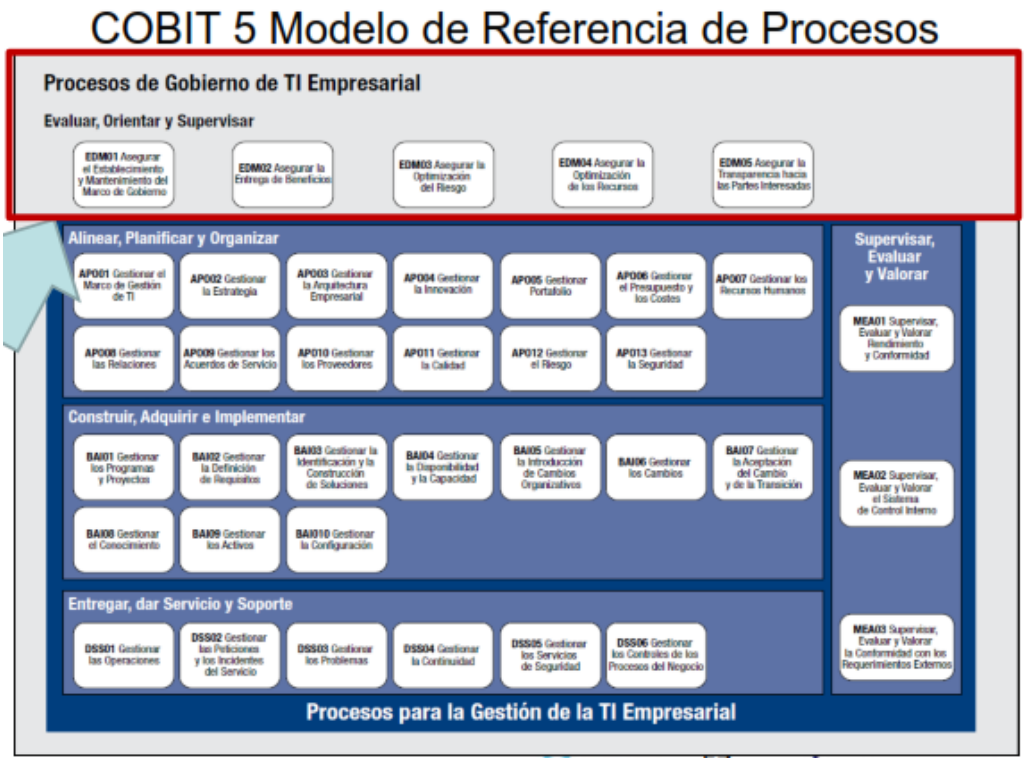

Figura 10 Modelo de referencia de procesos de COBIT 5

Fuente: (ISACA –COBIT, 2015)

Se puede decir entonces que COBIT 5 para Seguridad de la Información se refiere a varios catalizadores como roles, puestos, comités, procesos y políticas. Las características únicas de cada empresa pueden ocasionar que estos catalizadores sean utilizados de muchas formas distintas para proporcionar seguridad de la información de una forma óptima, además esta metodología utiliza guías y ejemplos que proporcionan una visión completa que explica cada concepto de COBIT 5 desde una perspectiva de seguridad de la información.

2.3.1.3. Norma ISO 31000 para gestión de riesgos

Se trata de una norma para evaluar gestión de riesgos. Mientras todas las organizaciones gestionan el riesgo a diferentes niveles, esta norma internacional establece un conjunto de principios que se deben a satisfacer para que la gestión del riesgo sea eficaz, recomienda que las organizaciones desarrollen, implementen y mejoren de manera continuada un marco de trabajo cuyo objetivo sea integrar el

proceso de gestión del riesgo en los procesos de gobierno, de estrategia y de planificación, de gestión, y de elaboración de informes, así como en las políticas, los valores y en la cultura de toda la organización.

- **Campo de aplicación de la norma**

  Esta norma internacional proporciona los principios y las directrices genéricas sobre gestión del riesgo.

  - Puede utilizarse por cualquier empresa pública, privada o social, asociación.
  - Puede utilizarse por cualquier empresa grupo o individuo. Por tanto, no es específica de una industria o sector concreto.

- **Beneficios de la norma**

  Cuando la gestión de riesgo se implementa y se mantiene de acuerdo con esta norma, dicha gestión le permite a la organización entre otros:

  - Aumentar la posibilidad de alcanzar los objetivos.
  - Fomentar la gestión proactiva.
  - Ser consciente de la necesidad de identificar y tratar los riesgos en toda la organización.
  - Cumplir con los requisitos legales y reglamentarios pertinentes y con las normas internacionales.
  - Mejorar la presentación de informes obligatorios y voluntarios.
  - Mejorar el gobierno.
  - Mejorar la confianza y honestidad de las partes involucradas.
  - Establecer una base confiable para la toma de decisiones y la planificación.
  - Mejorar controles.
  - Asignar y usar eficazmente los recursos para el tratamiento de los riesgos.
  - Mejorar la eficiencia y eficacia proactiva.
  - Incrementar el desempeño de la seguridad.
  - Mejorar la prevención de pérdidas y la gestión de incidentes.
  - Minimizar las perdidas.

CAPÍTULO III

METODOLOGÍA DE INVESTIGACIÓN

3.1. Tipo de investigación

Para el desarrollo del proyecto se aplica la investigación de campo, ya que se realiza en el sitio donde está el objeto de estudio en este caso ESPE Sede Santo Domingo, esto permite manejar un conocimiento más especializado sobre la situación. La investigación de campo se apoya en información obtenida mediante entrevistas, reuniones observación y asesoramiento técnico.

