ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRIA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS III PROMOCIÓN

TESIS DE GRADO MAESTRIA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

TEMA: "EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN AL PROCESO DE ADMISIÓN DE ESTUDIANTES DE LA UTE BASADA EN ISO/IEC 27000"

AUTORES: VALLEJO CIFUENTES RICARDO PATRICIO

VIVANCO RIOS EDWIN JAVIER

DIRECTOR: MsC. Ing. VELÁSQUEZ NANCY

SANGOLQUÍ, 2014

UNIVERSIDAD DE LA FUERZAS ARMANDAS-ESPE

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

DECLARACIÓN DE RESPONSABILIDAD

Ricardo Patricio Vallejo Cifuentes

Edwin Javier Vivanco Ríos

DECLARAMOS QUE:

El proyecto de grado denominado Evaluación de Seguridad de la Información al Proceso de Admisión de Estudiantes de la UTE basada en ISO/IEC 27000, ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan el pie de las páginas correspondiente, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es nuestra autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, Mayo de 2014

Edwin Javier Vivanco Ríos	Ricardo Patricio Vallejo Cifuentes

UNIVERSIDAD DE LAS FUERZAS ARMADAS

ESPE

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

CERTIFICADO

MsC. Ing. Nancy Velásquez

CERTIFICA

Que el trabajo titulado Evaluación de Seguridad de la Información al Proceso de Admisión de Estudiantes de la UTE basada en ISO/IEC 27000, realizado por el Ing. Ricardo Patricio Vallejo Cifuentes y el Ing. Edwin Javier Vivanco Ríos, ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidas de la Universidad de las Fuerzas Armadas-ESPE.

Debido al entero cumplimiento de los objetivos trazados en el presente trabajo de titulación si se recomienda su publicación.

El mencionado trabajo consta de un documento empastado y un disco compacto el cual contiene los archivos en formato portátil de Acrobat (pdf). Autorizan al Ing. Ricardo Patricio Vallejo Cifuentes y al Ing. Edwin Javier Vivanco Ríos que lo entreguen al Mayor Mario Ron, en su calidad de Director de la Carrera.

Sangolquí, Mayo de 2014

_____

Nancy Velásquez

DIRECTOR

UNIVERSIDAD DE LAS FUERZAS ARMADAS

ESPE

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

AUTORIZACIÓN

Nosotros, Ricardo Patricio Vallejo Cifuentes

y Edwin Javier Vivanco Ríos

Autorizamos a la UNIVERSIDAD DE LA FUERZAS ARMANDAS-ESPE, la publicación, en la biblioteca virtual de la Institución del trabajo Evaluación de Seguridad de la Información al Proceso de Admisión de Estudiantes de la UTE basada en ISO/IEC 27000, cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Sangolquí, Mayo de 2014

Edwin Javier Vivanco Ríos	Ricardo Patricio Vallejo Cifuentes

Dedicatoria

El presente trabajo de titulación se lo dedico primero a Dios, en segundo lugar a mi hijo Ian Franceso, quien es un ejemplo de lucha por vivir. A mis padres y familiares más cercanos. Y a todas las personas que han apoyado de alguna manera a la conclusión del presente trabajo.

Ricardo Patricio Vallejo Cifuentes.

La firmeza y la perseverancia son claves para conseguir el éxito.

A mi princesita bella, Paola Estefanía, mi fuente de inspiración y motivación para seguir adelante. A mi esposa Karina por brindarme su apoyo y compresión. Y a todas las personas que me han apoyado para culminar este trabajo.

Edwin Javier Vivanco Ríos.

Agradecimiento

Queremos expresar, en primer lugar, el agradecimiento a la MsC. Ing. Nancy Velásquez por la confianza depositada en nosotros y por su predisposición constante para guidarnos durante el desarrollo del presente proyecto.

A la Universidad Tecnológica Equinoccial por habernos proporcionado la información necesaria para la elaboración del presente proyecto y en especial a quienes conforman al departamento de Orientación Académica, al MsC. Ing. Julio Cevallos Gómez - Rector, Dra. Lourdez Armendariz Galarza - Vicerrectora General Académico y Dra. Salúa Almeida - Jefe del Departamento de Orientación Académica.

A nuestros familiares, amigos y compañeros que nos apoyaron continuamente para llevar a cabo este proyecto.

Índice de Contenidos

Índice de Figuras

Índice de Cuadros

Índice de Tablas

Índice de Anexos

Resumen

La Universidad Tecnológica Equinoccial (UTE) tiene incertidumbre por los incidentes de seguridad de la información del proceso de admisión de estudiantes de pregrado, campus Quito, ocurridos durante los últimos 6 meses y está preocupada por el grado de vulnerabilidad del proceso, efectividad de los controles de seguridad implementados actualmente y la protección efectiva de la información. La UTE ha planificado implantar un Sistema de Gestión de Seguridad de la Información (SGSI) en la matriz Quito y posteriormente replicarlo en las Sedes a nivel nacional.

Disponer de un SGSI representa un esfuerzo importante para toda organización que inicie el camino hacia la gestión de la seguridad de la información. Por tal razón, la UTE requiere iniciar las actividades para proteger la información del proceso crítico: admisión de estudiantes de pregrado, gestionar los riesgos relacionados a la elaboración de exámenes de admisión, evaluación de aspirantes, análisis y ponderaciones de datos requeridos para la toma de decisiones por parte de las autoridades.

Se pretende evaluar la seguridad de la información del proceso de admisión de estudiantes de Pregrado Campus Quito, basado en la norma internacional ISO/IEC 27000 para determinar el nivel de seguridad de la información, identificar y valorar los riesgos, y elaborar un plan de tratamiento de riesgos asociado a este proceso, se emplearán ISO/IEC 27001:2005 e NTE INEN-ISO/IEC 27005:2012.

En la investigación se utilizará la metodología cualitativa incluyendo investigación documental-bibliográfica, investigación de campo e investigación descriptiva, centrándose en el contexto de un caso de estudio. La recolección de datos será mediante la observación del entorno y hechos relevantes, entrevistas abiertas y semi-estructuradas al personal involucrado, así como empleo de documentos. En el análisis de

datos se utilizará la metodología de gestión de riesgos descrita en NTE INEN-ISO/IEC 27005:2012 para analizar y valorar los riesgos mediante el método cualitativo.

Palabras clave:

Seguridad de la Información,

ISO/IEC 27000,

Proceso de Admisión,

Gestión de Riesgos,

Análisis de brecha de seguridad.

Summary

Universidad Tecnológica Equinoccial (UTE) is unclear about the incidents of information security of the admission process of undergraduate students, occurred in Quito during the last 6 months and is concerned about the vulnerability of the process, effectiveness of security controls currently implemented and effective protection of information. UTE planned to implement a Management System of Information Security (ISMS) in the matrix Quito and after replicate this for extensions and support centers.

Have an ISMS represents a major effort for any organization to begin the road to managing information security. For this reason, UTE needs to initiate actions to protect critical information process: admission of undergraduate students, in order to manage risks related to the development of examinations testing, evaluation of candidates, analysis and data assessing required for authorities decisions.

We plan to evaluate the information security process for admitting Undergraduate students in Quito, based on ISO/IEC 27000 international standard for determining the level of information security, identify and assess risks, and develop a treatment plan risk associated with this process, ISO/IEC 27001:2005 and NTE INEN-ISO/IEC 27005:2012 to be used.

The research will use qualitative methodology including documentary research, field research and descriptive research, focusing on the context of a case study. Data collection will be through observation of the environment and relevant facts, open and semi -structured interviews with personnel involved and use of documents. In the data analysis the risk management methodology described in NTE INEN-ISO/IEC 27005:2012 to analyze and assess risk by qualitative method will be also used.

Key words:

Information Security,

SO/IEC 27000,

Admission Process,

Risk Management,

GAP analysis.

