ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA TECNOLÓGICA

DIRECCIÓN DE POSGRADOS

TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGÍSTER EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

TEMA: PLAN DE SEGURIDAD INFORMÁTICA PARA LA ESPE SEDE LATACUNGA

AUTORES: AGUIRRE MARTINEZ, CRISTIAN FABIAN
CASTELLANOS CAMPOVERDE, YINSON PATRICIO

DIRECTOR: MSc. QUINTANA CIFUENTES, MARCO VINICIO

SANGOLQUÍ,

2015

Universidad de las fuerzas Armadas- ESPE
Vicerrectorado de Investigación y Vinculación con la colectividad
Unidad de gestión de postgrados
Maestría en Evaluación y Auditoría de Sistemas Tecnológicos
Promoción VII

Certificado

En mi calidad de Director del proyecto "Plan de Seguridad Informática para la Espe sede Latacunga", realizado por los Ing. Aguirre Martínez, Cristian Fabian y Ing. Castellanos Campoverde, Yinson Patricio, para optar por el título de Magister en Evaluación y auditoria de sistemas tecnológicos, **CERTIFICO,** que dicho proyecto ha sido dirigido y revisado periódicamente y cumple con las normas establecidas por la ESPE, en el reglamento de estudiantes de posgrados y considero que reúne los requisitos y los méritos suficientes para ser sometida a la presentación pública y evaluación por parte del tribulan examinador que se designe

Sangolquí, abril del 2015

Ing. QUINTANA CIFUENTES, MARCO VINICIO MSc.

DIRECTOR

Universidad de las Fuerzas Armadas- ESPE
Vicerrectorado de Investigación y Vinculación con la colectividad
Unidad de gestión de postgrados
Maestría en Evaluación y Auditoría de Sistemas Tecnológicos
Promoción VII

DECLARACIÓN

La Tesis de grado titulada: "Plan de seguridad Informática para la Espe sede Latacunga"

Ha sido desarrollada en base a una investigación, respetando derechos intelectuales de terceros, cuyas fuentes son citadas e incorporadas en la bibliografía, consecuentemente este trabajo es de nuestra autoría

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico de esta tesis

Sangolquí, Abril del 2015

Ing. Cristian Aguirre Martínez

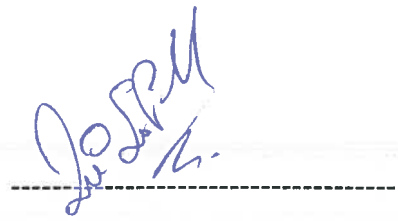
Ing. Yinson Castellanos Campoverde

Universidad de las Fuerzas Armadas- ESPE
Vicerrectorado de Investigación y Vinculación con la colectividad
Unidad de gestión de postgrados
Maestría en Evaluación y Auditoría de Sistemas Tecnológicos
Promoción VII

AUTORIZACIÓN

Nosotros: Aguirre Martínez Cristian Fabian y Castellanos Campoverde Yinson Patricio autorizamos a la Universidad de Fuerzas Armadas Espe, la publicación en la biblioteca virtual de la institución del trabajo "Plan de Seguridad Informática para la Espe sede Latacunga", cuyo contenido y criterios son de nuestra exclusiva responsabilidad y auditoría.

Sangolquí. Abril del 2015



Ing. Cristian Aguirre Martínez

Ing. Yinson Castellanos Campoverde

Agradecimiento

En primera instancia agradecer a Dios por darle la oportunidad de vivir y haber alcanzado tan anhelada meta

A todas aquellas personas que de forma directa e indirecta aportaron en el desarrollo de este proyecto; a mi familia ya que siempre están presentes apoyándome incondicionalmente.

A todos los profesores personas profesionales que impartieron sus conocimientos y experiencias a los largo de esta carrera universitaria.

A la ESPE sede Latacunga por brindarnos su colaboración y parte de su tiempo, en el auspicio de esta tesis, y por facilitarnos toda la información necesaria para el desarrollo del mismo.

A mi compañero y amigo no solo de tesis si no de mil y un batallas **Yinson "ratita" Castellanos,** ya que sin él tampoco hubiera sido factible este sueño ya que durante mucho tiempo hemos sabido saltar las dificultades no solo estudiantiles sino de la vida diaria y con él hemos alcanzado este gran triunfo profesional.

A todos mis amigos muchas gracias por estar conmigo en todo este tiempo donde hemos vivido momentos felices y tristes, gracias por ser mis amigos y recuerden que siempre están y los llevaré en mi corazón.

Verito, que te puedo decir, muchas gracias por todo la paciencia y tiempo en los cuales hemos compartido tantas cosas, hemos pasado tanto, ahora que estás conmigo en este día tan importante para mí. Solo quiero darte las gracias por todo el apoyo que me has dado para continuar y seguir con mi camino, gracias por estar conmigo y recuerda que eres muy importante para mí.

Gracias a todos.

Cristian Aguirre Martínez

Agradecimiento

A mí querido Padre mi Dios que con su Guía me ha permitido lograr este sueño.

Gracias a mi hijo Matteo que aunque he perdido algunas horas espero que mi Dios me de la vida para recompensarte, gracias por alegrarme con tus ocurrencias y por la motivación y el sentimiento que me regalas en tus tiernos abracitos.

Gracias A mi Madre y hermanos por toda la comprensión y el cariño dado.

A mi compañero, amigo y mi hermano: Cristian, gracias y mi sincera amistad.

Gracias también a toda mi familia y amigos en especial Cristian, Aman, Juan Sebastián, Zulema, Javier, Daniela y todas aquellas personas por compartir conmigo los buenos momentos y por ofrecerme su apoyo y consejos cuando se han presentado dificultades en mi camino.

Finalmente, pero no menos importante, un agradecimiento a todos mis maestros que como profesionales y seres humanos nos han orientado de la mejor forma posible con su apoyo constante, paciencia y atención demostrado a lo largo de nuestra carrera universitaria y de la presente tesis.

Quisiera agradecer a todas y cada una de las personas valiosas que han estado conmigo en la realización de esta tesis, no necesito nombrar porque tanto ellas como Yo sabemos que desde los más profundo de mí ser, les agradezco el haberme brindado todo el apoyo, colaboración y sobre todo cariño y amistad.

Yinson Patricio Castellanos.

Dedicatoria

Mi tesis la dedico con todo mi amor y cariño.

A ti DIOS que me diste la oportunidad de vivir y de regalarme una familia

Maravillosa.

Con mucho cariño principalmente a mis padres que me dieron la vida y han estado conmigo en todo momento.

Gracias por todo papá y mamá por la fortaleza diaria que me han brindado y por creer en mí, aunque hemos pasado momentos difíciles siempre han estado apoyándome y brindándome todo su amor, por todo esto les agradezco de todo corazón, el que estén conmigo a mi lado.

Los quiero con toda mi alma y este trabajo que me llevó tanto tiempo hacerlo es para ustedes y por ustedes, solamente les estoy devolviendo tan solo un poco lo que ustedes me han brindado

A mis hermanas Liz y Jade gracias por estar conmigo y apoyarme siempre, las quiero mucho.

Cristian Fabián Aguirre Martínez

"**He vivido una vida repleta de problemas, pero no son nada comparado con los problemas que tuvieron mis padres para lograr que mi vida empezase**

(bartrans hubbard)

Dedicatoria

A mí querido Padre mi Dios que ha sido mi Guía y Fortaleza en todos estos años, Por haberme permitido llegar hasta este punto por darme las fuerzas para lograr mis objetivos, con su infinita bondad y amor.

A mi Madre, por haberme apoyado en todo momento, por sus valores y su amor constate que me ha permitido ser una persona de bien.

A ti mi amor Matteo, hijo mío que aunque aún no sabes leer sé que un día los vas aprender y por eso te dedico esta tesis.

A mis familiares y a todos aquellos que participaron directa o indirectamente, en especial a ti Paola Patricia.

Nunca te rindas!!!

Yinson Patricio Castellanos

.

Índice general

Contenido

Índice de tablas

Índice de figuras

LISTADO DE ANEXOS

NOMENCLATURA UTILIZADA

CIS	Certification & Information Security Services
CMM	Modelo de Madurez de la Capacidad
COBIT	Marco de Referencia , Illinois, USA.
EGSI	Esquema Gubernamental de Seguridad de la Información
ESPE	Escuela Politecnica del Ejercito
INS001	Instrumento de trabajo
ITSFA	Instituto Tecnológico Superior de las Fuerzas Armadas
I.T.S.E	Instituto Tecnológico Superior del Ejército
ISACA	Information Systems Audit and Control Association
ISO	Organización Internacional de Normalización
ISSC	Comité de Seguridad de la Información
SGSI	Sistema de Seguridad de la Información
SNAP	Secretaria Nacional de la Administración Pública
MPSI	Metodología Plan de Seguridad Informática
NTE INEN-ISO/IEC	Siglas utilizadas en las normativas ecuatorianas
NTUST	La Universidad Nacional de Ciencia y Tecnología de Taiwán
PAM	Process Assessment Model
PDCA	Modelo del proceso Planear-Hacer-Chequear-Actuar

Resumen

El presente proyecto busca establecer un plan óptimo para la UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE SEDE LATACUNGA, para la aplicación del acuerdo No 166 expedido por la Secretaria Nacional de la Administración Pública SNAP sobre el Esquema Gubernamental de Seguridad de la información (EGSI), el mismo que está basado en la norma técnica ecuatoriana INEN ISO/IEC27002 dirigido para todas las entidades de la Administración Pública Central. El mencionado proyecto está basado en dicho acuerdo como fuente principal, adicionalmente maneja marcos de referencia tales como COBIT 5, COBIT PARA LA SEGURIDAD DE LA INFORMACIÓN, metodologías de gestión de riesgos tal como la norma internacional ISO/IEC27005, metodologías de gestión de activos como la que aplica la Superintendencia de Economía Popular y Solidaria, todo lo antes mencionado se utiliza con la finalidad de exteriorizar un plan de seguridad informática acorde a la realidad actual de la Espe sede Latacunga y que cumpla con estándares internacionales reconocidos y requerimientos actuales de los entidades reguladoras del país

PALABRAS CLAVE:

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN -EGSI

SECRETARIA NACIONAL DE LA ADMINISTRACIÓN PÚBLICA-SNAP

NORMAS INTERNACIONALES ISO 27000

COBIT 5

SEGURIDAD DE LA INFORMACION

Abstract

This project seeks to establish an optimal plan for the UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE SEDE LATACUNGA, for the implementation of the agreement No. 166 issued by the National Secretariat of Public Administration SNAP on Government Scheme Information Security (EGSI), the same which is based in the Ecuadorian INEN technical standard ISO / IEC27002 directed to all entities of the Central Public Administration. The said project is based on the agreement as a major source additionally handles frameworks such as COBIT 5 COBIT FOR INFORMATION SECURITY, methodologies for risk management as ISO/IEC27005, methodologies asset management as it applies the Superintendency Popular and Solidarity Economy, all the above is used in order to outsource IT security plan according to the current reality of Espe Latacunga complying with recognized international standards and current requirements the regulatory agencies of the country

KEYWORDS:

GOVERNMENT SCHEME INFORMATION SECURITY -EGSI

NATIONAL SECRETARY PUBLIC ADMINISTRATION -SNAP

INTERNATIONAL STANDARDS ISO 27000

COBIT 5

INFORMATION SECURITY

Capítulo I

1.1 Introducción

Actualmente la seguridad informática ha adquirido gran importancia en todas las organizaciones, ya sea del sector público o privado, a pesar de que el ambiente es cambiante y que la tecnología brinda herramientas para desarrollo en pro de un avance organizacional, también han surgido con mayor rapidez el desarrollo de aplicaciones que pretenden irrumpir la seguridad con diferentes fines que por lo general son maliciosos, situación que desemboca en la aparición de nuevas amenazas en los sistemas informáticos.

Esto ha llevado a que las organizaciones se preocupen por desarrollar estrategias que permitan combatir vulnerabilidades tanto internas como externas de la empresa y amenazas tecnológicas a las que podrían estar sometidas.

Por tal motivo se realizan varias estrategias para poder mitigar dichas amenazas tales como: Desarrollar documentos y directrices que orienten en el uso adecuado de estas tecnologías definiendo estratos de seguridad. Realizando un análisis de los potenciales riesgos, generación de políticas de seguridad informática que surgen como una herramienta para concienciar a los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos que permitan crear una cultura de seguridad dentro de la organización y además permiten a la organización desarrollarse y mantenerse en su sector de trabajo.

Es importante acotar que las políticas y procedimientos deben estar muy bien definidas para que puedan cubrir los aspectos más relevantes de seguridad dentro de la organización.

Al momento de implantar las estrategias se debe considerar que se tendrá que realizar un monitoreo constante y que es un proceso que nunca termina.

1.2 Antecedentes

La relación entre civiles y militares en Latacunga, se ha desenvuelto en sana armonía desde los inicios de la República, y sobra ver el aporte que hoy brindan al país con las

diferentes instituciones educativas al servicio de la ciudadanía. La fábrica de pólvora, en su mayoría se convirtió en hogar militar, así vemos como desde 1913 se establece el batallón constitución, de 1930 a 1933 la Escuela Aeronáutica y simultáneamente el batallón de ingenieros. De 1962 a 1984 se crea el CEMAI, Centro de Aprendizaje Industrial en donde capacitan al personal en ramas técnicas: Mecánica automotriz, oficios metalúrgicos, mecánica industrial y electricidad. El alto grado de perfección desarrollado permite que adicionalmente se ofrezca servicios a la industria del país. Se destaca los títulos de "Operario Calificado" conferidos a los estudiantes militares al término de los 12 meses de estudios. Para llegar a lo que hoy es la Universidad de las Fuerzas Armadas ESPE Extensión Latacunga, se tuvo que cumplir con ciertos requisitos académicos que satisfagan las metas y se crea en 1984 a 1987 el Instituto Tecnológico Superior de las Fuerzas Armadas (ITSFA), formando a tecnólogos militares y civiles por primera vez en 4 profesiones: Mecánica Automotriz, Control Automático, Telecomunicaciones y Electromecánica. Bajo la tutela total de la Fuerza Terrestre se crea el Instituto Tecnológico Superior del Ejército (I.T.S.E), manteniendo las 4 tecnologías e implementando un área de sistemas para obtener el título de Tecnólogo Analista de Sistemas.

En la actualidad, la ESPE Extensión Latacunga, es un establecimiento de Educación Superior, líder en la zona central del país, ofrece a la juventud carreras profesionales de excelente futuro laboral y económico, respaldadas por docentes de gran experiencia y por la Fuerza Terrestre del Ecuador. La ESPE Extensión Latacunga, ideal para estudiantes que buscan una carrera profesional en una urbe como lo es la Ciudad de Latacunga, que posee todos los servicios y con un gran valor agregado: su tranquilidad, seguridad y bajo costo de vida.

Después de toda esta basta historia se forma la ESPE extensión LATACUNGA cuya filosofía misión, visión principios que rige a esta universidad.