3.2. Métodos y Técnicas de Investigación

Para el desarrollo del proyecto se utiliza el método propositivo de (Pinal Mora, 2006), que parte del Análisis de la Situación actual de la ESPE Santo Domingo y concluye con la propuesta del Diseño del Sistema de Gestión de Seguridad.

Para el desarrollo del Plan de seguridad de la información e aplica las siguientes técnicas de investigación.

- Observación directa
- Entrevista
- Como instrumento Cuestionario

Los mismos que son desarrollados en base a las siguientes matrices:

- Matriz de objetivos ESPE-COBIT 5.
- Matriz de procesos COBIT 5 Security- Objetivos TI.
- Matriz de mapeo COBIT 5 Security con estándares relacionados.
- Matriz plan de investigación de campo COBIT 5.

3.3. Metodología de investigación para la Sede Santo Domingo

En la metodología de investigación campo, se obtiene información de la situación actual de la Universidad de las Fuerzas Armadas ESPE Sede Santo Domingo, cuya información es importante para el diseño de la propuesta de un Sistema de Gestión de Seguridad de la Información.

3.3.1. Información del ambiente para el diseño del Plan de seguridad de la información

El diseño del Plan de seguridad de la información tendrá como ambiente de desarrollo la Unidad de Tecnologías de Información y Comunicación (UTIC) ESPE Matriz y Sede Santo Domingo, el proceso de desarrollo y aplicación de los diferentes planes de gestión orientados a las tecnologías de la información serán aplicables tanto para la matriz como para sus sedes, nuestra investigación se orienta a la sede Santo Domingo.

- **Inventario de aplicaciones**

  La Unidad de Tecnologías de Información y Comunicación UTIC, administra diferentes aplicaciones del entorno educativo superior y de áreas relacionadas, en el **Anexo 4,** muestra el inventario correspondiente al software administrado por la unidad mencionada.

- **Estructura de red 2014**

  La **Figura 11**, describe la estructura de red que se administra por la UTIC, enfocado a establecer servicios de interconectividad de software, servicios de comunicación entre la ESPE matriz y sus sedes y demás especificaciones tecnológicas concernientes a la unidad.

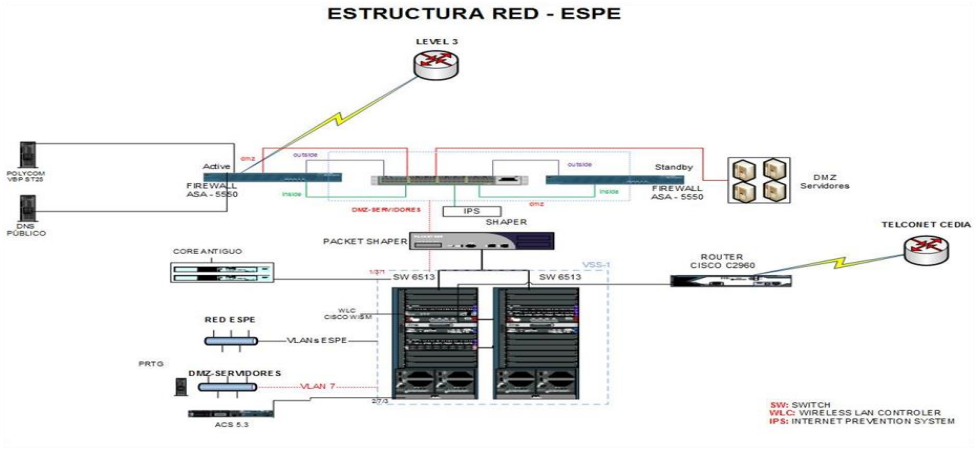

Figura 11 Estructura de Red UTIC

Fuente: (ESPE-UTIC, 2014)

- **Catálogo de servicios TICS 2014**

El **Anexo 4,** indica los diferentes servicios de recursos tecnológicos que presta la UTIC a la institución en general, además describe tipos de acceso, horarios y observaciones si fuese el caso para alguno de los servicios.

En el **Anexo 5,** se indica los recursos tecnológicos del que dispone para generar información la ESPE Sede Santo Domingo.

- **Recurso humano UTIC**

En la **Tabla 1,** se describe al personal de planta que se encuentra distribuido por áreas o departamentos que conforma la Unidad de Tecnologías de Información y Comunicación UTIC.

Tabla 1

Distributivo de Recurso Humano-UTIC

ORD.	NOMBRES	AREA
1	MAYO. DIEGO BURBANO	DIRECTOR
2	ING. MAGALI REASCOS	PLANIFICACION
3	SRA. JANNETH ONOFA	SECRETARIA
4	ING. MA. DEL CARMEN ACOSTA	COORDINADORA GESTION Y SOPORTE
5	ING. ALEJANDRA CUADROS	HELP DESK
6	ING. ALEXANDRA TAPIA	HELP DESK
7	ING. CHRISTIAN CORONEL	GESTION Y SOPORTE
8	TGLO. EFREN PICHUCHO	GESTION Y SOPORTE
9	ING. JONATHAN GUAMBI	GESTION Y SOPORTE
10	ING. MONICA ARMAS	COORDINADORA CONECTIVIDAD Y REDES
11	ING. ALEXANDRA GARCIA	CONECTIVIDAD Y REDES