CAPÍTULO 1

1 PLANTEAMIENTO DEL TEMA

1.1 Justificación e Importancia

1.1.1 Estado del arte a nivel mundial y local

La seguridad de la información ha sido utilizada en todos los sectores productivos de la sociedad, mediante la adopción de buenas prácticas como la norma ISO/IEC27001:2005.

Arean Melo, en su estudio enfatiza que las organizaciones deben estar alineadas a la norma ISO/IEC 27001:2005 para asegurar el cumplimiento jurídico relacionado con la seguridad de la información debido a que imparte reglas, amenazas y vulnerabilidades para que las organizaciones reglamenten o autorregulen la gestión de los activos de información de manera segura. (Melo, 2008)

Académicos de la Universidad Veracruzana realizaron un estudio aplicado a 150 empresas de la cuidad de Tuxpan, Veracruz, respecto al manejo y la importancia de la gestión de la seguridad de la información, utilizando como herramienta de recolección de datos mediante encuestas y determinaron que las empresas consideran indispensable la adopción de la norma ISO/IEC 27001:2005 para incrementar la productividad y competitividad en el mercado local y global, pero que la causa principal para no haber tomado las medidas correspondientes es la falta de asignación de recursos. (Flores Barrios, Soto del Ángel, Camacho Díaz, & Barrera Reyes, En el análisis de impacto de los sistemas de gestión de seguridad de la información bajo la norma ISO/IEC 27001 en las empresas de la cuidad Tuxpan, Mexico, 2011)

En conformidad a lo expuesto, las naciones están estableciendo leyes y regulaciones que contemplen la problemática de la seguridad de la información y se puede citar el Esquema Nacional de Seguridad en España que alinea el Real Decreto 3/2010 a la ISO/IEC 27000 y es de carácter obligatorio para las instituciones públicas (“Disposición 1330 del BOE núm. 25 de 2010 - BOE-A-2010-1330.pdf”), situación similar ocurre en Alemania a través de la Oficina Federal para la Seguridad de la Información (BSI) que ha alineado una guía para la seguridad de la información denominada "IT-Grundschutz" a la especificaciones de la norma ISO/IEC 27001 para apoyar a las autoridades y empresas en materia de seguridad vigente desde el 2006. (Disterer, 2013)

Situación análoga se presenta en Colombia que publica la Norma Técnica Colombiana NTC ISO/IEC 27001 en el 2006, sin carácter de obligatorio para el sector público y privado (“MINISTERIO DE COMUNICACIONES COLOMBIA - Diagnóstico de la situación Actual Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea”). El estado peruano también se ha pronunciado al respecto con la Norma Técnica Peruana NTP ISO/IEC17799. (“NTP ISO IEC 17799 - isoiec17799.pdf”)

En nuestro país a partir del 09 de mayo del 2012 el gobierno central a través del Instituto Ecuatoriano de Normalización INEN registró las normas NTE INEN-ISO/IEC 27001:2011, 27002:2009, 27003, 27004, 27005 y 27006 para estandarizar las tecnologías de información relacionada con la gestión de seguridad de la información, sin embargo aún no son de cumplimiento obligatorio ni para el sector público y ni privado. (Instituto Ecuatoriano de Normalización, 2013)

La norma internacional ISO/IEC 27001:2005 ha sido elaborada para proporcionar las mejores prácticas de la seguridad de la información, define el establecimiento, implementación, operación, seguimiento y revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad

de la Información (SGSI) adoptando el modelo de procesos "Planificar-Hacer-Verificar-Actuar". (PHVA, o en sus siglas en inglés DPCA:Plan-Do-Check-Act) aplicable a todo tipo de organización (ISO 27000, n.d., sec. 2d)

Por otro lado, la International Organization for Standardization ISO informa que 7940 empresas obtuvieron la certificación con el estándar ISO/IEC 27001:2005, de las cuales 229 pertenecen al sector educativo (ISO, 2011). En el ámbito universitario 75 Universidades han culminado el proceso de certificación, 2 Universidades de América, 6 de Europa y 67 de Asia. A nivel Latinoamericano y en Ecuador no existen Universidades certificadas en esta norma. (International Register of ISMS Certificates, 2013)

En el resultados de la encuesta de seguridad de la información del 2011 a 159 Instituciones de Educación Superior (IES), llevada a cabo por la Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES) en México se resalta que el 39% de las IES ha establecido algún plan de seguridad en TI y que el 47% de las instituciones participantes cuentan con certificaciones en estándares de TI o estándares de seguridad en TI, de las cuales 7 Universidades estan alineándose con la norma ISO/IEC 27000. (ANUIES, 2013)

En tal sentido, especialistas en el área y académicos de Universidades han planteado modelos alternativos para gestionar la seguridad de la información en Universidades.

Los académicos de la Universidad Central de Venezuela presentan un modelo para abordar temas de inseguridad de la información, denominado modelo sistémico de la seguridad de la información en las Universidades (MOSSIU) que tiene como base el modelo de Leavitt (1955) desde una perspectiva de organizaciones inteligentes (Viloria & Blanco, Modelo Sistémico de la Seguridad de la Información en las

Universidades, 2009), sin embargo lo plantean como un modelo referencial que puede ser adoptado por cualquier Universidad. La investigación se realizó a través de un estudio longitudinal, con una investigación de campo de tipo exploratoria y técnicas de recolección de datos basadas en observación, entrevistas y encuestas a especialistas de Seguridad de la Información de 11 Universidades venezolanas para la obtención de variables y tendencias del problema. Lo relevante de este modelo es la aplicación de ciclos de aprendizaje de la gestión de seguridad de la información para identificar el grado de madurez respecto a la efectividad y eficiencia del sistema desde un punto de vista sistémico, que parte desde la detección y corrección técnica de un ataque hasta el aprendizaje por parte de la organización. (Viloria, Villegas, & Blanco, La Seguridad de la Información bajo una Perspectiva de la Madurez Organizacional, 2009)

(Villegas, Meza, & Leon , 2011) presentan otro modelo para la gestión de seguridad de la información contextualizado de Colado & Franco (2003), adapta el contexto de acción (¿Para qué?, ¿Qué? y ¿Cómo?) de la seguridad informática a las Universidades para establecer un plan estratégico de seguridad de la información, mediante la indagación del estado de la seguridad de la información en Universidades, revisión de las fuentes de investigación y del análisis de los datos obtenidos; a partir del análisis de la realidad de varias Universidades se construyó un modelo basado en los indicadores y métricas que permiten determinar el modelo de madurez y el desempeño institucional, sin embargo es un modelo referencial que no evidencia aplicabilidad práctica.

En concordancia con los expertos en seguridad de la información de Universidades de Estados Unidos y México se considera que la mitigación de los riesgos en la Universidad se reduce a la gobernabilidad de alto nivel, la gestión de riesgos en la organización, incorporación de tecnologías y políticas de seguridad informática, uso de normas

internacionales y supervisión continua de eventos de seguridad para brindar confianza, crear un ambiente proactivo y asegurar los datos sin descuidar la infraestructura de seguridad. (Global, 2011) (UNAM, 2012)

Para el establecimiento del SGSI la norma ISO/IEC 27001 describe que se debe definir el enfoque organizacional de valoración del riesgo (sección 4.2.1.c) identificando una metodología para valorar el riesgo en la organización y desarrollar criterios para la aceptación del riesgo; identificar los activos, amenazas, vulnerabilidades y los impactos asociados para el negocio (sección 4.2.1.d). Posteriormente, analizar y evaluar los riesgos en función del impacto y la probabilidad de la materialización de una amenaza (sección 4.2.1.e) y finalizar con el plan de tratamiento del riesgo y selección de los controles pertinentes.