FILOSOFÍA

La Universidad de las Fuerzas Armadas ESPE Extensión Latacunga se encuentra dentro de un marco filosófico que le permite servir a la sociedad y entregar al ser humano el acceso al conocimiento al que tiene derecho, contribuyendo a la solución de sus problemas para alcanzar el desarrollo.

MISIÓN

Formar académicos, profesionales e investigadores de excelencia, creativos, humanistas, con capacidad de liderazgo, pensamiento crítico y alta conciencia ciudadana; generar, aplicar y difundir el conocimiento y proporcionar e implementar alternativas de solución a los problemas del país, acordes con el Plan Nacional de Desarrollo.

VISIÓN

Al 2016, líder en la gestión del conocimiento y 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.

1.3 Justificación e Importancia

Justificación teórica.- El uso de estándares de Tecnologías de Información para la realización de un Sistema de Gestión de Seguridad de la Información son fundamentales, no solo muestran las necesidades de la Gestión de TI sino que ayudan a encontrar los riesgos de los activos de información del negocio, estableciendo los controles necesarios.

La solución que se ha propuesto es presentar un Plan de Seguridad de Informática, para que el mismo sea implementado dentro de la Espe extensión Latacunga y así ser una de las universidades pioneras en dar cumplimiento al acuerdo Ministerial 166 que hace referencia a la "Implementación del Esquema Gubernamental de Seguridad de la Información EGSI".

Justificación Metodológica.- En este proyecto se trabajará con la familia NTE INEN ISO 27000, NTE INEN ISO 31000, COBIT 5 y COBIT PARA SEGURIDAD DE LA INFORMACIÓN como Marco de Referencia, lo que permitirá bosquejar un plan SGSI para la ESPE extensión LATACUNGA.

Justificación Práctica.- Con este proyecto se diseñará un plan de seguridad informática para la ESPE extensión Latacunga que permita conocer los riesgos a los que están expuestos sus activos de la información asumir, minimizar, transferir y controlar mediante una sistemática definida, documentada y conocida por todos, que se revise y mejore constantemente.

1.4 Planteamiento del Problema

En la actualidad vivimos en un entorno social donde uno de los principales activos para cualquier organización pública o privada es la información, sin importar el tamaño o giro de la organización. Si ocurriera algún incidente relacionado con la integridad, confidencialidad o disponibilidad a la información de cualquier organización púbica o privada, podrían generarse perjuicios importantes con respecto a otras instituciones del mismo sector e incluso podría dejarla expuesta al desprestigio, mala reputación etc.

En conjunto con el factor humano, la tecnología y el incremento de la dependencia de las organizaciones respecto a la misma para el manejo de su información y del aumento de interconectividad en todos los niveles, la información cada vez está más expuesta a una variedad más amplia y sofisticada de amenazas y vulnerabilidades. Estas amenazas pueden ser internas, externas, premeditadas, accidentales, etc. En la mayoría de los casos mencionados, se generan diversas pérdidas dentro de la organización, siendo las que afectan a la las más difíciles de contrarrestar.

Por lo antes expuesto, la Universidad de las Fuerzas Armadas ESPE extensión Latacunga, considera que las tecnologías de la información y comunicación son herramientas imprescindibles para el cumplimiento de la gestión institucional e inter institucional en tal virtud, debe cumplir con estándares de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información adoptar políticas estrategias, normas, procesos procedimientos tecnologías y medios necesarios para mantener la seguridad de la información que se genera y custodia en diferentes medios y formatos de la Universidad.

Adicionalmente que la ESPE al ser una institución educativa pública debe apegarse a ciertos lineamientos y disposiciones gubernamentales que sin ser obligatorios para la universidad son fundamentales para brindar un valor agregado a la comunidad universitaria y la comunidad en general, lineamientos como el "***Acuerdo 166*** de la Secretaria de Administración Pública SNAP **"** que obliga a las Instituciones públicas a utilizar las normas técnicas ecuatorianas NTE INEN-ISO/IEC 27000 para la gestión de seguridad de la información y la implementación del Esquema de Gestión de Seguridad de la Información (EGSI). Anexo B

Actualmente en la Universidad de las Fuerzas Armadas Espe en ninguna de sus extensiones cuentan con dicha implementación; Por tal motivo es básico apegarse a dicho acuerdo sobre todo como habíamos mencionado anteriormente brindar valor agregado a la comunidad universitaria y la comunidad en general.

1.5 Formulación del problema

1.5.1 Problema General

¿Cómo podría mitigar los riesgos asociados a los activos de la información dentro de la Espe extensión Latacunga y a su vez apegarse al Acuerdo 166 de la Secretaria de Administración Pública SNAP?

1.5.2 Problema Específicos

¿Cuáles son los niveles de efectividad, eficiencia, cumplimiento y confiabilidad de los servicios actuales; de acuerdo al grado de madurez de los procesos y al uso de los datos, sistemas de aplicaciones, tecnología, instalaciones y personal como recursos de TI?

¿Cómo se pueden identificar los activos de información de la ESPE extensión Latacunga?

¿Cómo se pueden categorizar los activos de la información según su nivel de criticidad, impacto?

¿Cómo se puede valorizar el nivel de impacto de los activos de información según su nivel de confiabilidad, integridad y disponibilidad?

¿Cuál es el nivel de apetito de riesgo de la Espe extensión Latacunga para sus activos de información?

1.6 Hipótesis (en tesis de investigación)

Para nuestro caso no aplica

1.7 Objetivo general

Realizar el Plan de Seguridad Informática aplicable para la Universidad de las Fuerzas Armadas ESPE extensión Latacunga, mediante la utilización del Marco de referencia COBIT 5, COBIT para la Seguridad de la Información y la normas técnicas ecuatorianas NTE INEN-ISO/IEC 27000 para la gestión de seguridad de la información.

1.8 Objetivos específicos

- Realizar el análisis de la situación actual de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga en base a la norma NTE INEN-ISO/ IEC 27000 en cuanto a la seguridad de información.
- Analizar y evaluar los riesgos a los que está expuesto los activos de información en la ESPE extensión Latacunga.
- Identificar el nivel de madurez de los dominios de la norma NTE INEN-ISO/ IEC 27002 (EGSI) en la Universidad de las Fueras Armadas ESPE extensión Latacunga.
- Presentar una metodología de clasificación de activos de la información apta para la implementación de un SGSI.
- Identificar los requerimientos existentes y faltantes exigidos por la norma internacional para la implementación de un SGSI
- Presentar el plan de Seguridad de Informática en base a los riesgos y el nivel de madurez identificados en los dominios de la norma NTE INEN-ISO/ IEC 27000.

Capítulo II.- Fundamentación teórica.

2.1. Marco teórico

2.1.1 Gestión de riesgos (ISO 31000)

Todas las actividades de una organización están sometidas de forma permanente a una serie de amenazas, lo cual las hace altamente vulnerables, comprometiendo su estabilidad. Accidentes operacionales, enfermedades, incendios u otras catástrofes naturales, son una muestra de este panorama, sin olvidar las amenazas propias de su negocio. (ISO 31500:2009)

2.1.1.1 ESTRUCTURA DE LA NORMA (ISO 31000.)

Estándar Internacional desarrollado por la IOS (International Organization for Standardization) propone unas pautas genéricas sobre cómo gestionar los riesgos de forma sistemática y transparente.

El diseño y la implantación de la gestión de riesgos dependerán de las diversas necesidades de cada organización, de sus objetivos concretos, contexto, estructura, operaciones, procesos operativos, proyectos, servicios. El enfoque está estructurado en tres elementos claves para una efectiva gestión de riesgos:

- Los principios para la gestión de riesgos.
- La estructura de soporte.
- El proceso de gestión de riesgos.

2.1.1.2 ESTRUCTURA DE LA NORMA (ISO 31000.)

Para una mayor eficacia, la gestión del riesgo en una organización debe tener en cuenta los siguientes principios:

Crea valor. Contribuye a la consecución de objetivos así como la mejora de aspectos tales como la seguridad y salud laboral, cumplimiento legal y normativo, protección ambiental, etc.

Está integrada en los procesos de una organización. No debe ser entendida como una actividad aislada sino como parte de las actividades y procesos principales de una organización.

Forma parte de la toma de decisiones. La gestión del riesgo ayuda a la toma de decisiones evaluando la información sobre las distintas alternativas.

Trata explícitamente la incertidumbre. La gestión del riesgo trata aquellos aspectos de la toma de decisiones que son inciertos, la naturaleza de esa incertidumbre y como puede tratarse.

Es sistemática, estructurada y adecuada. Contribuye a la eficiencia y, consecuentemente, a la obtención de resultados fiables.

Está basada en la mejor información disponible. Los inputs del proceso de gestión del riesgo están basados en fuentes de información como la experiencia, la observación, las previsiones y la opinión de expertos.

Está hecha a medida. La gestión del riesgo está alineada con el contexto externo e interno de la organización y con su perfil de riesgo.

Tiene en cuenta factores humanos y culturales. Reconoce la capacidad, percepción e intenciones de la gente, tanto externa como interna, que puede facilitar o dificultar la consecución de los objetivos de la organización.

Es transparente e inclusiva. La apropiada y oportuna participación de los grupos de interés (stakeholders) y, en particular, de los responsables a todos los niveles, asegura que la gestión del riesgo permanece relevante y actualizada.

Es dinámica, iterativa y sensible al cambio. La organización debe velar para que la gestión del riesgo detecte y responda a los cambios de la empresa.

Facilita la mejora continua de la organización. Las organizaciones deberían desarrollar e implementar estrategias para mejorar continuamente, tanto en la gestión del riesgo como en cualquier otro aspecto de la organización. (ISO 31500:2009)

La relación entre los principios de gestión, la estructura de soporte, así como el proceso de gestión del riesgo desarrollado en la norma se resume en la figura 1:

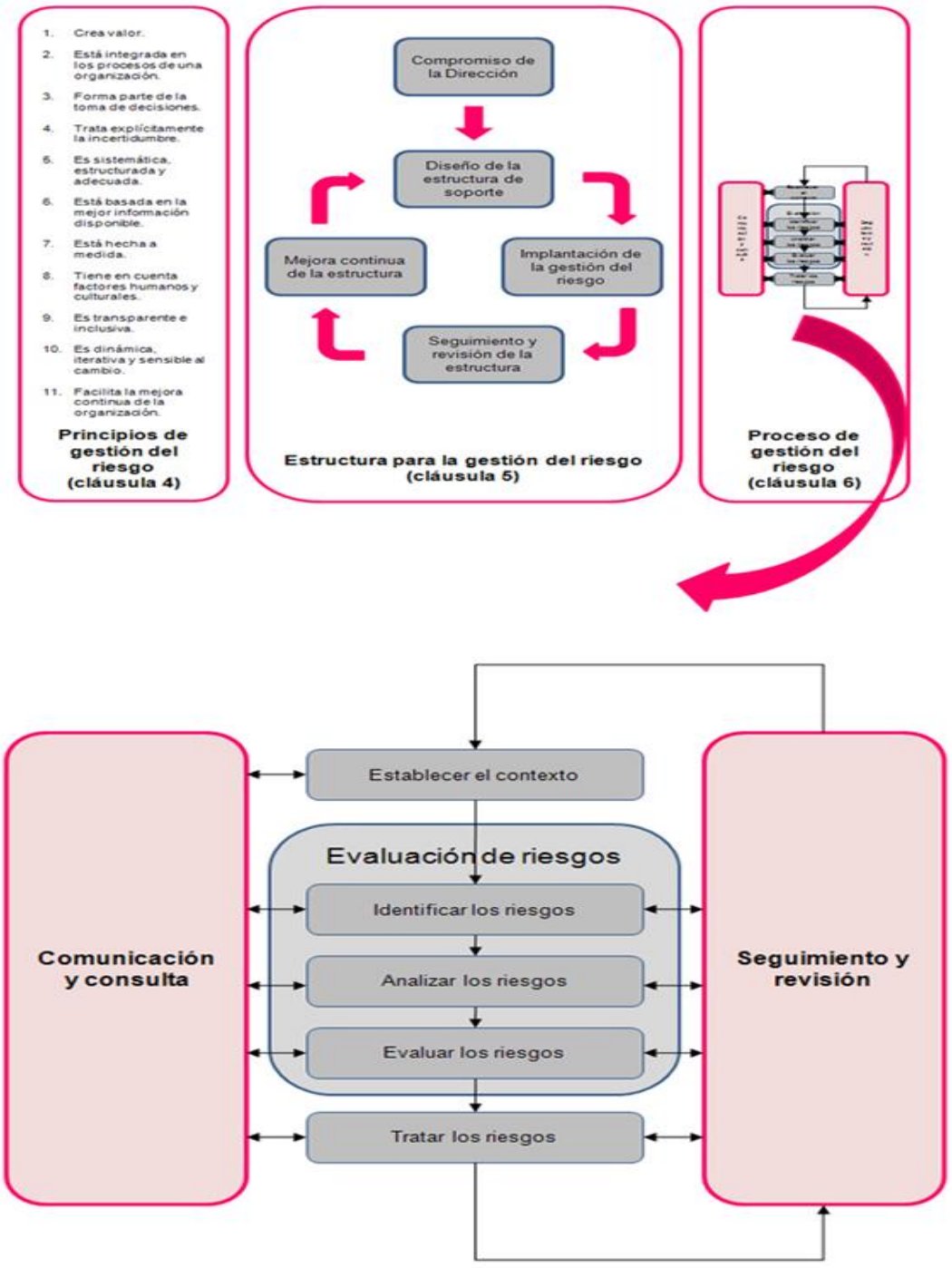


Figura 1 Relación entre los principios, estructura de soporte y proceso de gestión de riesgo

Fuente: Gestión de riesgos ISO 31000

2.1.2 Sistema de Gestión de Seguridad de la Información (ISO 27000)

Este Estándar Internacional ha sido preparado para proporcionar un modelo para establecer, Implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).(ISO 27000:2005)

2.1.2.1 Enfoque del Proceso

Este Estándar Internacional promueve la adopción de un enfoque del proceso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización.

Un enfoque del proceso para la gestión de la seguridad de la información presentado en este Estándar Internacional fomenta que sus usuarios enfaticen la importancia de:

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

Este Estándar Internacional adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI como muestra la figura 2 y se describe en la tabla 1

Figura 2 Adopción del modelo PDCA (SGSI)

Fuente: ISO 27000

Tabla 1

Modelo PDCA aplicado a los procesos SGSI	
Planear (establecer el SGSI)	Establecer política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.
Hacer (implementar y operar el SGSI)	Implementar y operar la política, controles, procesos y procedimientos SGSI.
Chequear (monitorear y revisar el SGSI)	Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión.
Actuar (mantener y mejorar el SGSI)	Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoria interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.