CONTINÚA ⟶

12	ING. ANDRES CASTILLO	CONECTIVIDAD Y REDES
13	ING. SANTIAGO PINTO	CONECTIVIDAD Y REDES
14	ING. MAURICIO BALDEON	CONECTIVIDAD Y REDES
15	TEC. MIGUEL ALMAGRO	CONECTIVIDAD Y REDES
16	ING. SANTIAGO SALVADOR	CONECTIVIDAD Y REDES
17	ING. PATRICIA NOGALES	COORDINADORA SISTEMAS DE INFORMACION
18	ING. NELLY CEVALLOS	SISTEMAS DE INFORMACION
19	ING. MONICA PULLAS	SISTEMAS DE INFORMACION
20	ING. ANITA TORRES	SISTEMAS DE INFORMACION
21	ING. LORENA DUQUE	SISTEMAS DE INFORMACION
22	ING. CARLOS ALDAS	SISTEMAS DE INFORMACION
23	ING. SANTIAGO HIDALGO	SISTEMAS DE INFORMACION

Fuente (ESPE – UTIC, 2015)

En el **Anexo 6**, se muestra el recurso humano con el que cuenta la ESPE sede Santo Domingo en sus diferentes áreas.

3.3.2. Selección de procesos relacionados con el diseño del Plan de seguridad de la información

Los recursos tecnológicos de la información (TI), requieren ser administrados de acuerdo al modelo integrador de COBIT 5 Security Information, aplicando los 5 principios y el modelo de gestión cascada de COBIT, dichos procesos se encuentran organizados de acuerdo a la estructura cascada y los catalizadores de medición como se muestra en la **Tabla 2**.

Tabla 2

Procesos COBIT 5

Procesos de Cobit Security 5		
Evaluar, Orientar y Monitorizar	EDM01	Asegurar el establecimiento y Mantenimiento del Marco de Gobierno
	EDM02	Asegurar la Entrega de Beneficios
	EDM03	Asegurar la Optimización del Riesgo
	EDM04	Asegurar la Optimización de los Recursos
	EDM05	Asegurar la Transparencia hacia las partes interesadas
Alinear, Planificar y Organizar	APO01	Gestionar el Marco de Gestión de TI
	APO02	Gestionar la Estrategia
	APO03	Gestionar la Arquitectura Empresarial
	APO04	Gestionar la Innovación
	APO05	Gestionar el Portafolio
	APO06	Gestionar el Presupuesto y los Costes

CONTINÚA

	APO07	Gestionar los Recursos Humanos
	APO08	Gestionar las Relaciones
	APO09	Gestionar los Acuerdos de Servicios
	APO10	Gestionar los Proveedores
	APO11	Gestionar la Calidad
	APO12	Gestionar el Riesgo
	APO13	Gestionar la Seguridad
Construcción, adquisición e implementación	BAI01	Gestionar los Programas y Proyectos
	BAI02	Gestionar la Definición de requisitos
	BAI03	Gestionar la identificación y la construcción de soluciones
	BAI04	Gestionar la disponibilidad y la capacidad
	BAI05	Gestionar la introducción de cambios organizados
	BAI06	Gestionar los cambios
	BAI07	Gestionar la aceptación del cambio y de la transición
	BAI09	Gestionar los activos
	BAI10	Gestionar la configuración
Entregar, dar servicio y soporte	DSS01	Gestionar las operaciones
	DSS02	Gestionar las peticiones y los incidentes del servicio
	DSS03	Gestionar los problemas
	DSS04	Gestionar la continuidad
	DSS05	Gestionar los servicios de seguridad
	DSS06	Gestionar los controles de los procesos del negocio
Supervisar, evaluar y valorar	MEA01	Supervisar, evaluar, valorar rendimiento y conformidad
	MEA02	Supervisar, evaluar, valorar el sistema de Control Interno
	MEA03	Supervisar, valorar, valorar la conformidad con los requerimientos externos

3.3.2.1. Matriz mapeo Objetivos ESPE-COBIT 5

Se realiza un mapeo de los objetivos estratégicos de la Universidad de las Fuerzas Armadas con los objetivos corporativos de COBIT 5 Security Information, como se muestra en el **Tabla3,** en la que se puede visualizar la relación entre los procesos y la forma de evaluar de acuerdo a la relación, cuyos valores se determinan de la siguiente manera:

0 = Ninguna relación
1 = Poca relación
2 = Mediana relación

3 = Directamente relacionado

Para el análisis de resultados se toma en cuenta los tres valores más altos, para la evaluación en las dos direcciones de la matriz**,** además estos resultados servirán para un posterior mapeo de análisis de los objetivos de COBIT y los objetivos de TI.

Tabla 3

Matriz mapeo objetivos ESPE-COBIT 5

Objetivos Corporativos Empresa/ Objetivos Corporativos COBIT Security Information	Valor para las partes interesadas de las inversiones de negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activo)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basadas en información	Optimización de costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Programas gestionados de cambio en el negocio	Optimización de los costes de los procesos de negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Personal entrenado y motivado	Cultura de innovación del producto y del negocio	
Incrementar el reconocimiento de la Universidad de las Fuerzas Armadas - ESPE como una institución referente a educación superior	3	0	0	1	0	0	0	0	1	0	2	0	0	0	0	0	1	**8**
Incrementar la calidad de los profesionales y postgraduados	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Incrementar la producción científica - tecnológica y su calidad	2	0	1	1	0	0	0	0	0	0	3	0	3	0	1	0	2	**13**
Incrementar el impacto social de los programas de vinculación	2	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	4
Incrementar la eficiencia y eficacia del sistema formativo de grado y pregrado	2	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	4
Incrementar la capacidad del sistema de investigación integrándolo con el modelo formativo	2	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	3
Incrementar la capacidad y calidad del sistema de vinculación integrándolo con el sistema de investigación y con el modelo formativo	2	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	3
Incrementar las capacidades de sustentación institucional. Talento humano-Finanzas-Recursos Físicos y Tecnológicos	2	0	0	0	1	0	1	1	0	0	2	1	0	1	1	1	2	**13**
	15	0	1	2	1	0	3	1	2	0	**7**	1	4	3	2	1	**5**	

Como indica la matriz, los objetivos estratégicos de la Universidad de las Fuerzas Armadas apuntan a la excelencia educativa, versus los objetivos corporativos de COBIT se enfocan en los optimización de procesos y recursos, proponiendo llegar a una cultura de gestión de información segura, esto tanto de autoridades como de personal en general para llegar a la satisfacción de las partes interesadas.