En las principales Universidades e instituciones educativas según una publicación de la PMA están marcando una tendencia importante en identificar, valorar, medir los riesgos con el fin de asistir con los recursos y capacidades necesarios para dar tratamiento, reducir y controlar los riesgos con lo que se enfrentan con el fin de tener un adecuado nivel de seguridad de la información y permanecer a un nivel aceptable (“PM157A_D04_WhitePaper_BestPractices_HigherEd_112811.indd - PMA_Education_BestPractices_WhitePaper.pdf”)

En el análisis para mejorar la gestión de los procesos educativos universitarios, expertos en el área infieren que es necesario evaluar y analizar los factores de riesgos asociados a los procesos, elaborar un plan de mejoras, definir y reajustar los indicadores del proceso utilizando el mismo enfoque que la norma ISO/IEC 27001:2005, mejora continua a través de ciclo de Deming, para crear sistemas dinámicos y adaptables a los cambios. (Gimer Torres, Michelena Fernández, & Hernández Rabell, 2010)

En el estudio desarrollado por la Universidad Nacional de Malasia se comprueba que los riesgos más comunes y de mayor impacto en las Universidades son los riesgos financieros, de enseñanza y aprendizaje, estratégico y de reputación (Huber, 2011). El estudio concluye indicando que las mejores oportunidades para la gestión de riesgos de TI se pueden lograr a través de su gestión dentro de un enfoque integrado de la gestión de todos los riesgos de la Universidad, para mantener una uniformidad de criterios e identificar en un modelo macro los riesgos más importantes de las Universidades en todas las áreas, siempre basándose en una norma de general aceptación o marco común como las propuestas por la ISO, como la 9001, 27001 y 30001. (Sayef Sami Hassen, 2013)

En un artículo publicado por la Universidad Simón Bolívar de Venezuela se indican los resultados para conocer las fortalezas y debilidades a las que pudieran estar sometidos los activos de información a cargo del departamento de TI de dicha Universidad. Se apoya en la identificación, valoración y evaluación de los riegos sugeridos en las normas ISO/IEC 27000, apoyados en un método cualitativo de valoración se identifica 8 activos críticos de la información de riesgo mediano o alto, por lo que se sugiere la aplicación de algunos controles establecidos en las normas ISO/IEC 27000, con el fin de sugerir estrategias que minimicen la ocurrencia de posibles amenazas que en la mayoría de los casos explotan las vulnerabilidades organizacionales. (De Freitas, 2009) Concluye recalcando la importancia que tienen las normas ISO/IEC 27000 para el tratamiento de los riegos de toda organización.

Luego de revisar estos antecedentes, los autores del presente proyecto de tesis adoptarán la norma ISO/IEC 27000 como camino para la gestión de la seguridad de la información en la Universidad, determinando la brecha con respecto a la norma ISO 27001: Sistema de Gestión de Seguridad de la Información en relación a los controles de seguridad de la información implementados, luego la siguiente etapa es analizar los

riesgos de seguridad de la información al proceso crítico admisión de estudiantes, para por último generar el plan de tratamiento de riesgos relacionados.

1.1.2 Planteamiento del problema

En la actualidad los delincuentes informáticos han enfocado sus ataques al sector educativo con el objetivo de perpetuar delitos informáticos relacionados con el robo de información, violación de identidad de usuarios, ciberespionaje, afectación a dispositivos móviles y fraudes informáticos usando técnicas como phishing, códigos maliciosos, actividades de malware, entre otros, que en su mayor parte usan servicios de las redes sociales para transportarlos y comprometer los computadores de los usuarios finales. (CSI Computer Security Institute, 2011)

Por otro lado, la liberación en los espacios de enseñanza para facilitar la comunicación, la cooperación y la colaboración en la Educación Superior, la existencia de un alto volumen de tráfico, una gran rotación de estudiantes y la diversidad de dispositivos conectados a las redes universitarias dificultan la adopción y cumplimiento de políticas establecidas en las Universidades creando un entorno de alto riesgo.

En este orden de ideas, los procesos universitarios: académico, investigación, gestión administrativa y vinculación con la sociedad presentan un alto grado de vulnerabilidad que puede comprometer la protección y conservación de la información, especialmente en procesos de investigación, inscripción, matriculación y admisión de estudiantes que utilizan en gran medida datos que son reservados y/o confidenciales.

El proceso de admisión de estudiantes de pregrado de la Universidad tiene como finalidad garantizar la igualdad de oportunidades a todos los aspirantes, evitar la deserción de estudiantes en los años siguientes y

mejorar la calidad académica (Universidad Tecnológica Equinoccial, 2009). Cumplir con lo estipulado en el inciso final de la Transitoria Quinta del Reglamento General a la Ley Orgánica de Educación Superior[1] (Sistema Nacional de Nivelación y Admisión - SNNA, 2013).

Este proceso en la UTE no incorpora lineamientos de seguridad de la información y/o estándares reconocidos a nivel internacional para la ejecución de sus tareas, uso de recursos informáticos, la generación, manejo y custodia de contenidos de los exámenes, evaluación a los aspirantes, procesamiento y análisis de datos, toma decisiones y formulación de resultados.

Existen implementados mecanismos de seguridad informática que intentan reducir los riesgos asociados en el proceso de admisión de estudiantes, sin embargo se han detectado incidentes de seguridad en: la protección de los exámenes, divulgación de preguntas del examen, interrupción de la evaluación a aspirantes por fallas en suministro de energía, versiones de programas y cambios de configuración, explotación de vulnerabilidades técnicas por desconocimiento de los usuarios, inadecuada configuración y mantenimiento de equipos informáticos, falla en los sistemas operativos clientes, presencia de virus, entre otros.

Informalmente se conocen varios riesgos asociados a la confidencialidad, disponibilidad e integridad de la información que pueden afectar al proceso de admisión de estudiantes: modificación de preguntas en el proceso manual de entrega de exámenes desde las áreas académicas hasta el Departamento de Orientación Académica, divulgación de la información relacionada con los contenidos de los exámenes, suplantación de identidades durante la evaluación de exámenes, acceso no autorizado debido al manejo de contraseñas débiles, cambios no

[1] "Las Universidades y escuelas politécnicas podrán realizar un examen de evaluación de conocimientos con fines de exoneración del período de nivelación".

autorizados de la información, interrupciones de servicios informáticos , soporte remoto sin autorización de control de equipos, permisos no adecuados sobre sistemas operativos y red, entre otros.

En este contexto, las autoridades de la Universidad preocupadas por la seguridad de la información en torno al proceso de admisión de estudiantes, necesitan determinar si los controles implementados actualmente son los adecuados para garantizar la confidencialidad, integridad y disponibilidad de los datos, conocer si los activos de información están expuesto a amenazas, las vulnerabilidades que podrían ser aprovechadas por estas amenazas y el impacto y afectación para la institución.

Para lo cual la UTE requiere gestionar adecuadamente la seguridad de la información y establecer un camino para obtener un SGSI basado en una norma internacional y cumplir con lo estipulado en el segundo inciso del artículo 356 de la Constitución de la República, brindar la igualdad de oportunidades a los aspirantes, evitar la deserción de los estudiantes admitidos y aportar confianza a las partes interesadas.

El primer paso para establecer un SGSI según la norma ISO/IEC 27001:2005 es cumplir con el literal 4.2.1.d “identificar los riesgos” sobre los activos de información, el literal 4.2.1.e “Análisis y evaluación de riesgos” para valorar el impacto que tendría en la Universidad, valorar la probabilidad realista de que ocurra una falla de seguridad, estimar los niveles de riesgo y determinar la aceptación del riesgo o la necesidad de su tratamiento y el literal 4.2.1.f “Plan de tratamiento de riesgos” para elaborar el plan de tratamiento de los riesgos priorizado por la Universidad sobre el proceso.