Fuente: (Instituto Ecuatoriano de Normalización, 27002:2010)

2.1.2.2. Dominios objetivos de control de la ISO 27000

A continuación en la figura 3 se muestra los dominios de control del SGSI

Figura 3 Dominios de Control de un SGSI

Fuente: ISO 27000

2.1.3 ISO/IEC 27002:2005

Este estándar internacional "establece los lineamiento y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de información en una organización" (ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management. EEUU.) Nos da marcos de control necesarios para la implementación de un SGSI. Contiene once cláusulas de control de seguridad y cada una de estas cláusulas contiene un número de categorías de seguridad principales como se muestra en la figura 4. A su vez, cada una de estas categorías de seguridad tiene un objetivo de control que es lo que se quiere lograr y los controles que se pueden aplicar para lograr dicho objetivo.

Las once cláusulas mencionadas previamente son:

- Política de Seguridad
- Organización de la Seguridad de Información
- Gestión de Activos
- Seguridad de Recursos Humanos
- Seguridad Física y Ambiental
- Gestión de Comunicaciones y Operaciones
- Control de acceso
- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
- Gestión de Incidentes de Seguridad de Información
- Gestión de la Continuidad Comercial
- Conformidad

Figura 4: Dominios y controles ISO27002

Fuente: ISO 27002

2.1.4 ISO/IEC 27003:2010

Este estándar internacional es nuestra guía para la implementación de un SGSI dentro de la institución educativa. Este documento explica dicha implementación enfocándose en la iniciación, planeamiento y la definición del proyecto: describe los 17 procesos desde la obtención de la aprobación de la alta gerencia para implementar el SGSI hasta la conclusión final del plan de proyecto a diferencia del ISO 27001, este documento nos da recomendaciones y buenas prácticas, mas no indica requerimientos ni obligaciones: es para el uso en conjunto con la norma ISO 27001 y no para modificar o reducir los requerimientos especificados en dicha norma. El proceso del planeamiento de la implementación de un SGSI contienen cinco fases y cada fase es representada por una clausula como se muestra en la figura 5. Todas estas cláusulas tienen una estructura similar: cada clausula tiene uno o varios objetivos y una o varias actividades necesarias para lograr dichos objetivos. (ISO/IEC 27003:2010)

Las cinco fases son:

- Obtención de la aprobación de la alta gerencia para iniciar el proyecto de SGSI.
- Definición del alcance las políticas del SGSI.

- Conducir el análisis de la organización.
- Conducir un análisis de riesgos y un plan de tratamiento de riesgos.
- Diseñar el SGSI.

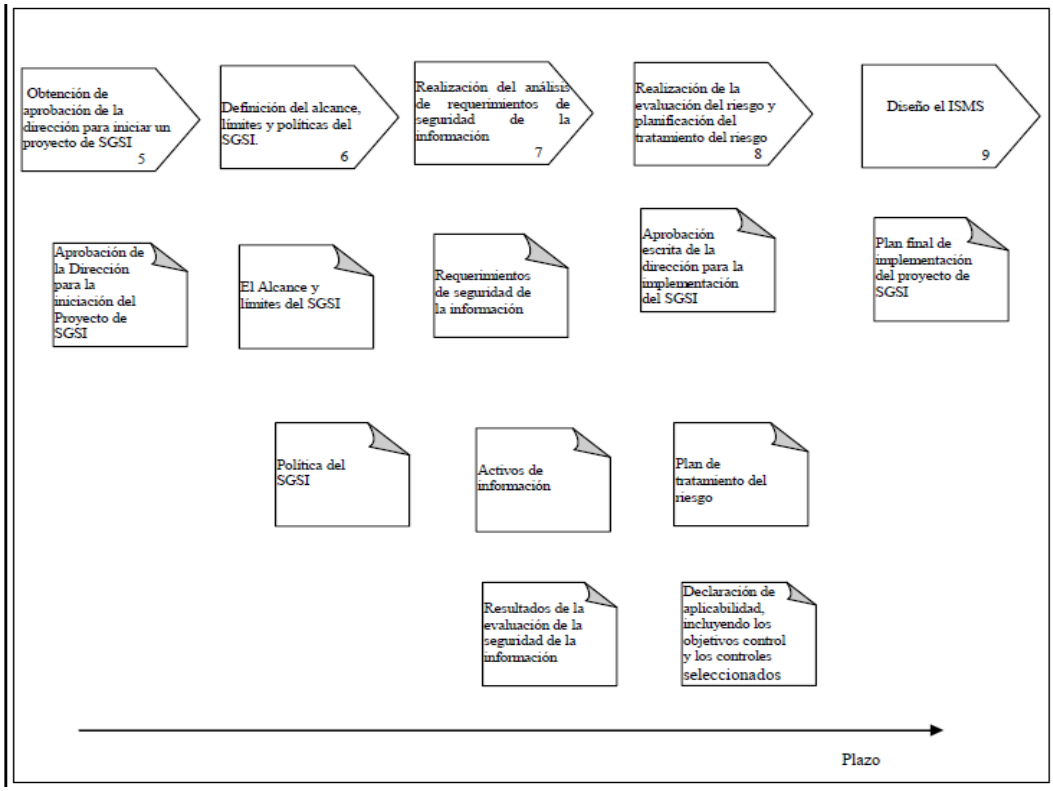


Figura 5: fases SGSI

Fuente: ISO 27003:2005

2.1.5 ISO/IEC 27005:2008

Este estándar internacional nos brinda directrices para la gestión de riesgos de la seguridad de información, dando soporte particularmente a los requerimientos de un SGSI, de acuerdo con la norma ISO/IEC 27001. Sin embargo, esta norma no es de por sí una metodología para la gestión de riesgos, (ISO/IEC 27005:2008) aunque lo puede llegar a ser, según el alcance que el SGSI tenga o el contexto de la gestión de riesgos donde se aplique dicha norma. La estructura de la norma se descompone en 12 cláusulas, las cuales son:

- Cláusula 1: Alcance.
- Cláusula 2: Referencias normativas.

- Cláusula 3: Términos y definiciones.
- Cláusula 4: Estructura de la norma.
- Cláusula 5: Background.
- Cláusula 6: Resumen del proceso de la gestión de los riesgos de la seguridad de información.
- Cláusula7: Establecimiento del contexto.
- Cláusula 8: Risk Assessment.
- Cláusula 9: Risk Treatment.
- Cláusula 10: Risk Acceptance.
- Cláusula 11: Risk Communication
- Cláusula 12: Risk Monitoring.

La siguiente figura 6 ilustra que el proceso de la gestión de los riesgos de la seguridad de información puede ser iterativo para la evaluación de los riesgos y/o las actividades que envuelvan el tratamiento de los mismos. Este enfoque iterativo que propone la norma nos puede incrementar la profundidad y el detalle en la evaluación de los riesgos en cada iteración, así como un balance adecuado entre minimizar el tiempo y el esfuerzo en identificar controles adecuados y asegurar que los riesgos con alto impacto y/o posibilidad de ocurrencia estén debidamente monitoreados.

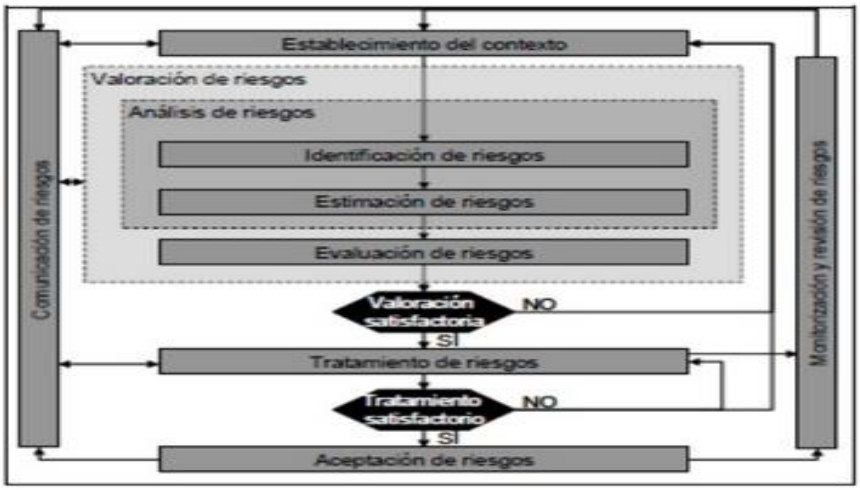


Figura 6 Proceso de Gestión de riesgo para la Seguridad de la Información

Fuente: ISO 27005:2008

2.1.6 COBIT 5

COBIT 5 provee un marco de referencia para asistir a las empresas y organizaciones a que alcancen sus objetivos de negocio y entregar valor a través de un gobierno eficiente y una buena gestión de sus tecnologías de información. Con esto las empresas se aseguran de que están entregando valor y obteniendo confianza de la información y sus sistemas, afrontando los retos a los que se enfrentan en la actualidad. COBIT 5 tiene una perspectiva de negocio, no solo de TI. Este es el principal cambio frente a sus anteriores ediciones. Este framework puede ser usado por cualquier usuario de cualquier área de la empresa. Asimismo, puede ser tomado como referencia por cualquier stakeholder que tenga la organización. COBIT 5 está basado en cinco principios clave como se ilustra en la figura 7 y son:

Principio 1: Satisfacer las necesidades de los Stakeholders Las empresas existen para crear valor a sus Stakeholders. Esto se logra manteniendo un balance entre los objetivos de negocio, la optimización de los riesgos que puedan existir y el uso de recursos dentro de la organización. COBIT 5 provee todos los procesos requeridos y otros habilitadores para dar soporte a la creación de valor a través del uso de las tecnologías de información.

Principio 2: Cubrir la organización de principio a fin: COBIT 5 cubre todas las funciones y procesos dentro de la empresa. No solo se enfoca en la parte de TI, sino que trata a la información y a la tecnología como activos que necesitan ser tratados como otro cualquier activo dentro de la empresa.

Principio 3: Aplicar un único marco de trabajo integrado, hay varios estándares relacionados a las tecnologías de información y sus buenas prácticas. COBIT 5 se alinea con estos estándares y frameworks en un alto nivel y puede ser utilizado como un marco contenedor de todos estos.

Principio 4: Aproximación holística COBIT 5 define un conjunto de habilitadores para dar soporte a la implementación de un gobierno y una gestión comprensiva de TI. Estos habilitadores son definidos como cualquier cosa que pueda ayudar a alcanzar los objetivos de negocio de la organización. Más adelante se definirán los siete habilitadores que propone COBIT 5.

Principio 5: Separar "Gestión" de "Gobierno" COBIT 5 hace una clara distinción entre gobierno y gestión. Estas dos disciplinas tienen diferentes tipos de actividades, requieren distintas estructuras organizacionales y sirven para diferentes propósitos.

Figura 7: Principios de COBIT

Fuente: COBIT 5: ISACA

Así mismo, COBIT 5 nos define siete categorías de habilitadores que se muestra en la figura 8 que son:

Principios, políticas y marcos de trabajo son el medio para trasladar el comportamiento deseado a una guía práctica para la conducir la gestión del día a día.

Procesos constituyen un conjunto organizado de prácticas y actividades para producir los outputs respectivos para alcanzar las metas de TI

Estructura organizacional son las entidades que toman las decisiones críticas en la organización.

Cultura, ética y comportamiento de los individuos y de la empresa son muy frecuentemente sobrestimados como un factor de éxito de los objetivos de gobierno y gestión establecidos.

La Información está en todos los ámbitos de la organización. Es requerida para mantener a la organización andando y bien gestionada. Asimismo, en un nivel operacional, la información es pieza clave.

Servicios, infraestructura y aplicaciones dan soporte a los procesos y servicios de TI.

Personas, habilidades y competencias están conectadas a las personas. Son requeridas para tomar decisiones correctas y tomar acciones correctivas adecuadas.

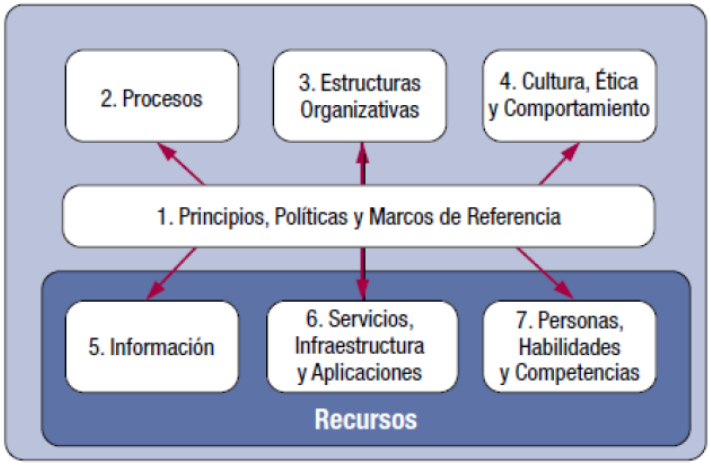


Figura 8: Catalizadores de COBIT

Fuente: COBIT 5: ISACA

Finalmente, COBIT 5 nos introduce una cascada de objetivos la cual permite definir las prioridades para la implementación, mejora y aseguramiento del gobierno de TI basada en los objetivos de negocio de la organización y el posible riesgo al que este expuesta. Principalmente, como se muestra la figura 9.

La cascada de objetivos:

- Define los objetivos más relevantes y tangibles en varios niveles de responsabilidad.
- Permite extraer la información más relevante del conocimiento base de COBIT 5 para su inclusión en proyectos específicos.
- Identifica y comunica claramente como los habilitadores son importantes para alcanzar los objetivos organizacionales.

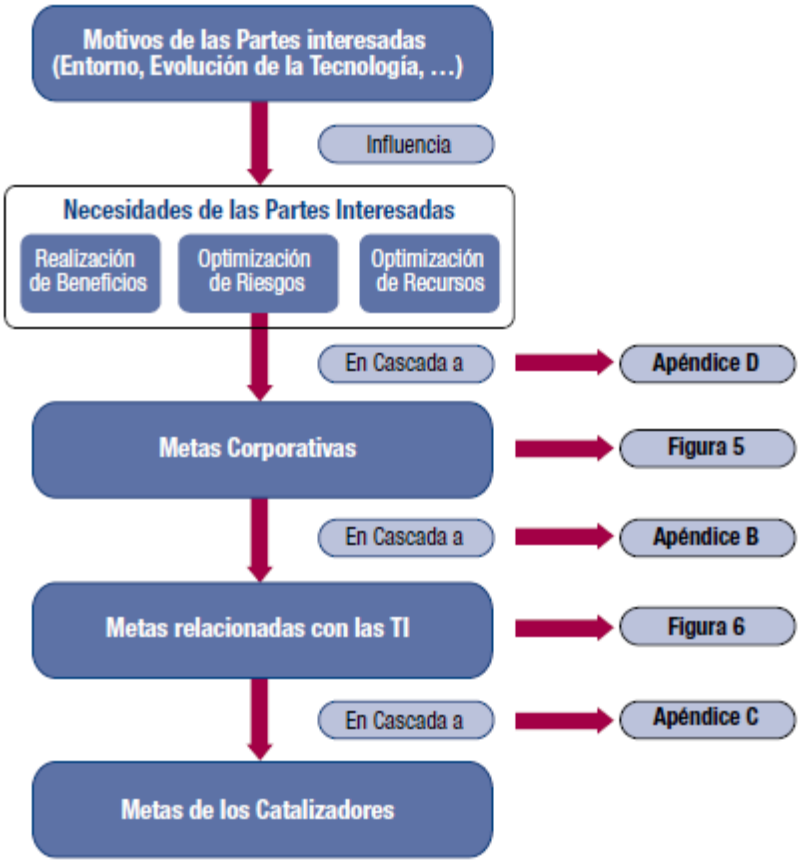


Figura 9 Modelo cascada objetivos de COBIT

Fuente: COBIT 5: ISACA

2.1.7 Plan De Seguridad De La Información según COBIT 5

EL plan de seguridad de la información según COBIT 5 para la seguridad de la información debe cumplir las siguientes metas:

El plan de la seguridad de la información debe ser preciso, exhaustivo y completo, y contener acciones realistas y correctas basadas en la estrategia de la seguridad de la información. Además, debe estar alineado con la arquitectura empresarial y con la situación concreta de la empresa, y en línea con el apetito de riesgo global (p. ej., hay suficiente dinero en el presupuesto). El plan de seguridad debe estar disponible a tiempo y ser accesible sólo para aquellos que lo necesiten (p. ej., partes interesadas).