3.3.2.2. Matriz mapeo Objetivos COBIT Security - TI

Los recursos de la Tecnología de la Información TI, requieren ser administrados por una optimización de procesos agrupados, con el fin de proporcionar la información que la institución, que necesite para alcanzar sus objetivos. La selección de procesos orientados a la realización Plan de seguridad de la información para la ESPE sede Santo Domingo, se basa en ponderaciones que satisfacen los requerimientos de información de la institución como muestra la **Tabla 4**, pero a su vez no son suficientes por lo que la definición de la valoración queda de la siguiente manera:

Primario (P): Grado de impacto directo a los objetivos y procesos.
Secundario (S): Grado de impacto indirecto o de menor medida de requerimiento de información.

Tabla 4

Matriz mapeo procesos COBIT Security vs Objetivos de TI

			Objetivos relacionados con TI																
			Alineamiento de TI y la Estrategia de Negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionado con las TI gestionados	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
	Procesos de Cobit Security 5		Financiera						Cliente		Interna							Aprendizaje - Crecimiento	
Evaluar, Orientar y Monitorizar	EDM01	Asegurar el establecimiento y Mantenimiento del Marco de Gobierno	P	S	P	S	S	S	P	P	S	P	S	S	S	S	P	P	S
	EDM02	Asegurar la Entrega de Beneficios	P		S	P		P	S				S			S		S	P
	EDM03	Asegurar la Optimización del Riesgo	P	P	S	P	S	P	S	S	S	P	S	S	S	S	P	S	S
	EDM04	Asegurar la Optimización de los Recursos	S	P	S	P	S	P	S	S	P	S	P	S	S	S	P	S	S
	EDM05	Asegurar la Transparencia hacia las partes interesadas	S	S	P			P	P			P			S	S	S		S
Alinear, Planificar y Organizar	APO01	Gestionar el Marco de Gestión de TI	P	P	S	S	S	S	S	S	P	P	P	S	S	S	P	S	S
	APO02	Gestionar la Estrategia	P	S	P	S	P	S	P	S	S	P	S	S	P	S	S	S	P
	APO03	Gestionar la Arquitectura Empresarial	P		S		S		S	S	P		P	S		S			S
	APO04	Gestionar la Innovación	S			S				P	P		P	S		S			P
	APO05	Gestionar el Portafolio	P		S	S		S	S	S	S		S		P				S
	APO06	Gestionar el Presupuesto y los Costes	S		S	S		S	S	S	S		S		P				
	APO07	Gestionar los Recursos Humanos	P	S	S	S	P	P	S	P	S	P	P	S	P	S	S	P	P
	APO08	Gestionar las Relaciones	P		S		S		S	S			S	P			S	S	P

CONTINÚA

	APO09	Gestionar los Acuerdos de Servicios	S	P	P	S	P	S	S	S	S	P	S	S	P	P	S	P	P
	APO10	Gestionar los Proveedores		S			S	S		S	P		S		S		S		
	APO11	Gestionar la Calidad	P	S	S	S	P	P	S	P	S	P	S	S	P	S	S	S	S
	APO12	Gestionar el Riesgo	P	P	S	P	S	P	S	P	S	P	P	S	P	S	P	S	S
	APO13	Gestionar la Seguridad	P	P	S	P	S	P	S	P	S	P	P	P	S	P	P	S	S
Construcción, adquisición e implementación	BAI01	Gestionar los Programas y Proyectos	S		P	P		S				P				S	P	P	
	BAI02	Gestionar la Definición de requisitos		S	S	S	S		P	S	S	S	S	P	S	S	P	S	S
	BAI03	Gestionar la identificación y la construcción de soluciones	S			S	S		P	S			S	S	S	S			S
	BAI04	Gestionar la disponibilidad y la capacidad				S	S		P	S	S		P		S	P			S
	BAI05	Gestionar la introducción de cambios organizados	S		S		S		S	P	S		S	S	P				P
	BAI06	Gestionar los cambios			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Gestionar la aceptación del cambio y de la transición				S	S		S	P	S			P	S	S	S		S
	BAI09	Gestionar los activos	P	S	P	P	S	P	P	P	S	S	P	S	P	S	S	S	P
	BAI10	Gestionar la configuración		P		S		S		S	S	S	P			P	S		
Entregar, dar servicio y soporte	DSS01	Gestionar las operaciones		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	Gestionar las peticiones y los incidentes del servicio							P	S		S				S	S		S
	DSS03	Gestionar los problemas		S			S			S	S		P	S		P	S		
	DSS04	Gestionar la continuidad	S	S	P	P	S	S	P	S	S	S	S	S	P	P	S	P	S
	DSS05	Gestionar los servicios de seguridad	S	P	P	P	S	P	S	S	P	P	S	S	P	S	S	P	S
	DSS06	Gestionar los controles de los procesos del negocio		S					P	S		S	S			S	S	S	S
Supervisar, evaluar y valorar	MEA01	Supervisar, evaluar, valorar rendimiento y conformidad	P	P			S	S			P			S	S		P	S	S
	MEA02	Supervisar, evaluar, valorar el sistema de Control Interno	P			S			S	P				S	S	P			S
	MEA03	Supervisar, valorar, valorar la conformidad con los requerimientos externos	S	P	P							S				P			P

3.3.2.3. Matriz mapeo COBIT Security con Estándares Relacionados

Para el aseguramiento de la selección de procesos se realiza un mapeo entre varios estándares y marcos internacionales, relacionados con la seguridad de la información como se muestra en la **Tabla 5**, además se fundamenta en requerimientos de algunos profesionales expertos en la seguridad de la información y el entorno de las organizaciones que se desarrollan en el tema.