1.1.3 Formulación del problema a resolver

Los cuestionamientos que el proyecto de tesis pretende responder se muestran a continuación:

Conocer los riesgos de seguridad de la información relacionados al proceso de Admisión de estudiantes de Pregrado de la Universidad Tecnológica Equinoccial, relacionados con la elaboración de contenidos de los exámenes, distribución y entrega de las preguntas al departamento encargado del proceso, evaluación de los aspirantes, procesamiento de datos y emisión de resultados

Determinar la efectividad de los controles actuales y los controles de la norma ISO/IEC 27001:2005 se deben aplicar al proceso de Admisión de estudiantes de Pregrado de la UTE para gestionar los riesgos relacionados con las amenazas sobre los activos, vulnerabilidades e impactos de seguridad de la información en la Universidad.

Recomendar las acciones que se requieren para gestionar los riesgos identificados en el proceso de admisión de estudiantes de Pregrado en la UTE y poder alcanzar un Sistema de Gestión de Seguridad de la Información – SGSI acorde a la realidad universitaria.

1.1.4 Justificación

La Universidad Tecnológica Equinoccial considera al proceso de Admisión de estudiantes de vital importancia porque es el primer contacto que la Universidad establece con los aspirantes y por reglamentación interna debe garantizarles la equidad de oportunidades en el ingreso a la Universidad a través de un proceso transparente y seguro. (Universidad Tecnológica Equinoccial, 2009). También, involucra el cumplimiento de

las disposiciones legales en relación a la evaluación de los aspirantes nuevos y aspirantes becados por el gobierno[2].

Las autoridades de la UTE tienen incertidumbre por los incidentes de seguridad de la información del proceso de Admisión de estudiantes de Pregrado del campus Quito modalidad presencial que han ocurrido durante los últimos 6 meses y está preocupada por el grado de vulnerabilidad del proceso, por la efectividad de los controles de seguridad implementados para contrarrestar las posibles amenazas de seguridad y por la protección de la información contra riesgos de pérdida, alteración y divulgación. Considera que la materialización de una amenaza puede afectar negativamente a la Universidad respecto al cumplimiento de los objetivos institucionales, la pérdida de confianza de las partes interesadas, el prestigio institucional y pérdidas económicas.

La Universidad pretende iniciar el camino para implantar un sistema de gestión de seguridad de la información en el campus matriz Quito y posteriormente replicarlo en las Sedes a nivel nacional, que ayude a minimizar los riesgos en la elaboración de exámenes, evaluación a los aspirantes, análisis de datos y ponderaciones requeridas para la toma de decisiones por parte de las autoridades.

En tal razón, para dar solución a lo expuesto se plantea definir los lineamientos generales de carácter obligatorio para la implantación del SGSI y los controles mínimos requeridos para minimizar los riesgos de seguridad de la información asociados al proceso de Admisión de estudiantes de la UTE, de acuerdo a la norma internacional ISO/IEC 27001:2005, mediante la aplicación de la norma de gestión de riesgos NTE INEN-ISO/IEC 27005:2012, la Universidad conocerá los niveles de riesgo del proceso de admisión de estudiantes, los controles adecuados a implementar y disponer del plan de tratamiento a los riesgos (reducir,

[2] Inciso final de la disposición Transitoria Quinta del Reglamento General a la Ley Orgánica de Educación Superior (LOES) (Sistema Nacional de Nivelación y Admisión - SNNA, 2013)

evitar, transferir, aceptar) para minimizar los incidentes de seguridad de la información producidos en la parte técnica y por el factor humano, en temas de confidencialidad, integridad y disponibilidad.

Adicionalmente al finalizar el proyecto, la Universidad contará con el análisis de la brecha para implantar un SGSI acorde con los estándares internacionales, en función de la realidad universitaria que potencialice las fortalezas, transforme las debilidades en oportunidades de mejora y genere una ventaja competitiva en sector universitario, mejorando la confianza de las autoridades acerca de los resultados del proceso de Admisión de Estudiantes para apoyar con el cumplimiento legal exigido por los organismos gubernamentales ecuatorianos.

La ejecución de este proyecto también brindará a las autoridades juicios de valor para la toma de decisiones, a fin de preparar el entorno para como siguiente etapa obtener una certificación internacional ISO/IEC 27001:2005 en el proceso de Admisión de Estudiantes avalada por un organismo legalmente autorizado.

1.2 Objetivo General

Evaluar la seguridad de la información del proceso de admisión de estudiantes de pregrado en la Universidad Tecnológica Equinoccial basado en la norma internacional ISO/IEC 27000 en la ciudad de Quito para determinar el nivel de seguridad y elaborar un plan de tratamiento de riesgos que permita dar respuesta a los riesgos de seguridad de la información asociados a este proceso.

1.3 Objetivos Específicos

Determinar el nivel de riesgo de seguridad de la información del proceso de Admisión en la UTE de acuerdo con la norma ISO/IEC 27005:2011

Determinar la brecha respecto a los requerimientos del estándar ISO/IEC 27001:2005 para el proceso de Admisión de estudiantes en la Universidad Tecnológica Equinoccial.

Elaborar un plan de tratamiento de riesgos para cubrir los puntos de mayor prioridad de la Universidad sobre este proceso.

1.4 Alcance

El presente proyecto estará enfocado exclusivamente en la evaluación del proceso de Admisión de estudiantes para las carreras de Pregrado, campus Matriz Quito, modalidad Educación Presencial y Distancia, no incluye al proceso de admisión de Posgrado, proceso de matrícula y nivelación de estudiantes.

No se evaluará los procesos y sistemas de apoyo de otros procesos relacionados al proceso de Admisión de Estudiantes, por ejemplo: académico, financiero, contable, recursos humanos, gestión de biblioteca, acreditación, planificación estratégica, investigación, vinculación con la colectividad, y los demás procesos universitarios.

Para elaborar la tesis se utilizará la norma ISO/IEC 27001:2005, permitirá determinar la brecha de la situación actual de la UTE con los requisitos obligatorios y controles mínimos requeridos para implementar un SGSI relacionados al proceso de admisión de estudiantes.

En conformidad con la norma ISO/IEC 27001:2005, en el literal “4.2.1.d” se identificará los activos de información del proceso y en el literal “4.2.1.e” se realizará el análisis y la valoración del impacto que tendría en la Universidad, la probabilidad de que ocurra una falla de seguridad y la estimación de los niveles de riesgo relacionados al proceso de Admisión de Estudiantes.

Posteriormente, se presentará a la Universidad un plan de tratamiento de riesgos de este proceso, con las recomendaciones necesarias para mitigar los riesgos encontrados durante la evaluación.

La aprobación del plan de tratamiento de riesgos no está considerada en el alcance de este proyecto, en lo posterior la Universidad debe realizar un plan de implementación del plan de tratamiento de riesgos.

CAPÍTULO 2

2 MARCO TEÓRICO

2.1 Desarrollo de la Universidad en América Latina

2.1.1 Siglo XIX: la herencia en la Universidad

(Brunner, 1990) Antes de las independencias de las naciones de América, la Universidad europea se multiplicó y consolidó sus tradiciones, mientras que en el nuevo mundo se quedó rezagado su avance y desarrollo. Durante el siglo XIX se producen varios procesos de clausuras y aperturas de varias Universidades debido a una crisis en varias de estas instituciones latinoamericanas, así mismo se producen cambios que se ajustan a la realidad de la sociedad dentro de una visión adaptada a las exigencias de la nueva sociedad industrial, urbana y nacional.

En 1843 se crea un nuevo modelo que tiene como característica ser una prolongación del estado y tener una estrecha relación con el Gobierno, entre las premisas más importantes está que la Universidad debe servir como órgano educativo de la nación, llegando a todos los ciudadanos hasta el nivel más elemental, con el fin de crear una base local de conocimientos científicos, humanísticos y literarios.