Estos objetivos pueden ser medidos por métricas incluyendo:

- Número de acciones que no pueden ser implementadas o ejecutadas.

- Número de discrepancias entre el plan de seguridad de la información y la arquitectura empresarial.
- Porcentaje de partes interesadas sin acceso al plan.
- Número de violaciones en contra del plan.

2.1.7.1 Ciclo de Vida

El plan de la seguridad de la información es creado y después mantenido de manera regular según lo requiera el ISSC, en sincronía con el ciclo presupuestario.

El plan de seguridad de la información define todas las inversiones necesarias para llevar a cabo la estrategia de seguridad de la información y su arquitectura. El plan de seguridad de la información está definido en términos de todos los facilitadores:

- Procesos que necesitan ser definidos, implementados o reforzados.
- Estructuras organizativas que necesitan ser creadas o reforzadas.
- Flujos de información relacionados con la gestión de la seguridad de la información que necesitan ser implementados.
- Políticas y procedimientos que necesitan ser definidos y puestos en práctica.
- Cultura de seguridad de la información que necesita ser ajustada o mantenida.
- Habilidades y comportamientos que necesitan ser desarrollados o cambiados.
- Capacidades que necesitan ser adquiridas, como por ejemplo, tecnología para seguridad de la información, aplicaciones y servicios específicos de seguridad de la información.

2.1.7.2 Requerimientos de Seguridad de la Información

Los requerimientos de la seguridad de información deben ser completos, realistas y alineados con el negocio y con los requisitos legales. Además, los requisitos deben estar disponibles a tiempo y ser accesibles solamente para las partes interesadas (es decir, para aquellos que necesiten acceder).

Ejemplos de métricas para esta área son:

- Número de proyectos con requerimientos de seguridad revisados por la función de seguridad de la información.
- Número de requerimientos que no se cumplen.

- Número de requerimientos entregados en los proyectos organizativos o que están ausentes en proyectos ya desplegados.
- Número de aceptaciones firmadas por los usuarios finales, manifestando recepción y reconocimiento de los requisitos de seguridad más recientes.

2.1.7.3 Ciclo de Vida de los requerimientos

Los requerimientos de la seguridad de la información se definen en varios puntos de activación:

- Al comienzo de nuevos proyectos de negocio, como parte del conjunto de los requerimientos de negocio y funcionales la seguridad de la información es un requerimiento de negocio; los requerimientos de la seguridad de la información son seguidos a lo largo de todo el ciclo de vida de la iniciativa.
- Durante la negociación del contrato/acuerdos con terceras partes.
- Cuando se están investigando adquisiciones/fusiones de compañías (establecer requerimientos para la gestión de las amenazas de las marcas).

2.2. Antecedentes del estado del arte

En la actualidad ninguna institución educativa ni universidad está certificada en la norma ISO 27001 dentro del contexto educativo ecuatoriano según una investigación del mercado educativo que se realizó para la presente tesis. Sin embargo, en este punto se mencionarán las universidades e instituciones educativas internacionales más importantes que sí han obtenido la certificación ISO/IEC 27001 hasta la fecha:

2.2.1 Universidad Nacional de Ciencia y Tecnología de Taiwán

La Universidad Nacional de Ciencia y Tecnología de Taiwán, NTUST por sus siglas en inglés, se creó el primero de Agosto en 1974 como el primer instituto educativo del tipo tecnológico dentro de Taiwán. Actualmente cuentan con 4953 alumnos, 48337 graduados y 336 profesores a tiempo completo. Al alcanzar el estado de “Universidad” en 1997, la escuela se reorganizo en 5 facultades: ingeniería, ingeniería eléctrica y de sistemas, gestión, diseño y arte y ciencias sociales. Entre los departamentos se incluyen

los programas de ingeniería mecánica, ingeniería civil, ingeniería química, ingeniería informática, etc. En conjunto con las carreras de ingeniería, el departamento de humanidades ofrece programas de humanidades y ciencias sociales, así como el departamento de educación ofrece programas a para futuros profesores. Todos los departamentos juntos forman 21 programas que la Universidad Nacional de Ciencia y Tecnología de Taiwán ofrece. Finalmente aceptan estudiantes para programas de pregrado, maestrías y doctorado. En Abril del 2011, el SGS (Société Générale de Surveillance) en Taiwán, una compañía certificadora reconocida a nivel mundial, le entrego la certificación de la ISO 27001 a la universidad NTUST, mencionando que la calidad de la gestión de la seguridad de información de la NTUST alcanza los más altos estándares de calidad e integridad hoy en día a nivel mundial. La certificación mencionada cubre los procesos de mantenimiento y operación del centro de cómputo de NTUST y el desarrollo, operación y mantenimiento de todos los sistemas de información de los alumnos. Las compañías de certificación visitaban el campus de vez en cuando para una serie de inspecciones de documentación e in-situ. Así mismo, condujeron una serie de entrevistas con los administradores de los sistemas para verificar si cada módulo de los sistemas de información está asegurado adecuadamente. Finalmente, luego de 10 meses de las fases de planeamiento e implementación que el estándar ISO 27001 demanda que se realice, en conjunto con las inspecciones de la entidad certificadora, la NTUST logro dicha certificación. (Aliaga Flores, Luis. 2013. Diseño de un sistema de gestión de Seguridad para un instituto Tesis de maestría. Pontifica Universidad Católica de Perú).

2.2.2 Universidad Libre de Bozen/Bolzano

La Universidad Libre de Bozen/Bolzano es fundada el 31 de Octubre de 1997 en Italia como una institución educativa orientada a la internalización y pluralidad de lenguas. Dicha universidad, promueve el libre intercambio de ideas y conocimiento científico, vinculándose con la tradición europea de humanidades y el respeto por los principios democráticos. Actualmente cuenta con 5 facultades: la facultad de ciencias de la computación, la escuela de administración y economía, la facultad de educación, la facultad de diseño y de arte y finalmente, la facultad de ciencias y tecnología. Cabe resaltar que tiene 3 campus y enseñan en 4 distintos lenguajes: inglés, alemán, italiano y latín.

Finalmente, cuentan con 3364 estudiantes actualmente, los cuales el 18% son de origen internacional, lo que demuestra que alientan el intercambio cultural estudiantil.

El 12 de Enero del 2007 la Universidad Libre de Bozen/Bolzano recibió la certificación ISO 27001. Esta universidad es la primera organización científica a nivel mundial en obtener en la certificación en el ISO 27001. Por una semana, dicha universidad estuvo auditada por dos entidades certificadoras: ÖQS (Austrian Association forcertification of quality and management systems) y CIS (Certification & Information Security Services). Ellas estuvieron auditando y verificando que todo el proceso de transferencia del conocimiento de la información (desde la infraestructura de bases de datos hasta el código de conducta dentro de la universidad) en la institución estuviera lo suficientemente segura, como lo exige la norma que se maneje. En conjunto con dicha certificación, el departamento de informática y comunicaciones, encargada de gestionar la red informática de la universidad y el desarrollo del software interno educativo, obtuvo también la certificación ISO 9001:2000 por la calidad de sus sistemas de gestión, siendo el primer y único departamento en la Universidad Libre de Bozen/Bolzano que maneja dichas certificaciones. (Aliaga Flores, Luis. 2013. Diseño de un sistema de gestión de Seguridad para un instituto Tesis de maestría. Pontifica Universidad Católica de Perú).

2.3. Marco conceptual

A continuación se muestra una serie de conceptos propios para elaborar un plan de Seguridad de la Información o un Sistema de Seguridad de la Información SGSI.

Información

Es un activo esencial para el negocio de una organización. Puede existir de muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. (ISO/IEC 27001:2005).

Seguridad de la Información

Asegura que dentro de la empresa, la información está protegida contra su divulgación a usuarios no autorizados (confidencialidad), modificación inadecuada (integridad) y su falta de acceso cuando se la necesita (disponibilidad). COBIT para la Seguridad de la Información (COBIT 5, ISACA)

Gobierno

El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas. (COBIT 5, Isaca)

Gestión

La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

Seguridad Informática.-

Conjunto de metodologías, políticas, técnicas, estrategias y procedimientos orientados a la protección del sistema informático, preservando la integridad, disponibilidad y confidencialidad de la información procesada en un sistema de informático (COBIT 5, Isaca).

Activos de Información.-

El activo de información es cualquier elemento que contiene información y represente valor para el soporte institucional. Todos los activos de información deberán estar claramente identificados dentro de un inventario; y pueden ser:

Activo en relación con la seguridad de la información.- Se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

Activos de información en medios físicos o electrónicos.- Incluye bases de datos, documentación, manuales, software, hardware, contratos, equipo de comunicaciones, servicios informáticos y de comunicaciones, utilidades generales como por ejemplo: calefacción, iluminación, energía y aire acondicionado y las personas, que son quienes generan, transmiten y destruyen información.

Los activos de información se pueden clasificar en: activos de la información tecnológicos, activos de información físicos, activos de información intangibles, activos de entorno.

Disponibilidad.-

Aquella autorización a los servidores públicos para acceder a la información y a los recursos relacionados con ella (ISO/IEC 27001:2005).

Integridad.-

Permite salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento, a través de las medidas de validación que permitirán detectar las modificaciones inapropiadas, la eliminación o la adulteración de los activos de información (ISO/IEC 27001:2005).

Confidencialidad.-

Garantizar que la información sea accesible solo a aquellas personas autorizadas a tener acceso a ella. Los activos de información deben estar debidamente protegidos para evitar la divulgación de la información almacenada, procesada, transmitida o recibida a individuos, entidades o procesos no autorizados (ISO/IEC 27001:2005).

Autenticidad.-

Define cual información es legítima, en caso de que sea interceptada, eventualmente podría ser copiada de su formato original y a pesar de que la información sea idéntica, no sea legítima pues no pertenece al autor original de la misma.

No repudiación.-

Improcedencia de la negativa en un proceso de control o seguimiento o transacción desde su inicio, pudiendo reconocerse de dónde provino, quien lo ejecutó y si estaba autorizado para ejecutarla (ISO/IEC 27001:2005).

Amenaza.-

Es el evento que puede provocar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos, que son de dos tipos:

Vulnerabilidad.-

Es un fallo de seguridad, que provoca que los sistemas informáticos funcionen de manera diferente para lo que estaban pensados, afectando a la seguridad de los mismos, pudiendo llegar a provocar entre otras cosas la pérdida y robo de información sensible. La vulnerabilidad de un activo es la potencialidad o posibilidad de ocurrencia de la materialización de una Amenaza sobre dicho Activo (ISO/IEC 27005:2008).

Impacto.-

Es la consecuencia materializada de una amenaza sobre el activo (ISO/IEC 27005:2008).

Riesgo.-

Posibilidad de la materialización de una amenaza en un activo, dominio o en toda la organización y que se aproveche una vulnerabilidad y dañe un activo de información (ISO/IEC 27005:2008).

Salvaguarda.-

Es la acción que reduce el riesgo (servicio de salvaguarda) o el procedimiento o dispositivo físico o lógico que reduce el riesgo (mecanismo de salvaguarda) (ISO/IEC 27005:2008).

Dueños de los Activos de Información.-

Son los servidores públicos que tienen un nivel jerárquico dentro de la Institución el cual les habilita para determinar el tipo de información que maneja cada uno de los procesos en los que está involucrada la misma, así como los niveles de riesgo a los cuales está expuesta, de forma que establezca los niveles de confidencialidad aplicables, los responsables de solicitar los niveles de seguridad que deben destinarse a la información, para mantener la confidencialidad, integridad y disponibilidad de la información (ISO/IEC 27001:2005).

Información sensible.-

Es el calificativo que recibe la información de tipo personal privada e un individuo (datos de tipo personal, contraseñas de correo electrónico u otros), usados para distinguir los datos privados relacionados con internet o la informática, sobre todo contraseñas de correo electrónico, conexión a internet, IP privada, sesiones del computador, Etc. (ISO/IEC 27001:2005).

Capítulo III.- Memoria Técnica Metodológica

3.1 Metodología de Investigación

Método de investigación, técnicas e instrumentos de recolección y procesamiento de datos e información

La metodología a utilizarse es: aplicativa, cualitativa, explorativa, bibliográfica .

a) Aplicativo

Permitirá aplicar los conocimientos teóricos, buscando evidenciar los riesgos y el nivel de madurez cada dominio de la norma NTE INEN-ISO/ IEC 27000. Y aplicarlos para fortalecer en el Plan de Seguridad de la Información en la Universidad de las Fuerzas Armadas Espe extensión Latacunga

b) Cualitativo

Permitirá investigar el por qué y el cómo se tomó una decisión, basándonos en la toma de muestras pequeñas.

c) Explorativo

Se utiliza éste método ya que se trata de un tema de investigación que no ha sido abordado antes, y a la vez permitirá obtener nuevos datos y elementos que pueden conducir a formular con mayor precisión las preguntas de investigación.

d) Bibliográfico

Mediante técnicas y estrategias permite localizar, identificar y acceder a aquellos documentos que contienen la información pertinente para la investigación.

Técnicas:

a) Entrevistas

Esta técnica permitirá captar información que puede ser considerada vital ya que serán aplicadas a expertos y directivos.

b) Observación

La información que se capte directamente en el lugar de los acontecimientos, motivos de diagnóstico, se lo hará a través de observación científica y para ello se tratará de que esta pase desapercibida a los observados, y así lograr veracidad en la información.

c) Documental

Para el desarrollo de todos los capítulos se investigará la información de calidad y referentemente actual o nueva existente en libros de texto, revistas, Internet, bibliotecas virtuales y documentos oficiales de educación.