Los siguientes estándares se incluyen en la matriz de comparación:

- Series ISO/IEC 27000: La norma 27000 proporciona un modelo para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un Plan de seguridad de la información. Los dominios y áreas de COBIT 5 para la seguridad de la información se cubren en la serie ISO/IEC 27000, incluyendo los objetivos de control.

- ISO/IEC 27001: Define procesos de seguridad, relativos a los riesgos de los dominios EDM, APO y DSS. Además varias actividades referentes a seguridad dentro de procesos en otros dominios. Se incluye también actividades de supervisión y evaluación del dominio MEA.

- ISF 2011 Standard of Good Practice for Information Security se basa en el Modelo de Seguridad de la Información de ISF y consiste en un esquema general de buenas prácticas de negocio que se agrupan por áreas y se dividen en cuatro categorías principales: gobierno de seguridad de la información, requerimientos de seguridad de la información, marco de control y supervisión y mejora de la seguridad de la información.

- Guide for Assessing the Information Security Controls in Federal Information Systems and Organisations, NIST: El propósito de esta guía es proporcionar una orientación con respecto a los controles de seguridad de una agencia ejecutiva del gobierno de los EEUU.

Tabla 5

Matriz mapeo COBIT Security con Estándares relacionados a la seguridad

COBIT 5 para seguridad de la información	ISO/IEC 27001	ISO/IEC 27002	ITIL(Buenas prácticas de la información)	NIST(Instituto Nacional de estándares y tecnología)
EDM01 Asegurar el establecimiento y mantenimiento del marco de gobierno	Compromiso de la dirección	Compromiso de la dirección con la seguridad de la información	Marco de Gobierno de la Seguridad	
	Política de Seguridad			
EDM03 Asegurar la optimización del riesgo	Construir el PLAN DE SEGURIDAD DE LA INFORMACIÓN	Continuidad de negocio y gestión de riesgos	Evaluación de riesgos de la información	
	Implementar y operar el PLAN DE SEGURIDAD DE LA INFORMACIÓN		Continuidad de negocio	
	Supervisar y revisar el PLAN DE SEGURIDAD DE LA INFORMACIÓN		Informes de seguridad de la información	
	Requisitos de documentación			
EDM04. Asegurar la optimización de los recursos	Gestión de recursos			Planificación
	Optimización de la seguridad de la información			
APO01. Gestionar el marco de gestión de las TI	Compromiso de la dirección	Organización de la seguridad de la información	Marco de Gobierno de la Seguridad	
	Política de la seguridad			
	Organización de la seguridad de la información			
APO02. Gestionar la estrategia	Construir el PLAN DE SEGURIDAD DE LA INFORMACIÓN		Estrategia de seguridad de la información	
APO07. Gestionar los recursos humanos	Formación, concienciación y competencia	Seguridad de la información de Recursos Humanos	Seguridad de la información de Recursos Humanos	Concienciación y formación
	Seguridad ligada a los recursos humanos			Planificación
				Seg. de inf. del personal
APO09. Gestionar los Acuerdos de Servicios		Provisión de servicios	Acuerdos de nivel de servicio	Adquisición de sistemas y servicios
		Supervisión y revisión de los servicios prestados por terceros	Supervisión de la seguridad	
		Gestión del cambio en los servicios prestados por terceros	Informes de riesgos de la información	
APO11. Gestionar la Calidad	Revisión de la gestión del PLAN DE SEGURIDAD DE LA INFORMACIÓN		Aseguramiento de la calidad	
	Mejora del PLAN DE SEGURIDAD DE LA INFORMACIÓN			
APO12. Gestionar el riesgo	Construir el PLAN DE SEGURIDAD DE LA INFORMACIÓN	Notificación de eventos de seguridad de la información	Evaluación de riesgos de la información	Respuesta a incidentes
			Cumplimiento	
	Implementar y operar el PLAN DE SEGURIDAD DE LA INFORMACIÓN	Notificación de puntos débiles de seguridad	Política y organización de la seguridad de la información	

CONTINÚA

			Gestión de amenazas y vulnerabilidades	
	Supervisar y revisar el PLAN DE SEGURIDAD DE LA INFORMACIÓN	Inclusión de seguridad de la información en el proceso de gestión de continuidad del negocio	Continuidad de negocio	Evaluación de riesgos
			Informes de riesgos de la información	
	Requisitos de documentación	Continuidad de negocio y gestión de riesgos	Supervisión del cumplimiento de la seguridad de loa información	
APO13. Gestionar la seguridad	Tratado a lo largo de esta norma	Tratado a lo largo de esta norma	Tratado a lo largo de esta norma	
BAI09. Gestionar los activos	Gestión de activos	Inventario de activos	Gestión de activos	Protección de medios
		Propiedad de los activos		
		Etiquetado y manipulado de la información		
		Seguridad de la documentación del sistema		
		Identificación de los equipos en las redes		
		Control de software en explotación		
		Protección de los datos de prueba del sistema	Seguridad física y ambiental de la información	Protección física y ambiental
		Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo		
		Restricciones a los cambios en los paquetes de software		
		Control de las vulnerabilidades técnicas		
		Prevención del uso indebido de los recursos de tratamiento de la información		
DSS04. Gestionar la continuidad	Mantener y mejorar el PLAN DE SEGURIDAD DE LA INFORMACIÓN	Gestión de la continuidad del negocio	Continuidad de negocio	Planificación de contingencias
	Requisitos de documentación			
	Mejora del PLAN DE SEGURIDAD DE LA INFORMACIÓN			
	Gestión de la continuidad del negocio			
DSS05. Gestionar los servicios de seguridad	Supervisar y revisar el PLAN DE SEGURIDAD DE LA INFORMACIÓN	Responsabilidades de la dirección	Política y organización de la seguridad de la información	Protección de medios
				Integridad de sistemas e información