A pesar de que las Universidades del siglo XIX difieren de los sistemas modernos de Educación Superior, se crearon las bases institucionales de éstos, por ejemplo nace la Universidad de Buenos Aires (1821), la Universidad de Caracas deja de ser pontificia y se convierte en la Universidad Central de Venezuela (1826), y en el mismo año la Universidad Santo Tomás de Aquino pasa a ser la Universidad Central del Ecuador. En 1842 se crea la Universidad de Chile en Santiago y en Montevideo la Universidad de Uruguay que empieza a funcionar en 1860. En 1889 se crea la Universidad Nacional de Asunción. En México luego

de la independencia la vieja Universidad colonial es reabierta y cerrada varias veces, llegando a consolidarse en 1910. Durante ese tiempo el nacimiento de las Universidades es lento, esporádico y se han frustran varios intentos de reformar la Universidad hasta que en 1918 la rebelión estudiantil en Argentina marca un quiebre que luego se diseminó a toda América Latina en contra del autoritarismo presente en esa época y las estructuras caducas coloniales, a favor de instaurar un modelo vanguardista, libertaria, ilustrada, urbana, científica y racionalista. Entre los logros obtenidos se instaura el cogobierno estudiantil y la participación estudiantil en la conducción de materias universitarias, así como la docencia libre, permitiendo que toda persona con competencia comprobada, título profesional habilitante, que tenga obras y publicaciones o especialización en un área del conocimiento, pueda solicitar al consejo Universitario su admisión como profesor libre para impartir cátedra. Con estas acciones se desencadena una serie de acontecimientos que reforman la Universidad en América Latina, y más tarde se dan fenómenos como la masificación universitaria, la diferenciación y diversificación, y la profesionalización y ampliación del cuerpo académico.

El movimiento de estudiantes en Córdoba (Argentina) no solo tuvo importancia en el régimen educacional sino también en el político-cultural que se contrastaron con la opresión del poder de los gobiernos y poder militar en toda Latinoamérica aplastando las conquistas logradas y reprimiendo los movimientos estudiantiles. A lo largo del tiempo hasta nuestros días bajo la presión de procesos menos visibles existen una serie de cambios en las Universidades que han tenido una mayor incidencia institucional afectando a la estructura misma de la Universidad y su organización, como la distribución real de autoridad y de sus influencias, los programas y métodos pedagógicos, las relaciones con la sociedad, entre otros.

El panorama común es que hasta 1950 en América Latina el crecimiento de Universidades es pobre siendo tan solo 75 Universidades y la gran mayoría son de carácter público o dependían en gran medida del Estado para su desarrollo. Eran poco diversificadas y había una hegemonía en las instituciones que se habían ganado un buen nombre relegando otras como de nivel inferior. Así mismo la escolaridad es reducida hasta esas fechas siendo la matrícula regional de 266 mil alumnos, que representaban tan solo el 1,9% del grupo de jóvenes entre 20 y 24 años quienes tenían acceso a la Educación Superior (siendo la gran mayoría hombres).

Posteriormente se producen nuevamente cambios significativos en las Universidades para atender tanto la multiplicación de la escolarización, la especialización y atención a las demandas de la sociedad, pasando de ser entidades simples a organizaciones complejas y las Universidades ya no solo públicas sino también privadas.

2.1.1.1 Sistemas de educación contemporáneos y sus emergencias

(Brunner, 1990) Durante los periodos comprendidos entre 1950 y 1975 se configuran los actuales sistemas nacionales de Educación Superior, caracterizándose por ser altamente diferenciados a través de establecimientos diversos ofreciendo servicios masivos de enseñanza superior. Se amplía considerablemente el cuerpo docente y el número de investigadores. Se produce un proceso de diferenciación y surgen múltiples grupos con identidades específicas e intereses propios. Dichos sistemas alcanzan una gran autonomía funcional dentro de la sociedad y sus relaciones con el gobierno, sistema político, economía y población se han vuelto más estrechas, cambiantes y complicadas.

Las acciones están enfocadas a proveer de los profesionales con los conocimientos adecuados para abordar los problemas de desarrollo,

reduciendo la brecha científico-tecnológica, y principalmente elevando la calidad de los servicios distribuyéndolos de forma más equitativa a todas las clases sociales.

En cuestión de poco tiempo las Universidades se vieron abarrotadas de estudiantes provocando aglomeraciones sin ningún orden aparente, tomando cursos con nombres peculiares para su titulación en carreras que no aseguraban un acceso seguro al mercado laboral. Con tales precedentes se produce un detrimento considerable en la calidad de la Educación Superior en general y el Estado debe tratar de resolver problemas relacionados con el acceso, la equidad, la calidad misma, el financiamiento, la acreditación, la coordinación, control y evaluación. Todo esto creó un ambiente de desconfianza entre el gobierno y las Universidades, lo que condujo a cierres de establecimientos y tiempos de inestabilidad en la adaptación.

2.1.2 Retos y gestión de la calidad en la Educación Superior en América Latina

(Gazzola & Didriksson, 2008) La complejidad de la Educación Superior en América Latina, se plasma en una serie de tendencias históricas y emergentes, para construir un nuevo escenario que permita mejorar sustancialmente los niveles de vida para sus poblaciones, y brinde la posibilidad de un mayor bienestar, democracia e igualdad desde la ciencia, la educación y la cultura.

Los cambios más destacados en la Educación Superior en América Latina se han caracterizado por:

- Un incremento importante en el número de Universidades no solo públicas sino mayormente de carácter privado, con sistemas de educación complejos, heterogéneos, segmentados socialmente y diversificados;

- La masificación de la demanda social por Educación Superior;
- La comercialización y mercantilización de las escuelas privadas;
- El impacto de las nuevas tecnologías;
- El desarrollo de nuevas áreas de conocimiento de base interdisciplinaria;
- La contracción rigurosa de los recursos financieros provistos por los gobiernos y la instauración de mecanismos de evaluación, de rendición de cuentas, de aparatos de acreditación que valoran el desempeño de instituciones, de programas y de personas;
- La importancia que está adquiriendo la internacionalización de los procesos de aprendizaje, el surgimiento de nuevas redes y asociaciones académicas;
- La movilidad de estudiantes y los nuevos procesos de transferencia y gestión de los conocimientos.

Además se deben tomar en cuenta los cambios en las instituciones de Educación Superior relacionados directamente con el nivel de desarrollo e innovación de los principales componentes de la ciencia y tecnología, siendo el impacto de las nuevas tecnologías de la información lo que ha permitido redefinir los espacios de aprendizaje generando nuevos modelos de formación, auto-formación, aprendizaje e innovación dentro de la sociedad moderna.

Con los antecedentes descritos se logra entender que a lo largo de la historia y desde su creación la Universidad latinoamericana ha sido influenciada por modelos exteriores, tanto europeos como norteamericanos, para llegar a los sistemas actuales que se rigen por modelos de gestión de la calidad de la educación y las medidas adoptadas para afrontar los retos a los cuales se enfrenta la Universidad actualmente.

(Gazzola & Didriksson, 2008) Por tal motivo para contrarrestar estos fenómenos se establecieron una serie de reacciones de las naciones en favor de tomar medidas que garanticen el correcto desenvolvimiento del aprendizaje en la Educación Superior, para lo cual se han desarrollado modelos de aseguramiento de la calidad de la educación, se han creado e instituido organismos regionales que regulen los parámetros básicos que las Universidades deben cumplir para garantizar la calidad en la Educación Superior, también se han llevado a cabo acuerdos y convenios multinacionales y finalmente se han establecido organizaciones de regulación y control a nivel de cada país.