3.2 Ejecución del Proceso de Investigación

El presente proyecto ha sido enfocado en la ESPE extensión Latacunga ubicada en la provincia de Cotopaxi en su capital la ciudad de Latacunga en las calles Calle Quijano y Ordoñez y Hermanas Páez; se analizará la situación actual de la Espe extensión Latacunga en cuanto a seguridad de la información utilizando las normas técnicas ecuatorianas ISO/IEC 27000 para la seguridad de la información, y marcos de referencia como COBIT 5

Adicionalmente para la ejecución del proyecto utilizará la Metodología MPSI ESPE-L (Metodología Plan de Seguridad Informática ESPE extensión Latacunga) la misma que ha sido adoptada por los desarrolladores del presente proyecto, dicha metodología es una recolección de la información proporcionada por las norma ISO/IEC27000 para implementación de un SGSI y COBIT 5

Cómo trabaja la Metología MPSI ESPE-LATACUNGA (MPSI ESPE-L) se muestra en la figura 10 y se describe a continuación

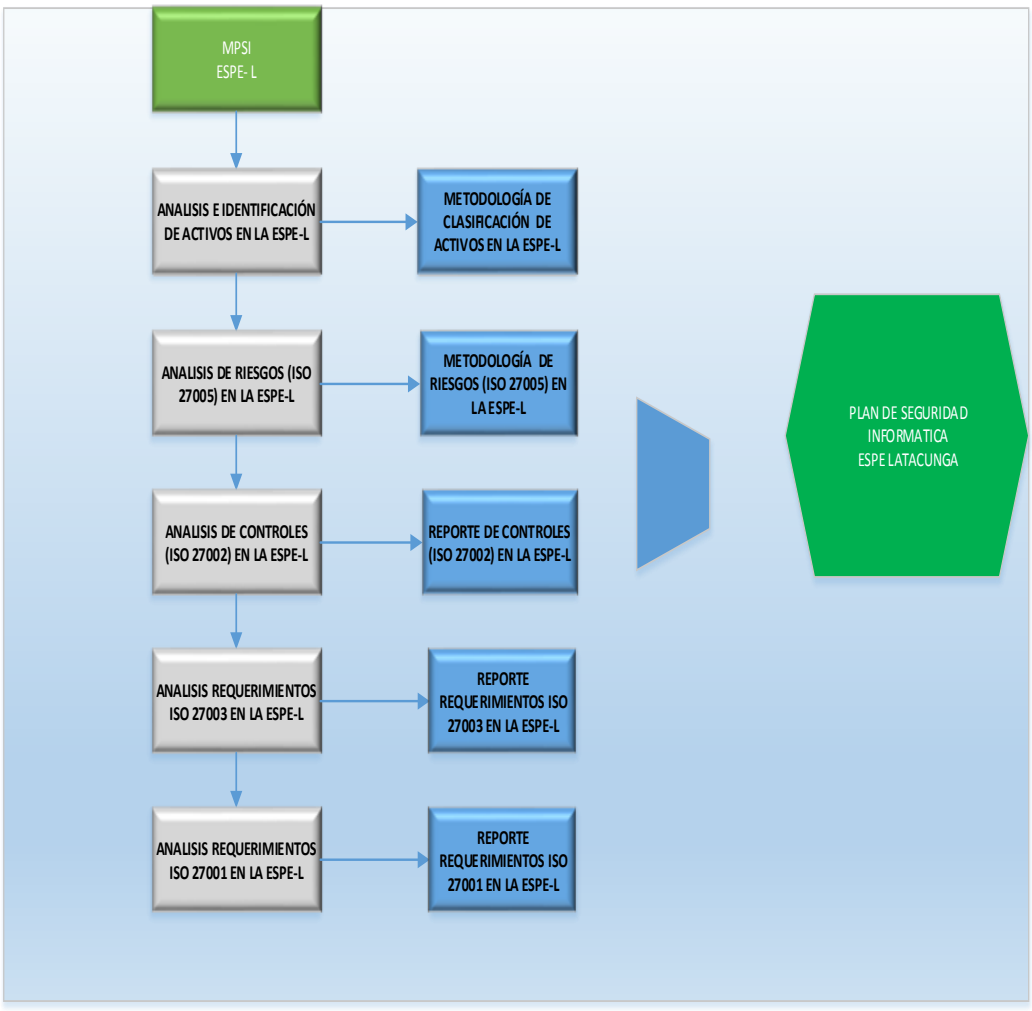


Figura 10 Metodología Plan de Seguridad Informática ESPE-LATACUNGA

Esta metodología está compuesta por diez (10) pasos los mismos que son basado en la norma ISO/IEC27000, cuyo resultado de la ejecución proveerá como resultado el **PLAN DE SEGURIDAD INFORMATICA PARA LA ESPE EXTENSIÓN LATACUNGA** dichos pasos se describe a continuación en la tabla 2:

Tabla 2

Descripción de Metodología MPSI ESPE-LATACUNGA	
Pasos	**Nombre**
1	Análisis e identificación de activos en la Espe-Latacunga
2	Metodología de clasificación de activos en la Espe- Latacunga
3	Análisis de riesgos (ISO 27005) en la Espe- Latacunga
4	Metodología de riesgos (ISO 27005) en la Espe- Latacunga
5	Análisis de controles (ISO 27002) en la Espe- Latacunga
6	Reporte de análisis de controles (ISO 27002) en la Espe-Latacunga
7	Análisis requerimientos según ISO 27003 en la Espe- Latacunga
8	Reporte requerimientos según ISO 27003 en la Espe- Latacunga
9	Análisis requerimientos ISO 27001 en la Espe- Latacunga
10	Reporte análisis de requerimientos ISO 27001 en la Espe-Latacunga

Adicionalmente para la ejecución de la metodología planteada se utilizara una serie de instrumentos en los cuales se procesará la información recolectada, los mismos que serán descritos en cada paso de la metodología y adjuntados en el presente proyecto

Paso 1 Análisis e identificación de activos en la Espe-Latacunga

Identificación de Activos

Este paso muestra la identificación de los principales elementos involucrados para la elaboración del Plan de Seguridad Informática como: Hardware, software, interfaces de sistemas, datos de información, personas involucradas, etc.

En este punto se identificarán los activos más sustanciales envueltos dentro de los procesos descritos en la información obtenida mediante la metodología de investigación expuesta en el numeral 3.1 del presente proyecto; la información obtenida se muestra en el Anexo C.

Recolección de información

Para la ejecución de este paso aplicará el Instrumento 001 (INS001) "Inventario de Activo" el mismo que está compuesto como se muestra en la tabla 3.

Tabla 3

Descripción del Instrumento 001 (INS001) Inventarios de activos ESPE-LATACUNGA	
ID	Codificación del Activo el mismo que está compuesto por las siglas AC de activo y la numeración consecutiva ejemplo: AC001
ACTIVO IDENTIFICADO	Nombre del Activo identificado
TIPO DE ACTIVO	La identificación de los activos está basado en la norma ecuatoriana ISO/IEC 27005:2008 en donde se pueden identificar dos tipos de activos: los primarios y los de soporte. Los primarios, según este estándar, son los procesos e información más sensibles para la organización. Los activos de soporte, son los activos que dan el debido soporte a estos activos primarios. Dentro de estas dos agrupaciones, se definieron siete distintos tipos específicos de activos: **Dato:** Es toda aquella información que se genera, envía, recibe y gestionan dentro de la organización. Dentro de este tipo, podemos encontrar distintos documentos que la institución educativa gestiona dentro de sus procesos.

Continúa

	Aplicación: Todo aquel software que se utilice como soporte en los procesos. **Personal:** Son todos los actores que se ven involucrados en el acceso y el manejo de una u otra manera a los activos de información de la organización. **Servicio:** Son los servicios que alguna área de la organización suministra a otra área o entidades externas a la misma. **Tecnología:** Es todo el hardware donde se maneje la información y las comunicaciones. **Instalación:** Es cualquier lugar donde se alojan los activos de información. Este lugar o ambiente puede estar ubicado dentro de la organización tanto como fuera de la misma. **Equipamiento auxiliar:** Son los activos que no se hallan definidos en ninguno de los anteriores tipos.

En la tabla 4 Inventario de Activos, se muestra el ejemplo de la aplicación del instrumento INS001.

Tabla 4

Ejemplo aplicación INS001 Inventarios de activos ESPE- LATACUNGA		
ID	ACTIVO IDENTIFICADO	TIPO DE ACTIVO
AC001	Computadora de escritorio	Tecnología
AC002	Licencia de Microsoft Windows XP	Aplicación
AC003	Licencia de Microsoft Office 2007	Aplicación
AC004	Especialista de red	Personal

Continúa

AC005	Intranet de la institución	Aplicación
AC006	Email (para el envío electrónico de información)	Aplicación
AC007	Teléfono	Tecnología

Paso 2 Metodología de clasificación de activos en la Espe-Latacunga

El resultado del primer paso es la metodología de clasificación de activos la misma que se expondrá en el próximo capítulo (IV), 4.2 Metodología para ejecutar la propuesta

Paso 3 Análisis de riesgos (ISO 27005) en la Espe-Latacunga

Los sistemas de gestión de seguridad de la información (SGSI) se inician con los procesos de valoración y mitigación de riesgos, pues las medidas de seguridad deben apuntar hacia los riesgos más importantes para el negocio.

Para la realización de dicha valorización, el estándar ISO 27005 propone varios ejemplos de métodos con los cuales se puede llevar a cabo la valorización de riesgos de manera adecuada. Adicionalmente según la misma norma en el anexo C propone ejemplos de amenazas comunes se pueden tipificar en varias clases como:

Causantes de daño físico (Fuego, daño por agua, contaminación, destrucción de equipos o medios, polvo corrosión, congelamiento, etc.), Eventos naturales, Perdida de servicios esenciales, Perturbación por radiación, Compromiso de la información, Fallas técnicas, Acciones no autorizadas, Compromiso de las funciones, Intrusiones, terrorismo, etc.

Hay que tomar en cuenta que el análisis de riesgo detallado, es un trabajo muy extenso y consumidor de tiempo, porque requiere que se compruebe todos los posibles daños de cada recurso de una institución contra todas las posibles amenazas, es decir terminaríamos con un sin número de grafos de riesgo que deberíamos analizar y clasificar.

Tomando en consideración esta premisa para la ejecución de este proyecto lo que se pretende es proporcionar de una herramienta de análisis de riesgos que ayuden a identificar estos riesgos; sin embargo se va a identificar algunos riesgos más significativos con la finalidad de tomar acciones formadas en decisiones para evitar efectos negativos en la institución.

La matriz está diseñada de la siguiente manera:

Utiliza la fórmula: **Riesgo = Probabilidad de Amenaza x Magnitud de Daño**

En la tabla 5 se considera los siguientes valores y condiciones:

Tabla 5

Valores y condiciones para matriz de riesgo ESPE-LATACUNGA	
Valor	Condición
1	Insignificante (incluido Ninguna)
2	Baja
3	Mediana
4	Alta

En la tabla 6 se considera el código de colores para la matriz de riesgo.

Tabla 6

Código de colores para matriz de riesgo ESPE-LATACUNGA	
Valor	Probabilidad de Amenaza
1-6	Riesgo Bajo
8-9	Riesgo Medio
12-16	Riesgo Alto

En la figura 11 podemos visualizar el grafo resultante después de la aplicación de la matriz de riesgo

Análisis de Riesgo ESPE-L promedio

		Probabilidad de Amenaza		
		Ataques Intencionados	Sucesos de origen físico	Negligencia y Institucional
Impacto	Datos e Información	9,6	7,3	7,2
	Sistemas e Infraestructura	5,5	7,1	6,0
	Personal (acceso a la informacion)	5,3	4,0	6,1

Figura 11 Grafo resultante en la matriz de riesgo ESPE-LATACUNGA

Cabe mencionar que posteriormente se debe aplicar la matriz considerando que los activos de información de cada proceso o actividad analizada son identificados y clasificados de acuerdo a su criticidad (integridad, confidencialidad y disponibilidad) y a su vez los recursos críticos son agrupados de acuerdo a sus funciones dentro de los procesos, para posteriormente ser revisados a través de un ciclo continuo de valoración de riesgos para determinar las amenazas relevantes, las consecuencias de su materialización y la existencia y efectividad de controles implementados que disminuyen el impacto o la probabilidad de concretar la amenaza.

Paso 4 Metodología de riesgos (ISO 27005) en la Espe-Latacunga

El resultado del paso número 3 es la metodología de riesgos la misma que se expondrá en el próximo capítulo (IV), 4.2 Metodología para ejecutar la propuesta.

Paso 5 Análisis de controles (ISO 27002) en la Espe- Latacunga

Tomando como base los requerimientos generales de la norma ISO 27001 y en los 11 dominios, 39 objetivos de control y 133 controles relacionados en su anexo A se elaboró un marco general para realizar un análisis de brecha, de la seguridad de la información en la ESPE extensión Latacunga a la mencionada norma. Adicionalmente se tuvo en cuenta las recomendaciones de implementación relacionadas en la norma ISO 27002 para estimar el estado y porcentaje de implementación de cada control en la ESPE extensión Latacunga sobre todo considerando que en el País existe el Esquema Gubernamental para la Seguridad de la Información (EGSI) emitido por la Secretaria Nacional de la Administración Pública (SNAP) y que básicamente es dicha norma.

El análisis se realizó considerando el estado de la seguridad de la información en la ESPE extensión Latacunga antes de haber dado inicio a la definición de este proyecto.

La metodología utilizada para realizar este análisis se describe a continuación en la tabla7.

Tabla 7

Matriz para análisis de brecha ESPE-LATACUNGA						
Requerimiento, Control u Objetivo de Control ISO 27001				**IMPLEMENTACIÓN**		
Requisito	# Sección	Nombre	Descripción/Objetivo	Estado	%	Observación

Tabla 8

Descripción de matriz para análisis de brecha ESPE-LATACUNGA	
Nombre	**Descripción**
Requisito	Permite identificar y diferenciar los requisitos generales, dominios, objetivos de control o controles
# de Sección	Se encuentra ligado a los números de sección de la norma ISO 27001:2005
Nombre	Corresponde al nombre del requisito, dominio, objetivo de control o control evaluado.
Descripción/Objetivo	Se relaciona una breve descripción extraída de la norma ISO 27002.
Estado	Corresponde a "Implementado", "Parcialmente implementado" o "No implementado" según corresponda. El estado se encuentra directamente relacionado con el porcentaje (%) de implementación mediante una estimación matemática, de manera que si tenemos un control en el 0% equivale a un control "No implementado", si se encuentra por encima del 60% se puede considerar "Implementado" y en los demás casos será "Parcialmente implementado".
%	Corresponde al porcentaje estimado de implementación del control o requisito basado en la realidad actual de la ESPE-L evaluada respecto a la norma ISO 27001 teniendo en cuenta los lineamientos dados por la norma ISO 27002.
Observaciones	Se incluyen a manera explicativa sobre la forma o condición específica en la que se encuentra implementado cada control

Cabe recalcar que en este análisis se han incluido todos los controles del **Anexo A de la norma ISO 27001**, independientemente que algunos de los controles se apliquen o no a la ESPE extensión LATACUNGA.