3.3.2.4. Levantamiento de requerimientos

Para recopilar la información se utiliza la matriz de investigación de campo, como se muestra en el **Anexo 7** además de realizar la matriz de los procesos seleccionados con su respectiva entradas/salidas y demás información como muestra el **Tabla 6**, este análisis permitirá la obtención de preguntas relativas a la gestión de riesgos, la documentación que respaldará el levantamiento de información así como sus respectivos responsables.

Tabla 6

Levantamiento de requerimientos para el diseño Plan de seguridad de la información

Código	Descripción Proceso	Pregunta
EDM01	Asegurar el establecimiento y Mantenimiento del Marco de Gobierno	¿El sistema de gobierno de la seguridad de la información está integrado con los procesos institucionales?
EDM03	Asegurar la Optimización del Riesgo	¿La gestión de riesgos asociados a la información forma parte de la gestión general de los riesgos corporativos de la institución?
EDM04	Asegurar la Optimización de los Recursos	¿Los recursos de seguridad de la información están alineados con los requerimientos de la institución?
APO01	Gestionar el Marco de Gestión de TI	
APO02	Gestionar la Estrategia	¿Estrategias relacionadas con la seguridad de la información?
APO07	Gestionar los Recursos Humanos	¿Las capacidades y procesos de recursos humanos están alineados con los requisitos de la seguridad de información?
		¿Número de empleados a los que se les proporciona una inserción en la cultura de la seguridad e información por departamento de la UTIC?
		¿El personal cuenta con capacitaciones, certificaciones y experiencia en seguridad TI?
APO09	Gestionar los Acuerdos de Servicios	¿La unidad de TI cuenta con el portafolio de servicios de seguridad de la información?
APO11	Gestionar la Calidad	¿Existen normas, practicas, políticas y procedimientos de calidad con respecto a la seguridad de la información?

CONTINÚA ⟶

APO12	Gestionar el Riesgo	¿Existe información sobre identificación y políticas de seguridad en el departamento de TI y sus sedes?
APO13	Gestionar la Seguridad	¿Se comunicado a las autoridades de la institución sobre la necesidad de un plan de seguridad de la información para la ESPE matriz y sus sedes?
BAI09	Gestionar los activos	¿Se asignan responsabilidades de salvaguarda y uso a los empleados de la institución respecto a los activos de la ESPE matriz y sus sedes?
		¿Se realizan la revisión periódica de la red para detectar software autorizado?
DSS04	Gestionar la continuidad	¿Existe políticas, objetivos y alcances de continuidad del negocio?
DSS05	Gestionar los servicios de seguridad	¿Existen procedimientos de gestión relacionado con la protección de la información en la infraestructura tecnológica de la ESPE Matriz y sus sedes?

3.4. Análisis de Resultados

En la **Tabla 7,** se muestra el formato para análisis de información, luego de la entrevista realizada con la Ing. Magali Reascos MSc. Funcionaria de la UTIC, autorizada como apoyo en el levantamiento de información requerida para el diseño del Plan de seguridad de la información para la ESPE Sede Santo Domingo.

Tabla 7

Formato para análisis de información

Código	Descripción Proceso	Pregunta	Evidencia/Documentación	No es consciente de la Gestión	Es consciente de la Gestión	Existe un compromiso por resolver

Se inició implementación	La implementación está en Marcha	Tiene una solución implementada	Hay una solución sostenible	La solución está siendo optimizada	Documentación de Control	Observación

Durante la entrevista con la mencionada funcionaria, se define la fundamentación teórica para el análisis basado en la documentación de la UTIC que fue proporcionada para su análisis. En la **Tabla 8**, se indica el mencionado análisis sobre la documentación obtenida de la UTIC, versus los procesos seleccionados y

orientados a la seguridad de la información previa al diseño del Sistema de Gestión de Seguridad de la Información para la ESPE Sede Santo Domingo.

Tabla 8

Matriz de encuesta a la UTIC

Unidad de Tecnologías de Información y Comunicaciones

El presente instrumento permite obtener información necesaria para el análisis de procesos según COBIT 5 for Information Security, con el fin de realizar el análisis de Riesgos para el Diseño de un Sistema de Gestión de Información

Nro.	Código	Descripción Proceso	Pregunta	Evidencia/Documentación	No es consciente de la Gestión	Es consciente de la Gestión	Existe un compromiso por resolver	Se inició implementación	La implementación está en Marcha	Tiene una solución implementada	Observación
1	EDM01	Asegurar el establecimiento y Mantenimiento del Marco de Gobierno	¿El sistema de gobierno de la seguridad de la información está integrado con los procesos institucionales ?	Compromiso de Gobierno (Autoridades) con el desarrollo de proyecto PLAN DE SEGURIDAD DE LA INFORMACIÓN para la Institución		x					Toda la información proporcionada por la UTIC Sede Principal , se informa también que la Sede Principal será quien proporcione los
2	EDM03	Asegurar la Optimización del Riesgo	¿La gestión de riesgos asociados a la información forma parte de la gestión general de los riesgos corporativos de la	Plan de gestión de riesgos		x					