Entre los principales organismos latinoamericanos y programas de regulación y control se puede citar:

- El sistema de acreditación ARCU-SUR: El mecanismo de acreditación Mercosur se inició en 1998, con la suscripción por parte de los ministros de educación de Argentina, Brasil, Paraguay y Uruguay, como miembros plenos, y Bolivia y Chile como asociados.
- En Centroamérica, a partir de 1998, con el apoyo de la cooperación alemana, se desarrolló un ambicioso programa destinado a instalar procesos de aseguramiento de la calidad. El programa, denominado SICEVAES (Sistema Centroamericano de Evaluación y Acreditación de la Educación Superior) tuvo un fuerte impacto, principalmente en las Universidades públicas de la región, a través de la generación y aplicación de criterios en múltiples procesos de autoevaluación y evaluación externa.
- En 2003 se constituyó en Buenos Aires la Red Iberoamericana para la Acreditación de la Calidad de la Educación Superior, RIACES, que agrupa a agencias de aseguramiento de la calidad, a organismos de gobierno responsables de la gestión y la calidad de los sistemas de Educación Superior y a asociaciones nacionales y regionales de

instituciones de Educación Superior. Este organismo cuenta con el respaldo de la UNESCO y del Banco Mundial.

En las páginas 34 a 38 del texto “Aseguramiento de la calidad en Iberoamérica” se pueden consultar los organismos de Evaluación y Acreditación de Colombia, Chile, México y Argentina, que son países que ya tienen sistemas establecidos que se consideran como referentes en la región y sirven de modelo para los países que están iniciando en este proceso como es el caso de Ecuador. El estado de los sistemas de aseguramiento de la calidad de Educación Superior de varios países de Iberoamérica de gran influencia se ilustra en la Cuadro 1 junto con el estado de los sistemas de los países que están iniciando este proceso de mejoramiento.

Cuadro 1: Descripción general del estado de la Evaluación y Acreditación de la Educación Superior en América Latina, España, Bélgica, Italia y Portugal

(CINDA, 2012)

Descripción general

	Sistema de Aseguramiento de la Calidad	Habitantes (2010/11)	PIB per cápita (2010)	Índice De Desarrollo Humano (PNUD – 2010/11)		Nć IES (Todas)	Nć IES Universitarias	Gasto público en Educación Superior	% población con <2USD-PPP x día
ARGENTINA	Si	40.091.359	15.200	0,78	Alto	2.205	113	0,9%	11,3
CHILE	Si	17.248.450	15.200	0,78	Alto	177	60	0,3%	2,4
COLOMBIA	Si	46.050.630	9.683	0,69	Alto	292	80	1,1%	27,9
COSTA RICA	Si	4.615.518	7.851	0,73	Alto	80	56	1,2%	8,6
ESPAÑA	Si	47.021.031	30.400	0,86	Muy Alto	5.315	78	1,1%	**
MÉXICO	Si	112.336.538	14.115	0,75	Alto	2.573	2571	0,5%	4,8
PORTUGAL	Si	10.623.000	21.473	0,80	Muy Alto	146	59	0,9%	**
BELGICA	En fase inicial	10.839.905	37.624	0,87	Muy Alto	-	-	1,1%	-
BRASIL	En fase inicial	190.732.694	11.019	0,72	Alto	2.314	186	0,8%	12,7
ECUADOR	En fase inicial	14.483.499	8.400	0,72	Alto	72	61	-	12,8
PANAMA	En fase inicial	3.405.813	13.438	0,77	Alto	50	39	0,9%	17,8
PARAGUAY	En fase inicial	6.530.000	5.176	0,67	Medio	89	52	0,8%	14,2
PERU	En fase inicial	29.797.694	9.335	0,73	Alto	1.120	100	0,4%	18,5
URUGUAY	En fase inicial	3.368.595	13.988	0,87	Alto	18	5	0,6%	4,2
BOLIVIA	En proceso	10.426.160	4.800	0,66	Medio	816	85	1,5%	30,3
ITALIA	En proceso	60.626.442	31.027	0,85	Muy Alto	109	89	0,6%	-
VENEZUELA	En proceso	29.450.000	12.374	0,74	Alto	170	58	1,6%	10,2

2.1.3 Ecuador: Primeros pasos para la Gestión de Calidad en la Educación Superior

(CINDA, 2012) El Ecuador se encuentra en un proceso de modificación de su sistema de Aseguramiento de la Calidad. Anteriormente, el organismo encargado de esta labor fue el Consejo Nacional de Evaluación y Acreditación de la Educación Superior (CONEA), el cual diseñó instrumentos técnicos así como la normatividad para la evaluación en las Instituciones de Educación Superior.

Posteriormente, en el año 2011 es reemplazado por el CEAACES (Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior del Ecuador), cuya finalidad esencial es el mejoramiento de la calidad académica y de gestión de las Universidades, escuelas politécnicas e institutos superiores técnicos y tecnológicos del país, a través de los procesos de autoevaluación institucional, evaluación externa y acreditación. El CEAACES trabaja en coordinación con el Consejo de Educación Superior (CES) del Ecuador, y tiene facultades regulatoria y de gestión.

(CINDA, 2012) El CEAACES, es el único organismo facultado para conferir la acreditación, como certificar oficialmente una institución, carrera, programa o unidad académica del Sistema Nacional de Educación Superior.

Con el fin de aterrizar las funciones de estos organismos se han desarrollado y establecido reformas a la Ley de Educación Superior (LOES) y su respectivo reglamento para cumplir con los derechos y deberes establecidos en la Constitución de la República del Ecuador del 2008.

2.2 Sistemas de Admisión y Nivelación

La Educación Superior ha sufrido varias transformaciones complejas debido a los factores influyentes descritos anteriormente, pero para el presente caso de estudio en función del alcance y el proceso que se desea evaluar con este trabajo se analizará el desarrollo de los Sistemas de Admisión y Nivelación en Latinoamericana ya que ha sido una de las estrategias comúnmente adoptadas por varios países en la región.

Los Sistemas de Admisión y Nivelación nacen fundamentalmente debido al aumento de la demanda de estudiantes, producto de la desvalorización de las certificaciones educativas y la jerarquización de los conocimientos especializados, sumado a la exigencia social y política de democratizar la Universidad bajo la premisa de brindar igualdad de oportunidades para todos los ciudadanos y aspirantes provenientes de los sectores populares, que con frecuencia a lo largo de la historia han sido excluidos. Así mismo otros factores que han sido de consideración para la creación de Sistemas de Admisión y Nivelación son la explosión de la privatización de la Educación Superior, debida al desfinanciamiento de la Universidad pública, así como la facilidad e incentivos para la oferta educativa privada y la operación mediante una forma transaccional bajo un formato preponderantemente mercantil. (SEMPLADES , 2008)

2.2.1 Datos estadísticos de implementación de Sistemas de Admisión y Nivelación para ingresos a la Universidad

(SEMPLADES , 2008) La masificación se ha dado en un nivel de crecimiento sin precedentes antes experimentados, y varios estudios han cuantificado esta tendencia. Se habla de que la matrícula en la Educación Superior mundial ha aumentado de 92 a 132 millones entre 1999 y 2004. Así mismo en américa Latina la matrícula total ha pasado de 1’219.730 de

estudiantes en 2001 a 18’595.322 en 2008, aumentando en un 50% a principios de este nuevo milenio.

En relación al número total de establecimientos de Educación Superior en 1960 se tiene datos de 164 instituciones de las cuales el 31% eran privadas, y para el periodo de 2000-2003 se incrementó a 7.514, de las cuales el 65% son privadas, y en un informe del Centro Interuniversitario de Desarrollo, CINDA, al año 2007 indica que existían más de 10.000 establecimientos de Educación Superior.

(SEMPLADES , 2008) Otro cambio que se ha presentado es la diversificación del alumnado en términos culturales y socio-económicos, ya que tradicionalmente se suponía una cierta homogeneidad en estos términos. Ahora se tienen variedad de estudiantes étnicamente diferentes pertenecientes a diferentes culturas por lo que se debe asumir una nueva forma de producir y transmitir conocimientos.