Paso 6 Reporte de controles (ISO 27002) en la Espe-Latacunga

El resultado del paso número 6 es el reporte de los controles los mismos que se expondrá en el próximo capítulo (IV).

Paso 7 Análisis requerimientos ISO 27003 en la Espe-Latacunga

Tomando como base los requerimientos generales de la norma ISO 27003 para la ejecución de un SGSI relacionados en su Anexo A (Descripción del listado de verificación) se elaboró una matriz referencial general que permitirá obtener una listado de verificación de actividades requeridas para establecer e implementar un SGSI y mapear las actividades relacionadas con la implementación del SGSI, con los requisitos de la NTE INEN ISO/IEC 27001 y que se puedan considerar para un SGSI en la ESPE-Latacunga

El análisis se realizó considerando el estado de la seguridad de la información en la ESPE-Latacunga antes de haber dado inicio a la definición de este proyecto.

La metodología utilizada para realizar este análisis se muestra en la tabla 9 y toma los valores modelo de evaluación de procesos (Process Assessment Model, PAM) de COBIT 5, que se basa en la norma ISO 15504 y que se describe a continuación:

Tabla 9

Valoración del modelo de evaluación de procesos				
Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
Inicial	En desarrollo	Definido	Gestionado	Optimizado

Fuente:(ISACA, 2012)

Adicionalmente a esta valoración se elaboró el instrumento 2 (Inst002) Anexo D que nos describe paso a paso las salidas documentadas exigidas por la norma ISO 27003 y tomado de dicha norma para la Espe extensión Latacunga para la implementación de un SGSI la misma que se describe a continuación en la tabla 10:

Tabla10

Matriz de salidas exigidas en la norma ISO 27003	
Nombre	**Descripción**
Fase de Implementación NTE INEN ISO/IEC 27003	Permite identificar la fase en la que nos encontramos de la implementación del SGSI
# de Número de paso	Se encuentra ligado a los números de sección de la norma ISO 27001:2005
Actividad, referencia NTE INEN ISO/IEC 27003	Identifica la actividad a realizar.
Paso Pre-Requisito	Se relaciona con un algún paso previo antes de ejecutar el mismo.
Salida Documentada	Corresponde a la salida del requisito documentada que se tiene como resultado.
Referencia a la NTE INEN ISO/IEC 27001	Corresponde al dominio de la norma.
Nivel	Mide el nivel de madurez del proceso

Fuente:(Instituto Ecuatoriano de Normalización , 2010)

Paso 8 Reporte requerimientos ISO 27003 en la Espe-Latacunga

El resultado del paso número 8 es el reporte del análisis de la norma ISO27003 los mismos que se expondrá en el próximo capítulo (IV).

Paso 9 Análisis requerimientos ISO 27001 en la Espe-Latacunga

Para este paso vamos utilizar la matriz de evaluación del nivel de madurez en seguridad de la información tomando como base el Modelo de Madurez de la Capacidad (CMM), de COBIT 5 dando una estimación del nivel de madurez de cada uno de los controles implantados en la ESPE extensión Latacunga, para con ello obtener una estimación de la madurez de los objetivos de control y dominios planteados en la norma ISO 27002.

De acuerdo al modelo planteado, existen cinco (5) posibles niveles de madurez y un nivel adicional para los controles que se consideran inexistentes (nivel cero). A medida que se avanza en los niveles se considera que el control es más efectivo para la ESPE

extensión Latacunga, por ello se mide adicionalmente el porcentaje de efectividad para cada control. Expresado de la siguiente forma en la tabla número 11:

Tabla11

Nivel de madurez ISO 27001					
	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
	Inicial	En desarrollo	Definido	Gestionado	Optimizado
Política	Ausencia de política	Política limitada	Política integral definida y publicada	Política publicada e implementada de manera uniforme	Revisión y mejora continuas de la política
Roles y responsabilidades	Roles y responsabilidades no definidos	Roles parcialmente definidos	Roles y responsabilidades bien determinados y definidos	Roles y responsabilidades definidos y ejecutados	Roles y responsabilidades revisados de manera continua
Automatización	Manual	Semiautomatizada	Automatizada	Automatizada y completamente operativa	Actualización permanente de la automatización
Alcance	No implementado	Cobertura limitada	Activos críticos	Completo	Revisión periódica del alcance para garantizar la cobertura total
Eficacia	N/A	Baja	Media	Alta	Muy alta
Gestión de incidentes	Sin seguimiento	Visibilidad limitada	Seguimiento de incidentes críticos	Seguimiento y cierre de todos los incidentes	RCA aplicado a todos los incidentes y solucionados
Medición	Sin medición	Medición limitada	Mediciones integrales definidas	Medido y revisado de forma periódica	Criterios de medición revisados periódicamente

Continúa

Informes	Sin informes	Informes limitados	Informes definidos	Informes enviados a la alta dirección y revisados	Requerimientos de informes periódicamente revisados y actualizados

Adicionalmente se utilizará la metodología utilizada para medir la escala de madurez de seguridad respecto a la norma ISO 27002 proporcionada por "***Jácome, Andrés, Universitat Oberta de Catalunya, En su proyecto Elaboración del plan de implementación de la norma ISO/IEC 27001:2005 en una empresa del sector retail"*** y que es expresada en la figura12 Anexo E

Efectividad (%)	Nivel de Madurez (CMM)		Descripción
0%	L0	Inexistente	-Carencia completa de cualquier proceso. -La empresa no ha reconocido que existe un problema a resolver.
Entre 0% y 10%	L1	Inicial / Ad-hoc	-El éxito de las actividades de los procesos se basa la mayoría de las veces en esfuerzos individuales. -No existen plantillas definidas a nivel corporativo.
Entre 10% y 50%	L2	Reproducible, pero intuitivo	-Los procesos similares se ejecutan en forma similar por diferentes personas con la misma tarea. -Se normalizan las buenas prácticas en base a la experiencia y al método. -No hay comunicación o entrenamiento formal -Las responsabilidades quedan a cargo de cada individuo. -Se depende del grado de conocimiento de cada individuo.
Entre 50% y 90%	L3	Proceso definido	-La organización entera participa en el proceso. -Los procesos están implantados, documentados y comunicados formalmente.
Entre 90% y 95%	L4	Gestionado y medible	-Se cuenta con indicadores y métricas que permiten cuantificar la evolución de los procesos.
Mayor a 95%	L5	Optimizado	-Los procesos están bajo constante mejora. -En base a los indicadores y métricas se determinan las desviaciones más comunes y se optimizan los procesos.

Figura 12 Escala de madurez ISO 27002 para la ESPE-LATACUNGA

Fuente: Jácome, 2014

Capítulo IV.- Resultados

4.1 Informe de Resultados

Después del análisis realizado durante la ejecución del proyecto en la ESPE extensión Latacunga y la Metodología Plan de Seguridad Informática ESPE-LATACUNGA podemos identificar los siguientes resultados:

4.1.1 Paso 1 Análisis e identificación de activos en la Espe-Latacunga

Los activos más relevantes identificados durante la ejecución de las entrevistas y la recepción de la información proporcionado por las partes interesadas se expresa en la Tabla 12.

Tabla 12

Inventario de activos ESPE extensión Latacunga		
ID	ACTIVO IDENTIFICADO	TIPO DE ACTIVO
AC001	Computadora de escritorio	Tecnología
AC002	Licencia de Microsoft Windows XP	Aplicación
AC003	Licencia de Microsoft Office 2007	Aplicación
AC004	Especialista de red	Personal
AC005	Intranet de la institución	Aplicación
AC006	Email (para el envío electrónico de información)	Aplicación
AC007	Teléfono	Tecnología
AC008	Impresora	Tecnología
AC009	Cableado Ethernet	Tecnología
AC010	Firewall	Tecnología
AC011	Vitrinas informativas	Instalación
AC012	Archivos de la extensión	Instalación
AC013	Archivadores para los documentos	Instalación
AC014	Documento de encuestas	Dato

Continúa

AC015	Documento de la programación académica anual y mensual	Dato
AC016	Información de alumnos de semestres anteriores	Dato
AC017	Materiales de estudio (silabo, presentaciones, casos, lecturas)	Dato
AC018	Registro de aulas	Dato
AC019	Servidor SPOTANIA	Tecnología
AC020	Material informativo / Documentación relacionada a los programas	Dato
AC021	Ficha de Admisión (en físico)	Dato
AC022	Ficha de Matricula (en físico)	Dato
AC023	Reporte de alumnos matriculados (en físico)	Dato
AC024	Solicitud de expedición del título	Dato
AC025	Servidor para el sistema de información	Tecnología
AC026	Director de extensión	Personal
AC027	vicerrector de extensión	Personal
AC028	Jefe de Unidad de tecnología	Personal
AC029	Alumno	Personal
AC030	Asistente de Admisión	Personal
AC031	Asistente Administración	Personal
AC032	Cajero	Personal
AC033	Egresado	Personal
AC034	Documento del perfil profesional de la nueva carrera (misión, perfil del egresado, etc.)	Dato
AC035	Documento del nuevo plan de estudios	Dato
AC036	Servidores de base de datos y aplicaciones	Tecnología
AC037	Sistema contable Financiero "Olympo"	Aplicación
AC038	Sistema Registro de ingresos "SISRIN"	Aplicación
AC039	Sistema de Órdenes de pago "GASPAG"	Aplicación
AC040	Sistema de Control Biométrico "SQUARENET"	Aplicación

Continúa

AC041	Sistema DIMM Anexo y Formulario	Aplicación
AC042	Sistema de Activos "SAF"	Aplicación
AC043	Sistema Académico de Posgrados	Aplicación
AC044	Sistema Académico de Carreras	Aplicación
AC045	Sistema Académico de Idiomas	Aplicación
AC046	Servidor de la Biblioteca "SIABUC"	Tecnología
AC047	Servidor de la BBDD	Tecnología
AC048	Sistema Record Académico Histórico	Aplicación
AC049	Servidor de servicios web	Tecnología
AC050	Servidor de Gestión de la Escuela de conducción ESPE-L	Tecnología
AC051	Portal Institucional	Aplicación
AC052	Plataforma Virtual "MOODLE"	Aplicación
AC053	Sistema de gestión de servicios	Aplicación
AC054	Sistema de gestión de Graduados "ALUMNI-ESPEL"	Aplicación
AC055	Sistema de Gestión de laboratorios de computación "SG-LAB"	Aplicación
AC056	Sistema de Gestión de consulta de comprobantes electrónicos	Aplicación
AC057	Sistema de Incidencias OTRS	Aplicación
AC058	Sistema de Mensajería y video Conferencia	Aplicación
AC059	Sistema de Encuesta	Aplicación
AC060	Micrositios de la ESPE-L	Aplicación
AC061	Ciencias Exactas	Servicios
AC062	Lenguas	Servicios
AC063	Energía Mecánica	Servicios
AC064	Ciencias Económicas, Administrativas y del comercio	Servicios
AC065	Eléctrica y Electrónica	Servicios
AC066	Biblioteca	Servicios
AC067	Educación Continua	Servicios

Continúa

AC068	Admisión y registro	Servicios
AC069	Investigación y vinculación con la colectividad	Servicios
AC070	Bienestar estudiantil	Servicios
AC071	Gastronomía	Servicios
AC072	Empleamiento	Servicios
AC073	Revista digital ESPECTACUM	Dato
AC074	Club de cultura	Servicios
AC075	Escuela de conducción	Servicios
AC076	Club de robótica	Servicios
AC077	Noticias ESPEL	Dato
AC078	Grupo de Vehículos sostenibles	Servicios
AC079	Grupo Procesamiento digital	Servicios
AC080	Grupo Investigación automática control	Servicios
AC081	Grupo de mecánica aplicada computacional	Servicios
AC082	Grupo de Sistemas Estratificados de recursos turísticos	Servicios
AC083	Unidad de tecnología de Información y comunicación	Instalación
AC084	Unidad Financiera	Servicios
AC085	Especialista de comunicaciones de red	Personal
AC086	Sistema de Idiomas "ACAD"	Aplicación
AC087	Administrador de Servicios de red y comunicación	Personal
AC088	Especialista de servicios técnicos	Personal
AC089	Técnico de mantenimiento de equipos	Personal
AC090	Especialista en desarrollo de aplicativos	Personal
AC091	Especialista en desarrollo de base de datos	Personal
AC092	Edificio talleres y bodega	Instalación
AC093	Edificio bloque PLAZA centro de datos	Instalación
AC094	Edificio laboratorios de sistemas	Instalación
AC095	Edificio nuevo	Instalación
AC096	Edificio Biblioteca	Instalación

Continúa

AC097	Instructivo para la regulación de adquisición de equipos de computo	Dato
AC098	Departamentos académicos y jefatura	Instalación
AC099	Jefatura de investigación	Instalación
AC100	Jefatura Administrativa Financiera	Instalación
AC101	Unidad de Bienes e inventarios	Instalación
AC102	Unidad de logística	Instalación
AC103	Instructivo para la utilización del servicio de almacenamiento y respaldo de información	Dato
AC104	Instructivo para la utilización del servicio de internet a través de la red wireless	Dato
AC105	Mapa de cobertura del servicio de internet	Dato
AC106	Instructivo sobre la regulación de la adquisición de software	Dato
AC107	Instructivo sobre la utilización de los micrositios de la universidad	Dato
AC108	Lista de micrositios de la Espe extensión Latacunga	Dato
AC109	Esquema de contenidos	Dato
AC110	Configuraciones de sistemas	Dato
AC111	Política de correo electrónico (Espe matriz)	Dato
AC112	Política de uso de correo electrónico	Dato
AC113	Política de uso del servicio de internet	Dato
AC114	Política de acceso a los recursos y la información	Dato
AC115	Política de uso de los recursos y servicios de tecnologías de información	Dato
AC116	Políticas de gestión de tecnologías de la información	Dato
AC117	Diagrama unifilar ESPE-Latacunga	Dato
AC118	Plan de capacitación ESPE-Latacunga	Dato

Las amenazas identificadas durante la ejecución de las entrevistas y la recepción de la información proporcionado por las partes interesadas se expresa en la Tabla 13.