CONTINÚA ⟶

			institución?								lineamientos bases para los documentos disponibles a la Sede Sto. Domingo
3	EDM04	Asegurar la Optimización de los Recursos	¿Los recursos de seguridad de la información están alineados con los requerimientos de la institución?	Plan de desarrollo de la UTIC		x					
4	APO01	Gestionar el Marco de Gestión de TI		Plan de desarrollo de la UTIC		x					
5	APO02	Gestionar la Estrategia	¿Estrategias relacionadas con la seguridad de la información?	Plan estratégico institucional			x				
6	APO07	Gestionar los Recursos Humanos	¿Las capacidades y procesos de recursos humanos están alineados con los requisitos de la seguridad de información?	Plan de capacitación UTIC 2014			x				

CONTINÚA ⟶

			¿Número de empleados a los que se les proporciona una inserción en la cultura de la seguridad e información por departamento de la UTIC?	Nueva Estructura de procesos de la UTIC			X				
			¿El personal cuenta con capacitaciones, certificaciones y experiencia en seguridad TI?	Plan de capacitación UTIC 2014		X					
7	APO09	Gestionar los Acuerdos de Servicios	¿La unidad de TI cuenta con el portafolio de servicios de seguridad de la información?	Portafolio de acuerdos y niveles de servicio		X					
8	APO11	Gestionar la Calidad	¿Existen normas, practicas, políticas y procedimientos de calidad con respecto a la seguridad de la información?	Normas de calidad dirigidas a la seguridad de la información		X					

CONTINÚA ⟶

9	APO12	Gestionar el Riesgo	¿Existe información sobre identificación y políticas de seguridad en el departamento de TI y sus sedes?	Plan de contingencia		x					
10	APO13	Gestionar la Seguridad	¿Se ha comunicado a las autoridades de la institución sobre la necesidad de un plan de seguridad de la información para la ESPE matriz y sus sedes?	Nueva Estructura de procesos de la UTIC			x				
11	BAI09	Gestionar los activos	¿Se asignan responsabilidades de salvaguarda y uso a los empleados de la institución respecto a los activos de la ESPE matriz y sus sedes?	Inventario de activos, actas de entrega y recepción			x				
			¿Se realizan la revisión periódica de la				x				

CONTINÚA

			red para detectar software autorizado?								
12	DSS04	Gestionar la continuidad	¿Existe políticas, objetivos y alcances de continuidad del negocio?	Plan de Contingencia			x				
13	DSS05	Gestionar los servicios de seguridad	¿Existen procedimientos de gestión relacionado con la protección de la información en la infraestructura tecnológica de la ESPE Matriz y sus sedes?	Nueva Estructura de procesos de la UTIC			x				

En base al análisis de la tabla anterior y tomando en cuenta que la información proporcionada relaciona con los recursos existentes en la Sede Santo Domingo, seleccionamos los procesos que se encuentra en etapa de compromiso por resolver.

- **APO07** Gestionar los Recursos Humanos

  Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada.

- **APO12** Gestionar el Riesgo

  Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.

- **APO13** Gestionar la seguridad

  Definir, administrar y supervisar un sistema de gestión de seguridad de la información.

- **BAI09** Gestionar los activos

  Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, que se mantendrán en funcionamiento (acorde a los objetivos), que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para el negocio y que el software instalado cumple con los acuerdos de licencia.

- **DSS04** Gestionar la continuidad

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

- **DSS05** Gestionar los servicios de seguridad

  Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.

Arquitectura de seguridad de la información

Figura 12 Arquitectura de la Información
Fuente: (COBIT, 2015)

Los procesos descritos serán analizados en la gestión de riesgos y en base a esto se desarrollará el Plan de seguridad de la información.

CAPÍTULO IV

PROPUESTA DE PLAN DE SEGURIDAD INFORMATICA

Este capítulo se desarrolla en el ambiente de la ESPE sede Santo Domingo se basa en el levantamiento y análisis de la información realizada a la Institución, de acuerdo a la selección de procesos de COBIT 5 y aplicando estándares de gestión de seguridad y análisis de riesgos. El **Anexo 8**, muestra el desarrollo del Plan de seguridad.

4.1. Esquema del Plan de Seguridad

El presente plan se ha desarrollado siguiendo algunas de las especificaciones de la Normas ISO 27002 y 27003, para control y diseño de un Sistema de Gestión de la Seguridad.

- El primer paso es definir un equipo de trabajo, para el caso se denominará "Comité de Seguridad de la Información", este grupo de trabajo especificará responsabilidades y toma de decisiones en el desarrollo del proyecto y trabajará en conjunto con la gerencia para las debidas autorizaciones.

- Establecidas las responsabilidades y las autorizaciones respectivas se definirá un alcance del Plan de Seguridad de la Información, de la misma manera es establece limitaciones en este proyecto ya que no se llegará a la implementación.

- Continuando y en base a los procesos seleccionados de COBIT 5, se clasifica los activos de la ESPE Sede Santo Domingo y se relaciona con la seguridad de la información.

- Clasificados los activos se identifica amenazas, vulnerabilidades y riesgos que puedan afectar la seguridad de los activos mencionados. Luego se evalúa los

riesgos en términos de medio, bajo y alto dependiendo de la impacto y la probabilidad.