(SEMPLADES , 2008) Por tales situaciones las instituciones educativas han implementado soluciones variadas para abordar el problema del acceso a la Educación Superior en temas de la masificación, por ejemplo: cobro de aranceles, implementación de aranceles diferenciados, exámenes de ingreso, cupos por carreras, pruebas de aptitud, créditos educativos y creación de nuevas carreras o promoción de las que tienen una baja demanda, entre otros.

Pero estas medidas en América Latina no han sido establecidas siempre, de manera específica y clara, como políticas de admisión o mecanismos de regulación para el ingreso a las instituciones de Educación Superior, menos aún en instancias de nivelación. Por lo que se tiene diferentes medidas según la institución para garantizar la calidad y equidad en la Educación Superior.

Para garantizar la equidad se debería establecer el acceso libre e irrestricto, pero eso impone otros desafíos para lograr eficiencia del

sistema, ya que se presentan problemas relacionados con el porcentaje de alumnos que terminan sus estudios a tiempo siendo tan solo el 43% en un periodo normal. Así como la deserción que alcanza el 57% en el entorno global de Latinoamérica, por lo que no solo se debe contar con un mecanismo de ingreso sino de acompañamiento de los estudiantes a lo largo de su carrera. También pueden mantenerse prácticas de exclusión que atenten con la equidad debido a la preparación en la etapa secundaria o dificultades socio-económicas.

Con respecto a la calidad, se favorecería a los estudiantes con una buena educación inicial, básica y media si solo se establecen políticas que privilegien el mérito académico.

Por tales motivos los principios de equidad y calidad en la aplicación de políticas de admisión y nivelación exigen un tratamiento articulado y complementario, siendo el objetivo principal de los sistemas de Sistemas de Admisión y Nivelación adoptados por cada uno de los países de América Latina que han optado por esta medida.

2.2.2 Políticas de Admisión y Nivelación en el Ecuador

(SEMPLADES , 2008) A lo largo de la historia del Ecuador se han presentado diversas características respecto a la aplicación de políticas de admisión y nivelación. Al inicio luego de la independencia, las políticas de admisión estaban vinculadas a exámenes de ingreso de diferentes materias. Luego en 1874 se crea una escuela para nivelar a los bachilleres que deseaban ingresar a la Escuela Politécnica Nacional.

En el año de 1937, en la LOES se establecen los requisitos básicos para el ingreso a la Universidad, siendo tener al menos 18 años, haber completado la educación secundaria, tener buena conducta y aprobar un examen preliminar de aptitud psicofísica para estudios superiores. Luego en 1938 se expide una nueva ley que añade haber cumplido las

obligaciones militares y cumplir con los requisitos de los reglamentos y estatutos universitarios. En el año 1964 se publica la Ley Orgánica de Educación Superior que mantiene los requisitos de 1938 y añade haber pagado los derechos fijados por esta ley y reglamentos, aprobar los cursos propedéuticos o exámenes de ingreso, y se dispone la creación de departamentos de Orientación Vocacional. Requisitos que se mantienen en las leyes de 1965, 1966 y 1971.

A principios de los años setenta se desarrolló un movimiento de reforma universitaria, que consideraba discriminatorio el examen de ingreso a las Universidades públicas, y terminó imponiéndose en acceso libre frente a otros planteamientos reformistas. Luego en 1998 se establece por mandato constitucional que solo puedan ingresar a las Universidades y escuelas politécnicas quienes cumplan con los requisitos del Sistema Nacional Obligatorio de Admisión y Nivelación, nunca se cumplió a cabalidad por las instituciones de Educación Superior ya que mantenían mecanismos y requisitos diferentes.

Con la reforma constitucional de 2008 se declara la gratuidad para la educación hasta tercer nivel y mediante la expedición de la Ley Orgánica de Educación Superior en 2010 se establece un Sistema Nacional de Admisión y Nivelación que establece la recepción de un examen de ingreso a todos los aspirantes para las Universidades públicas del Ecuador.

2.2.3 Fundamentación Legal

Constitución del 2008: Gratuidad de la Educación y Sistema de Nivelación y Admisión

Luego de una serie de encuentros integrados por varios actores de la Educación Superior de la sociedad ecuatoriana y expertos de otros países de Latinoamérica respecto a los sistemas de admisión y nivelación se

desarrollaron 15 acuerdos básicos, fueron presentados a la Asamblea Constituyente para ser incluidos en la Constitución del 2008. Los artículos y secciones fundamentales incluidos en la Constitución, respecto a la admisión y nivelación se detallan a continuación:

Art. 348.- La educación pública será gratuita y el Estado la financiará de manera oportuna, regular y suficiente. La distribución de los recursos destinados a la educación se regirá por criterios de equidad social, poblacional y territorial, entre otros…

Art. 353.- El sistema de Educación Superior se regirá por:

Un organismo público de planificación, regulación y coordinación interna del sistema y de la relación entre sus distintos actores con la Función Ejecutiva.

Un organismo público técnico de acreditación y aseguramiento de localidad de instituciones, carreras y programas, que no podrá conformarse por representantes de las instituciones objeto de regulación.

Y principalmente:

Art. 356.- La Educación Superior pública será gratuita hasta el tercer nivel.

El ingreso a las instituciones públicas de Educación Superior se regulará a través de un sistema de nivelación y admisión, definido en la ley. La gratuidad se vinculará a la responsabilidad académica de las estudiantes y los estudiantes.

Con independencia de su carácter público o particular, se garantiza la igualdad de oportunidades en el acceso, en la permanencia, y en la movilidad y en el egreso, con excepción del cobro de aranceles en la educación particular.

El cobro de aranceles en la Educación Superior particular contará con mecanismos tales como becas, créditos, cuotas de ingreso u otros que permitan la integración y equidad social en sus múltiples dimensiones.

LOES: ¿Qué dice acerca de la Admisión y Nivelación?

En octubre del 2010 se publica la Ley Orgánica de Educación Superior, que en relación al tema de estudio establece:

Art. 12.- Principios del Sistema.- El Sistema de Educación Superior se regirá por los principios de autonomía responsable, cogobierno, igualdad de oportunidades, calidad, pertinencia, integralidad y autodeterminación para la producción del pensamiento y conocimiento en el marco del diálogo de saberes, pensamiento universal y producción científica tecnológica global.

Art. 81.- Sistema de Nivelación y Admisión.- El ingreso a las instituciones de Educación Superior públicas estará regulado a través del Sistema de Nivelación y Admisión, al que se someterán todos los y las estudiantes aspirantes.

Para el diseño de este Sistema, la Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT) coordinará con el Ministerio de Educación lo relativo a la articulación entre el nivel bachiller o su equivalente y la Educación Superior pública, y consultará a los organismos establecidos por la Ley para el efecto.

El componente de nivelación del sistema se someterá a evaluaciones quinquenales con el objeto de determinar su pertinencia y/o necesidad de continuidad, en función de los logros obtenidos en el mejoramiento de la calidad de la educación bachiller o su equivalente.

2.3 Seguridad de la información

2.3.1 Desafíos de la seguridad de la información en el sector universitario

(Silvio, 2000) Varios autores coinciden que la sociedad está viviendo en la era de la información debido principalmente al desarrollo de la informática y la telemática, siendo entonces la información la materia prima de la producción en un mundo globalizado, del conocimiento y el tratamiento de los datos para identificar oportunidades, camino hacia la denominada “sociedad del conocimiento”.