Tabla 13

Inventario de Amenazas ESPE EXTENSIÓN LATACUNGA		
ID	AMENAZA	TIPO
AMZ001	Manipulación de la configuración (externa)	INTENCIONADOS
AMZ002	Suplantación de la identidad del usuario	
AMZ003	Acceso no autorizado	
AMZ004	Sabotaje (ataque físico y electrónico)	
AMZ005	Abuso de Privilegio de acceso (interno)	
AMZ006	Robo / Hurto (físico)	
AMZ007	Robo / Hurto de información electrónica	
AMZ008	Introducción de falsa información	
AMZ009	Destrucción de información	
AMZ010	Divulgación de información	
AMZ011	Virus / Ejecución no autorizado de programas	
AMZ012	Indisponibilidad del personal	
AMZ013	Violación a derechos de autor	
AMZ014	Incendio	FISICOS
AMZ015	condiciones inadecuadas de temperatura y/o humedad	
AMZ016	Fallos de servicio de comunicación	
AMZ017	Sobrecarga eléctrica	
AMZ018	Falla de corriente (apagones)	
AMZ019	Averías de origen físico o lógico	
AMZ020	Deficiencias en la organización (falta de inducción al personal)	Sucesos derivados de la inexperiencia, negligencia de usuarios/as y
AMZ021	Errores de configuración	
AMZ022	Errores de usuario	

Continúa

AMZ023	Error de administrador	decisiones institucionales
AMZ024	Error de monitorización (log)	
AMZ025	Divulgación de información	
AMZ026	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	
AMZ027	Errores de mantenimiento actualización del programa	
AMZ028	Errores de mantenimiento actualización de los equipos	
AMZ029	Caída del sistema por agotamiento de recursos	
AMZ030	Transmisión de contraseñas por teléfono	
AMZ031	Falta de definición de perfil, privilegios y restricciones del personal (implantación)	
AMZ032	Falta de mantenimiento físico (proceso, repuestos e insumos)	
AMZ033	Falta de actualización de software (proceso y recursos)	
AMZ034	Introducción de información errónea	
AMZ035	Repudio (Interno)	

Una vez identificado los activos de información y para la elaboración del presente proyecto, por cada activo de información se realizó el análisis con los respectivos responsables, acerca de las posibles amenazas potenciales (pueden suceder) y reales (han sucedido). Esta información se consolido en la Matriz Análisis de Riesgo Anexo F y a continuación en la figura 13 y figura 14 se presentan estadísticas de análisis a los resultados obtenidos agrupando las amenazas por su categoría:

Análisis de Riesgo ESPE-L promedio

		Probabilidad de Amenaza		
		Ataques Intencionados	Sucesos de origen físico	Negligencia y Institucional
Impacto	Datos e Información	9,6	7,3	7,2
	Sistemas e Infraestructura	5,5	7,1	6,0
	Personal (acceso a la informacion)	5,3	4,0	6,1

Figura 13 Análisis riesgo impacto amenaza para la ESPE-Latacunga

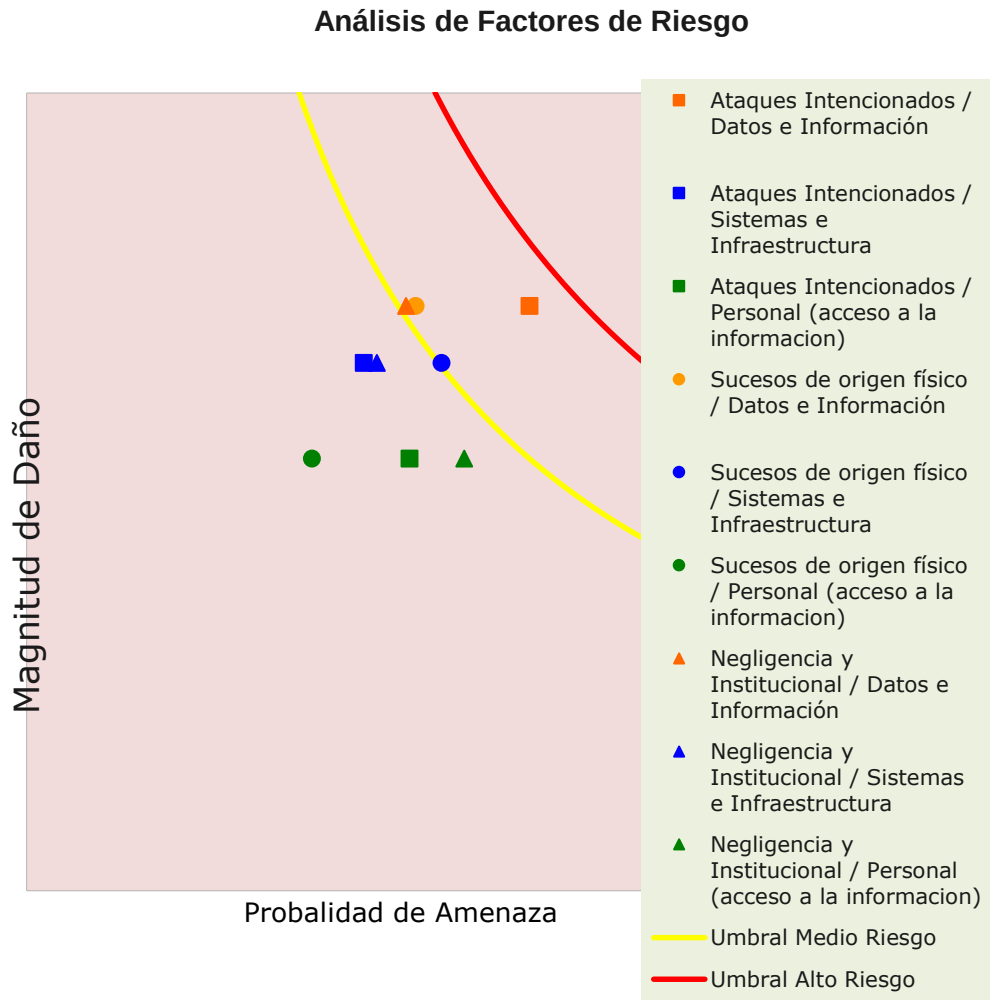


Figura 14 Análisis de factores de riesgo para la ESPE-Latacunga

Análisis

En el análisis de los resultados de la aplicación de la matriz amenazas vs impacto podemos evidenciar que existen un riesgo de nivel medio en toda la categoría datos e información y riesgo medio en cuanto a la seguridad de la infraestructura suscitados de origen físico.

Por otro lado las amenazas más importantes son: los ataques intencionados en los datos e información, seguidos por los suceso de orden físico y negligencia institucional mientras los sucesos de orden físico ligado al personal con el acceso a la información son las amenazas que han sido controladas debido diferentes procedimientos establecidos en la ESPE extensión Latacunga.

4.1.2 Reporte de análisis de controles (ISO 27002) en la Espe-Latacunga

En cuanto al análisis de los controles del anexo A de la norma ISO 27002, Manejada en la matriz análisis de brecha respecto a la norma ISO 27002 Anexo G, se muestra el resumen consolidado de dicha evaluación agrupado por dominios y en general para todos los controles tabla 14.

Tabla 14

Estado general de implementación ISO 27001 por dominios de su anexo A

# Sección	Nombre	% implementación
A.5	Política de Seguridad	0%
A.6	Aspectos Organizativos de la Seguridad de la Información	43%
A.7	Gestión de Activos	23%
A.8	Seguridad Ligada a los Recursos Humanos	72%
A.9	Seguridad Física y del Entorno	65%
A.10	Gestión de Comunicaciones y Operaciones	56%
A.11	Control de Acceso	37%
A.12	Adquisición,Desarrollo y Mantenimiento de Sistemas de Información	41%
A.13	Gestión de Incidentes de Seguridad de la Información	26%
A.14	Gestión de la Continuidad del Negocio	2%
A.15	Cumplimiento	56%
TOTAL SGSI		38%

En la figura 15 y Figura 16 mostradas a continuación se identifica la relación entre todos los dominios respecto al máximo posible (100%) evidenciando en color rojo aquellos que están por debajo del valor medio posible

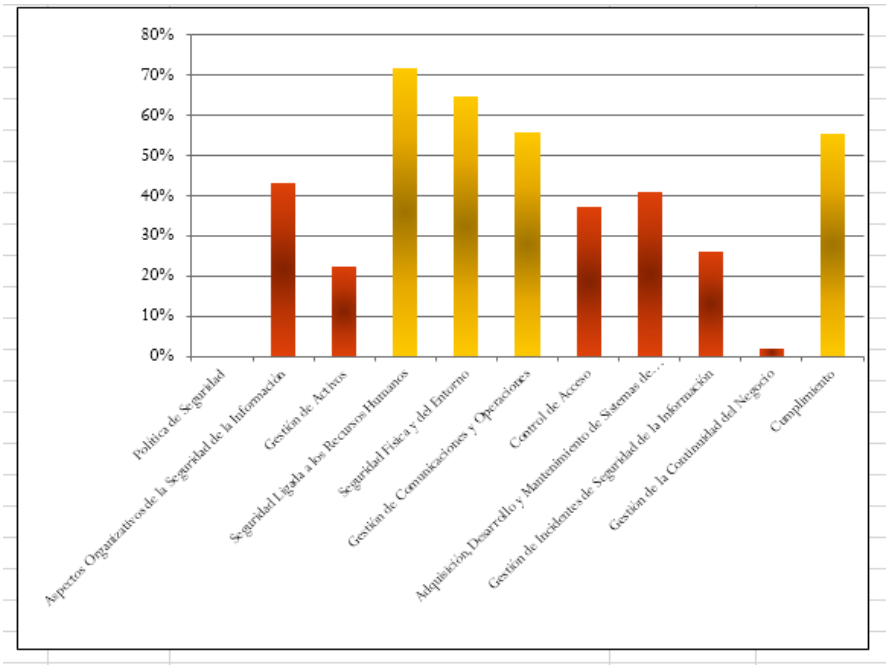


Figura 15 Diagrama de Barras de la implementación de controles de ISO 27002

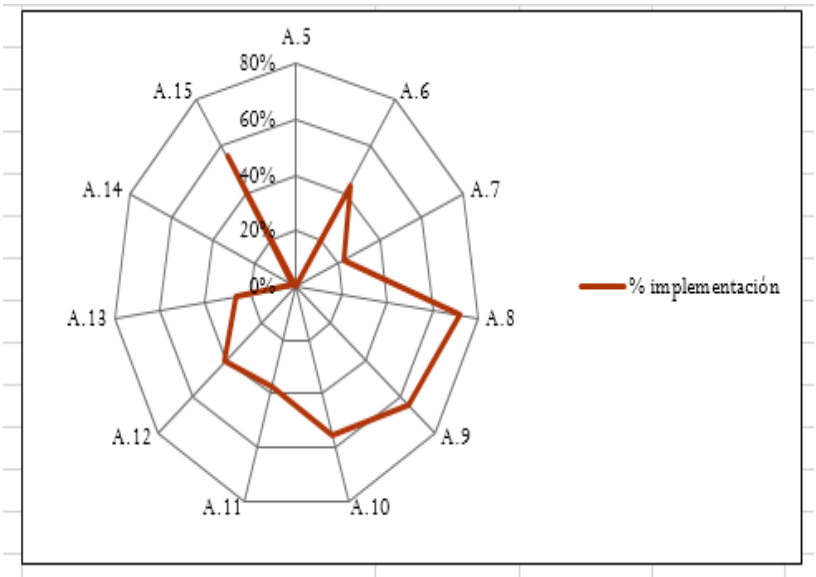


Figura 16. Diagrama de Radar de la implementación de controles de ISO 27002

En los datos presentados en la Tabla 14, hay que destacar el siguiente análisis en el dominio A.8 Seguridad Ligada a los Recursos Humanos, es el Dominio que más se lo tratado en la ESPE-Latacunga con un 72% y el dominio A.5 es el dominio que menos atención se lo ha prestado, habiendo de considerar que para este análisis se toma en cuenta los controles de la ISO 27000, un punto a reflexionar que la ESPE-Latacunga NO tiene IMPLEMENTADO un SGSI y por consiguiente se pudo considerar este punto como la incidencia principal por el bajo índice de implementación de controles.

4.1.3 Reporte requerimientos según ISO 27003 en la Espe-Latacunga

En cuanto al análisis de los controles del anexo A de la norma ISO 27003, manejada en el Anexo H, a continuación se muestra el resumen consolidado tabla 15.

Tabla 15

Estado general de implementación ISO 27003 por dominios de su anexo A

Norma 27003		Evaluación	Calificación /(5)
A05	Obtener Aprobación de la Dirección para la	1,4	5
A-06	Definición del alcance y política del SGSI	3,3	5
A–07	Realizar el Análisis de la Organización	2,0	5
A-08	Realizar la Evaluación del Riesgo y Selección de las Opciones de Tratamiento del Riesgo	0,0	5
A-09	Modelo de información organizacional	3,3	5

Como se puede observar en la figura 17, la ESPE extensión Latacunga tiene un índice bajo en la implementación de la norma por lo que se requiere urgente la implementación de un SGSI en la institución, sobre todo un análisis primordial del riesgo en cuanto a los activos de la información.

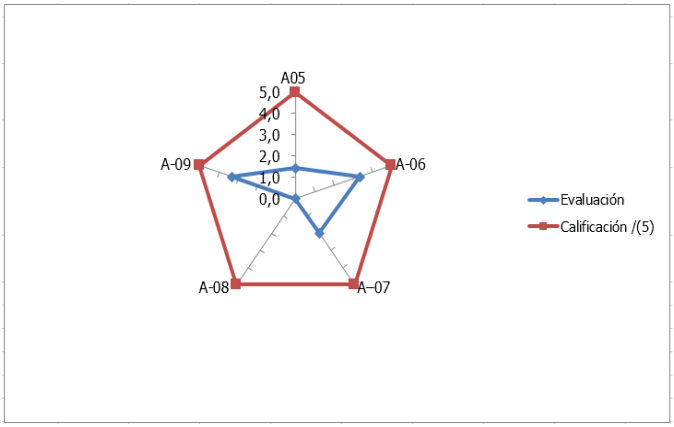


Figura 17. Diagrama de Radar de la implementación de controles de ISO 27003

4.1.4 Reporte análisis de requerimientos ISO 27001 en la Espe-Latacunga

Para dar un valor aritmético del nivel de implementación de los objetivos de control se ha realizado un promedio de las evaluaciones de los controles incluidos en éstos objetivos. Así mismo, la evaluación de los Dominios de la ISO 27001 corresponde al promedio resultante de la evaluación de sus objetivos de control y controles establecidos.

De acuerdo a la evaluación realizada del cumplimiento de los requisitos generales de la ISO 27001, Anexo G se obtuvo que en promedio solo el 16% Tabla de éstos se encuentran implementados en la ESPE extensión Latacunga. Lo anterior no quiere decir que la seguridad de la información en la institución no exista, sino que actualmente no cuenta con el nivel de madurez en sus procesos de seguridad de la información de acuerdo a lo establecido en la norma ISO 27001

Tabla 16

Estado general de implementación ISO 27001

Implementación de Requisitos Generales ISO 27001	16%

Como último análisis se muestra el nivel de madurez en el que se encuentra la ESPE extensión Latacunga con respecto a los requerimientos de la Secretaria Nacional de Administración Pública SNAP en cuanto a la implementación del acuerdo 166 “Implementación del EGSI”.