- Identificados los riesgos, ingresaran a un tratamiento para realizar controles y su madurez de aplicación, también se definirá en políticas para proteger los activos de la ESPE Sede Santo Domingo.

- Posterior al desarrollo del Plan, el Comité de Seguridad establecerá como y cuando realizar la implementación siguiendo las especificaciones de la Norma ISO 27003.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- El desarrollo del presente proyecto ha aplicado varias metodologías orientadas al levantamiento de información, análisis de riesgos y diseño del Sistema de Gestión de Seguridad de la Información.

- Las metodologías desarrolladas en el proyecto se fundamentan en estándares nacionales e internacionales, como se ha descrito a lo largo de la documentación.

- Se indica que el desarrollo del proyecto ha permito identificar puntos críticos que se han convertido en amenazas y algunos en potenciales riesgos que pueden afectar la seguridad de la información de la ESPE y sus Sedes.

- Un adecuado manejo de la metodología de diseño del Plan de seguridad de la información, ayudara en el futuro en la aplicación del ciclo de Deming respecto a la continuidad de procesos, identificando posibles omisiones a la seguridad que se han presentado en el transcurso y avance de procesos tecnológicos de la institución.

- Los controles definidos dentro de una política bien estructurada permite mejorar los niveles de seguridad ya sea en su parte física, estructura, tecnológica y en su parte metódica documental, donde se podrán ir identificando amenazas y vulnerabilidades. Lo cual podrá ser tomado como tema de estudio Para identificar posibles mecanismos de solución y la aplicación de controles y políticas de seguridad dentro de la ESPE y sus Sedes.

- En la actualidad la UTIC se encuentra desarrollando proyectos que apoyaran una buena gestión de seguridad de la información aplicando estándares relacionados con el desarrollo del presente trabajo.

5.2. Recomendaciones

- Como parte del estudio realizado, se recomienda aplicar las metodologías desarrolladas la mejora continua y determinar procesos críticos que puedan a afectar la seguridad de la información crítica de la sede.

- De la misma manera aplicar los controles y políticas sugeridas en este proyecto que determinen la protección de la información y evitar contratiempos con las vulnerabilidades que están presentes en el desarrollo tecnológico de la institución.

- Utilice estándares relacionados con la seguridad de la información actualizada ya que la evolución tecnológica avanza a pasos agigantados y siempre existen modificaciones respecto a temas tecnológicos como seguridad de la información.

- La implementación de este documento permitirá reducir el riesgo actualmente encontrados en procesos de activos, recursos humanos y continuidad de servicios de seguridad. El cual podrá servir como ayuda para futuras mejoras continuas y su implementación.

5.3. Bibliografía

- AGUILERA LOPEZ Purificación , "Seguridad Informática". Editorial Index. Junio 2010.
- CALDERON HONOFRE Diana, ESTRELLA OCHOA MartíN y FLORES VILLAMARIN Manuel, " Implementación de Sistema de Gestión de Seguridad de la Información Aplicada al Área de Recursos Humanos de la Empresa Decevale S.A. Escuela Politécnica del Litoral. Guayaquil 2011
- INEN (2012), Gestión de la seguridad de la información, ISO/IEC 27000
- INEN (2012), Gestión de riesgos en seguridad de la información, ISO/IEC 27005
- INEN (2012), Implementación de la seguridad de la información, ISO/IEC 27003
- INEN (2012), Gestión del Riesgo – Principios y Directrices (ISO 31000:2009, IDT), primera edición 2014-07
- ISACA(2012), COBIT-5-Risk_res_Spa_1114
- ISACA(2012),COBIT-5-Information-Security_res_spa_1213
- ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN, "Guía para la implementación de un Sistema de Gestión de Seguridad de la Información con Normas ISO 27002. Diciembre 2014
- PEÑA IBARRA José Ángel, " Conferencia, Confiar en el Valor de los Sitemas de Información" México-Moterrey. Mayo 2012
- PINAL MORA Karla, "Apuntes de Metodología y Redacción". Publicaciones Cruz. México D.F. Enero del 2006
- SECRETARIA NACIONAL DE LA ADMINISTRACIÓN PÚBLICA (2011), Acuerdo 166 Esquema gubernamental de la seguridad de la información (EGSI)
- SECRETARIA NACIONAL DE LA ADMINISTRACIÓN PÚBLICA , 2013)
- SECRETARIA NACIONAL DE PLANIFICACIÓN Y DESARROLLO (2013-2017), Plan Nacional del Buen Vivir

- SISTEMAS DE GESTION DE SEGURIDAD INFORMATICA 27003. “Guía para la implementación de un Sistema de Gestión de Seguridad de la Información. Enero del 2014

Referencias web:

- http://Plan de Seguridad de la Información-iso27001.blogspot.com
- http://www.isaca.org/knowledge-center/academia/pages/information-security-using-cobit-5-for-information-security.aspx recuperado el cinco de mayo del 2015
- http://www.iso.org/iso/home/standards/iso31000.htm
- http://www.iso27000.es/doc_Plan de Seguridad de la Información_all.html
- http://www.tgnsystems.com/sistemas/seguridad-informatica/ Recuperado el cinco de febrero del 2015

Anexo 1 Organigrama estructural de la Universidad de las Fuerzas Armadas ESPE

Anexo 2 Estructura Organizacional ESPE sede Santo Domingo

Anexo 3 Plan estratégico ESPE

Anexo 4 Catálogo de servicios de TICs

Anexo 5 Activos de la ESPE Sede Santo Domingo

Anexo 6 Recurso Humano de la ESPE Sede Santo Domingo

Anexo 7 Matriz de investigación de campo

Anexo 8 Plan de Seguridad de la Información para la ESPE sede Santo Domingo