Podemos visualizar en la tabla 17 que el nivel de madurez de la ISO27002 Anexo I en la ESPE extensión Latacunga es de 38% .Obviamente considerando que la extensión no cuenta aún con la implementación del EGSI

Tabla 17

Madurez de Seguridad Dominios ISO 27002

# Sección	Nombre	Efectividad (%)	Nivel de Madurez	Nivel de Madurez (CMM)
A.5	Política de Seguridad	0%	0	Inexistente
A.6	Aspectos Organizativos de la Seguridad de la Información	35%	2	Reproducible, pero intuitivo
A.7	Gestión de Activos	17%	2	Reproducible, pero intuitivo
A.8	Seguridad Ligada a los Recursos Humanos	81%	3	Proceso definido
A.9	Seguridad Física y del Entorno	62%	3	Proceso definido
A.10	Gestión de Comunicaciones y Operaciones	66%	3	Proceso definido
A.11	Control de Acceso	48%	2	Reproducible, pero intuitivo
A.12	Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	43%	2	Reproducible, pero intuitivo
A.13	Gestión de Incidentes de Seguridad de la Información	8%	2	Inicial / Ad-hoc
A.14	Gestión de la Continuidad del Negocio	8%	1	Inicial / Ad-hoc
A.15	Cumplimiento	55%	3	Proceso definido
TOTAL SGSI		38%	2	Proceso definido

En la figura 18 y figura 19 se puede observar que el nivel de madurez de la norma ISO27002 y en general de los requerimientos exigidos por el EGSI en los dominios: A.8 atado a Niveles Seguridad ligada a los recursos humanos, A.9 ligado a la Seguridad Física y del entorno, A.10 Gestión de las comunicaciones y operaciones y el dominio A.15 ligado a el cumplimiento, se encuentra en PROCESOS DEFINIDOS según el nivel de madurez establecido en la métrica COBIT 5 utilizada para este proyecto.

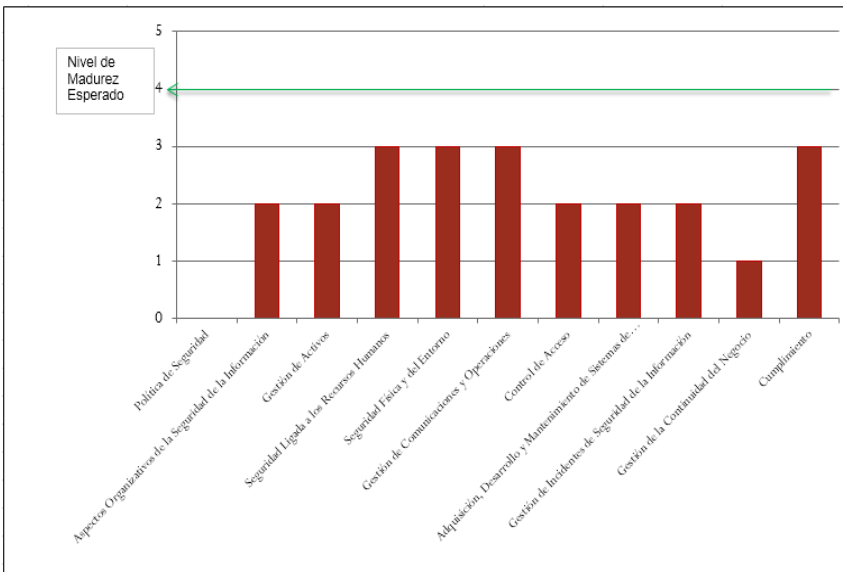


Figura 18. Diagrama de Barras de Madurez de Seguridad Dominios ISO 27002 (EGSI)

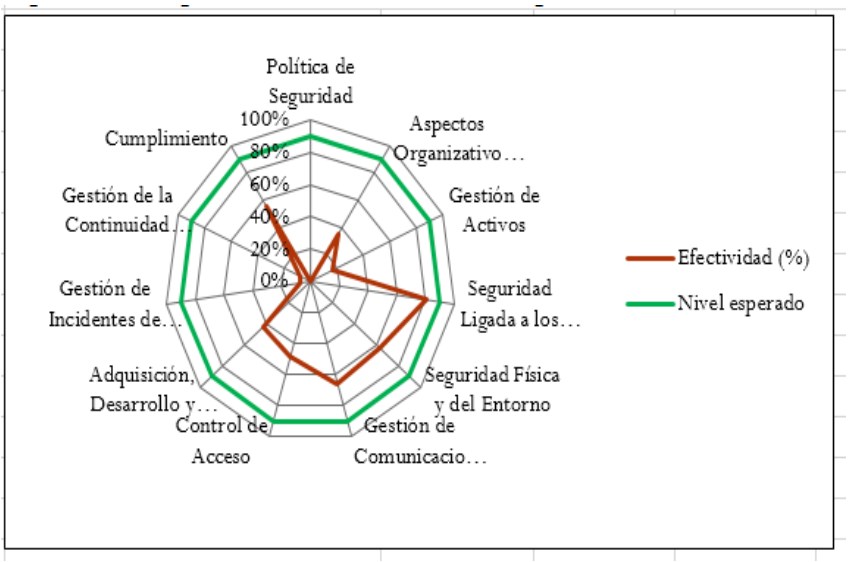


Figura 19. Diagrama de Radar de Madurez de Seguridad Dominios ISO 27002 (EGSI)

4.2 Metodología para ejecutar la propuesta

Como habíamos mencionado en los capítulos anteriores la metodología de investigación diseñada por los autores del presente proyecto se denominó **MSPSI** 'Metodología Plan de Seguridad Informática ESPE-Latacunga' como lo muestra la figura 20 y está conformado por los pasos que se describe en la tabla 18, dicha metodología dará como resultado el PLAN DE SEGURIDAD INFORMATICA PARA LA ESPE EXTENSIÓN LATACUNGA. Anexo H

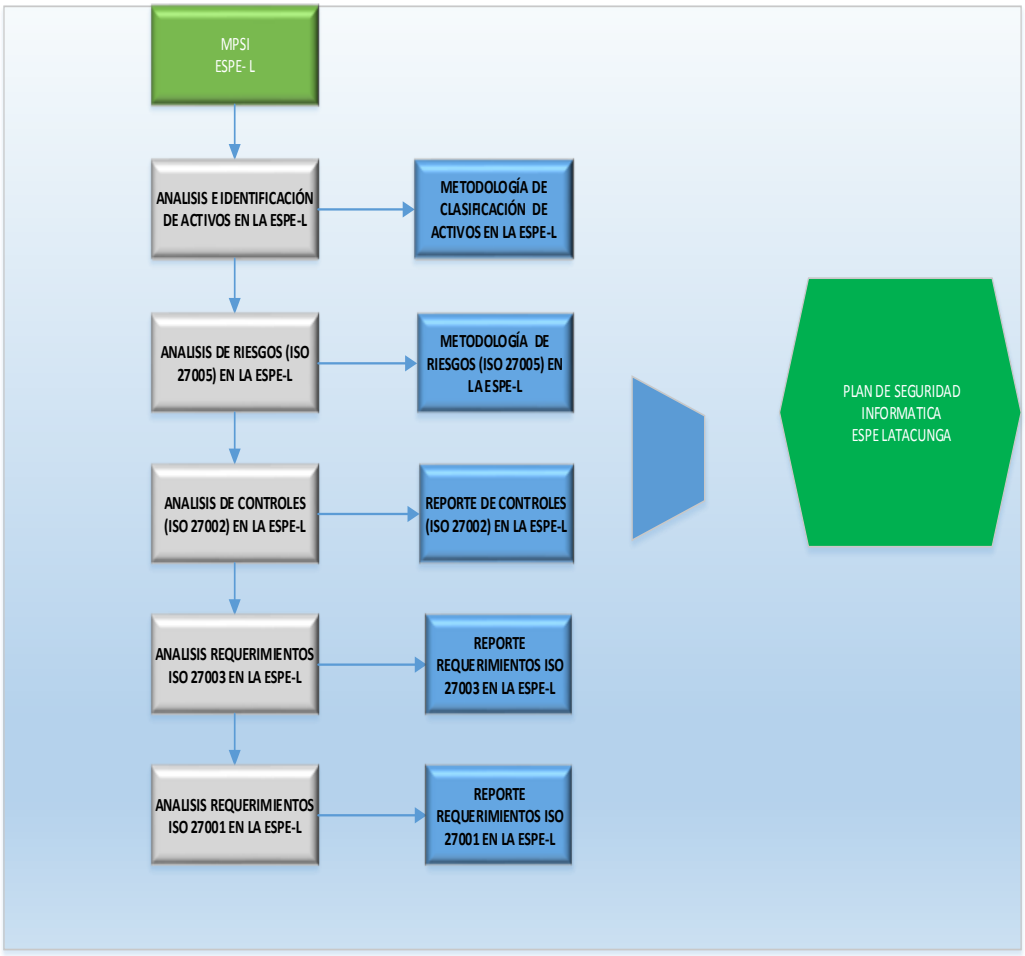


Figura 20 Metodología Plan de Seguridad Informática ESPE-Latacunga

Tabla 18

Descripción de Metodología MSPSI ESPE- LATACUNGA	
Pasos	**Nombre**
1	Análisis e identificación de activos en la Espe-Latacunga
2	Metodología de clasificación de activos en la Espe-Latacunga
3	Análisis de riesgos (ISO 27005) en la Espe-Latacunga
4	Metodología de riesgos (ISO 27005) en la Espe-Latacunga
5	Análisis de controles (ISO 27002) en la Espe-Latacunga
6	Reporte de análisis de controles (ISO 27002) en la Espe-Latacunga
7	Análisis requerimientos según ISO 27003 en la Espe-Latacunga
8	Reporte requerimientos según ISO 27003 en la Espe-Latacunga
9	Análisis requerimientos ISO 27001 en la Espe-Latacunga
10	Reporte análisis de requerimientos ISO 27001 en la Espe-Latacunga

Adicionalmente esta metodología efectúa un análisis en cada paso y considera los resultados de cada análisis.

Capítulo V.- Conclusiones y Recomendaciones

4.1 Conclusiones

En conjunto con las personas, la información es el activo más importante que tiene cualquier organización. La no presencia de controles y políticas orientadas a su seguridad puede acarrear consecuencias graves para el cumplimiento de los objetivos de la universidad.

En la ESPE extensión Latacunga no hay un adecuado Manejo con respecto a la seguridad de información tomando como referencia la Iso "27000, partiendo de que existe deficiencia en la seguridad de los procesos y la en la documentación de la mismos

No existe metodología de clasificación de Activos, ni de mitigación de riesgos es por eso que existe la implementación del SGSI/EGSI en la Espe extensión Latacunga de un 16%

En la ESPE extensión Latacunga no hay un adecuado manejo con respecto a la seguridad de información, partiendo de que no existen procesos definidos y documentados.

Dicha falta de definición de procesos se puede evidenciar en la carencia de políticas, normas y controles dentro de la Espe extensión Latacunga y en la falta de gestión del personal.

Un Sistema de Gestión de Seguridad de Información (SGSI)/EGSI establecido en la ESPE extensión Latacunga se muestra como la solución para que el flujo de información que se da entre los procesos críticos y los activos involucrados dentro de dichos procesos, logren el nivel de seguridad adecuado para garantizar el cumplimiento de los objetivos de TI y en consecuencia, los objetivos organizacionales.

Finalmente, cabe resaltar que si no se cuenta con el apoyo de la alta gerencia de la institución no se contara con el soporte necesario para lograr los objetivos del SGSI. Así mismo, si el personal de la organización no sigue las políticas y lineamientos propuestos

por la alta gerencia siguiendo dicho SGSI /EGSI, no se obtendrá el nivel adecuado de seguridad en los flujos de información de los distintos procesos de la Espe extensión Latacunga.

4.2 Recomendaciones

Seguir los lineamientos establecidos en el Plan de Seguridad de la Información expresado como Anexo J, en el presente documento.

Realizar campañas de concientización periódicas para el personal de la institución con respecto a la seguridad de información, de tal manera que todos los empleados de los diversos niveles jerárquicos existentes de la Espe extensión Latacunga, conozcan la importancia y las consecuencias de no seguir los lineamientos de seguridad en el día a día.

Lograr establecer un rol de "Oficial de Seguridad de Información" dentro de la Espe extensión Latacunga para el monitoreo y cumplimiento de las políticas y controles establecidos por la alta dirección. Este rol no implica la contratación de personal, sino que puede ser algún colaborador de la Universidad y que le brinden todo el apoyo que se requiere para el cargo.

Implementar y actualizar periódicamente el SGSI. El plazo recomendado es cada 2 años ya que este período implica la posible adquisición de nuevas tecnologías dentro del campus, o la posible modificación de las actividades de los procesos "core", teniendo como consecuencia el incremento o decremento de activos de información. Esta actualización, la debe realizar la persona que tenga el rol de "Oficial de Seguridad de Información" dentro de la institución.

Realizar ejercicios de escritorio para comprobar los controles establecidos dentro del SGSI. Por lo menos una vez al año.

Bibliografía

International organization for standardization. (2008). ISO/IEC 27005:2008. *Information technology - Security techniques - Information security risk management*. EEUU.

Alexander, A. (2005). *Diseño de un sistema de Seguridad de la Información.* México: Grupo Alfa Omega.

Aliaga Flores, L. C. (febrero de (2013). Diseño de un sistema de gestión de seguridad de información para un instituto educativo. *Diseño de un sistema de gestión de seguridad de información para un instituto educativo*. Lima, Peru, Peru. Obtenido de http://tesis.pucp.edu.pe/repositorio/handle/123456789/933

Cano, J. (2011, Volumen 2). El debido Cuidado en Seguirdad de la Información, Un ejercicio de virtudes . *Isaca Journal*, 1-8.

Chang, C. E. (Abril de 2011). Diseño de un sistema de gestión de seguridad de información para una compañía de seguros. Lima, Lima, Peru. Obtenido de http://tesis.pucp.edu.pe/repositorio/handle/123456789/933

Instituto Ecuatoriano de Normalización . (2010). *NTE INEN ISO/IEC27003.* QUITO.

Instituto Ecuatoriano de Normalización. (27002:2010). *Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27001.* Quito.

International Organization for Standardization. (2004). Iso /Iec. *Management Of Information and comunications technology Security*. EEUU.

International organization for standardization. (2005). ISO/IEC 27002:2005. *Information technology - Security techniques* . EEUU.

International organization for standardization,. (2010). ISO/IEC 27003:2010. *Security techniques - Information security management systems implementation guidance*. EEUU.

International Organization for Standarization. (2002). ISO /IEC. *Risk management-Vocabulary*. EEUU.

ISACA. (2012). *Cobit 5.* Rolling Meadows.

ISACA. (2012). *COBIT 5. Information Securty.* Illinois: USA.

It governance institute. (2012). *COBIT 5.* Illinois: USA.

Jácome, A. (25 de Agosto de 2014). Elaboración del plan de implementación de la norma ISO/IEC 27001:2005 . *Tesis para optar por el título de Máster Universitat Oberta de*

Catalunya. Bogota, Colombia. Obtenido de http://openaccess.uoc.edu/webapps/o2/handle/10609/35821