Los adelantos tecnológicos históricamente han generado desigualdades y el desarrollo del internet y la informática no es una excepción, ya que ha dotado de mayor velocidad de cambio, innovación y diversidad de utilidades y aplicaciones a los seres humanos que cualquier otro invento en toda la historia, pero a su vez estos han sido aprovechados en mayor medida por los países más desarrollados, cambiando muchos de los paradigmas establecidos tradicionalmente e imponiendo ciertos modelos. La evolución vertiginosa de las redes de computadoras, informática, la telemática, el internet, han modificado varios aspectos de la sociedad y el ¿cómo hacer las cosas? por ejemplo la compra-venta por internet, las redes sociales, las transacciones online, los sitios web de difusión de medios audiovisuales, las telecomunicaciones y en general las organizaciones públicas y privadas, y naturalmente no se podía quedar fuera el involucramiento respecto a la Educación Superior.

La sociedad está rodeada de equipos y productos que procesan, almacenan y transmiten la información, con una gran tasa de penetración en todos los sectores sociales. Consecuencia de ello la seguridad de la información juega un papel de crucial relevancia, que cada vez preocupa más a las empresas, gobiernos, organismos públicos y privados, y a la

sociedad en general, consideran que una inadecuada protección de uno de sus activos más valiosos - la información – les podría llevar a tener graves consecuencias para su devenir.

(Elisabete Piresa, 2012) No siendo ajena la Educación Superior a la inserción de las nuevas tecnologías de la información y comunicación éstas se han involucrado en el ámbito universitario posibilitando tener sistemas que manejan información de uso transversal abarcando actividades de enseñanza académica y no académicas, ofreciendo oportunidades y beneficios pero a su vez exponiendo a todos los involucrados a los riesgos asociados.

Sin embargo, debido al precepto de ser lo más abierto posible para facilitar la comunicación, la cooperación y la colaboración en la Educación Superior, las Universidades implantan infraestructuras TI que soporten miles de dispositivos de diferentes marcas y modelos, un alto volumen de tráfico y el uso de datos personales, en donde se genera un entorno vulnerable de alto riesgo que puede afectar a la información y se enfrentan a una serie de desafíos de seguridad en TI, como por ejemplo:

- Las Universidades tienen miles de nuevos usuarios en sus redes todos los años e igual número de usuarios que están de salida.
- Soportan casi todo tipo de dispositivos disponibles, y pugnan con una población joven que es mucho más propensa a involucrarse en conductas de riesgo en línea. A menudo tienen organizaciones descentralizadas de TI, lo que dificulta la implementación de tecnologías estándar, o la adopción y cumplimiento de políticas estándares". (Bel Ibérica Soluciones de Seguridad Global, 2011)

Rodney J. Petersen, oficial de relaciones gubernamentales de alto nivel en EDUCAUSE indica que la mitigación de los riesgos, hoy en día se reduce a la gobernabilidad de alto nivel y la gestión de riesgos, entonces los líderes de seguridad de TI en la Educación Superior deberían

establecer estrategias hacia la búsqueda de soluciones mediante la elevación de la seguridad al nivel ejecutivo de gestión de riesgos, donde se puede evaluar el riesgo, asignar diferentes niveles de acceso de seguridad, y desarrollar las políticas de usuarios que trabajen con las garantías basadas en la tecnología que se despliegan. (Bel Ibérica Soluciones de Seguridad Global, 2011)

Según Jinx P. Walton, director de servicios de computación y desarrollo de sistemas en la Universidad de Pittsburgh, las Universidades deben establecer un modelo de seguridad por capas, donde se combinen herramientas (detección de intrusos, antivirus, etc.), procesos y la educación, "incorporando una serie de tecnologías y políticas que son estándares en la seguridad informática" mediante estrategias más avanzadas para mantener los datos de la Universidad y la infraestructura de seguridad. (Bel Ibérica Soluciones de Seguridad Global, 2011)

Tammy Clark, directora de seguridad de información en Georgia State University en Atlanta (una de las primeras instituciones de Educación Superior que adoptó la serie de normas ISO 27000 para la seguridad de la información), señala "que ha adoptado un enfoque que involucra a personas, procesos y tecnología, sin excepción, "la gestión se centra en la mejora de su arquitectura y la capacitación de sus empleados del centro de datos para supervisar los informes procedentes del software de seguridad de la escuela, y para manejar las respuestas de primer nivel de incidencia, independientemente de cuándo los hackers lanzan sus ataques". (Bel Ibérica Soluciones de Seguridad Global, 2011)

Según Jon Allen oficial de seguridad de la Universidad de Baylor en Waco - Texas, el enfoque está cambiando desde dispositivos a los datos, ahora se da mayor importancia a los datos en sí, sin descuidar la utilización de firewalls y herramientas anti-malware que protegen equipos finales, buscando envolver la seguridad alrededor de los datos, mediante una

clasificación de los datos, y asignación de niveles escalables de seguridad que se quedan con ellos mientras viajan. (Bel Ibérica Soluciones de Seguridad Global, 2011)

Entonces resulta que las instituciones educativas alojan un tesoro de información para los Hackers que pueden ir desde registros de recursos humanos y archivos referentes a los estudiantes, datos de investigaciones desarrolladas y en desarrollo, mayoría los cuales son propietarios, se almacenan datos financieros, tales como números de tarjetas de crédito de los estudiantes, ex alumnos, padres y visitantes. En algunos casos, tienen almacenados datos y registros médicos. Otros aspectos atractivos para los atacantes son los vastos y poderosos sistemas informáticos que mantienen las Universidades y la infraestructura que podrían utilizarse para sus propios fines. (BELT, n.d.)

Según un análisis realizado por la empresa de seguridad norteamericana denominada Application Security Inc., entre el año 2005 y 2011 se han producido 435 infracciones a la seguridad de información que afectaron a 8,5 millones de archivos en las instituciones de Educación Superior de los Estados Unidos, año en que la Privacy Rights Clearinghouse y otras organizaciones comenzaron a registrar estos eventos. Se indica también que entre el año 2009 a 2010 se registraron 60 eventos relacionados con el robo de 93000 registros de las bases de datos de algunas instituciones de Educación Superior en Estados Unidos, y según Ponemon Institute estos registros tiene un valor promedio aproximado de pérdida de $204 para las Universidades, lo que representaría un perjuicio de alrededor de $18`972.000. (BELT, n.d.)

2.3.2 Introducción a la seguridad de la información

Los requerimientos en la seguridad de la información de las organizaciones han sufrido dos cambios importantes en las últimas décadas, antes de la expansión del procesamiento de datos, la

información considerada valiosa para una organización utilizaba medios físicos para su protección y medios administrativos como procedimientos de protección de datos del personal durante el proceso de contratación. (Stallings, 2003)

El segundo cambio que afectó a la seguridad de la información se da con la introducción de las redes de computadores y los sistemas distribuidos, ya que se deben considerar medidas de seguridad que garanticen la confiabilidad y autenticidad de los datos en la transmisión en este nuevo medio.

Todo este nuevo estilo de vida se ha desarrollado función del avance de las nuevas Tecnologías de la Información y Comunicación (TICs), del desarrollo computacional y de las telecomunicaciones, de las redes de información, de la introducción de los dispositivos móviles e inteligentes, y su el ámbito de acción se ha introducido en cualquier sector de sociedad, sea productivo, financiero, de gobierno, educacional, etc.

En la actual era digital, la sociedad está rodeada de equipos y productos que procesan, almacenan y transmiten la información de diferente índole a una gran velocidad, el aspecto de la Seguridad de la Información juega un papel de crucial relevancia, que cada vez preocupa a las empresas, gobiernos, organismos públicos y privados, y a la sociedad en general, que consideran que una inadecuada protección de uno de sus activos más valiosos - la información – les podría llevar a tener graves consecuencias para su devenir.

La seguridad en los sistemas de información y de cómputo se ha convertido en uno de los problemas más grandes desde la aparición y globalización de Internet. Dada la potencialidad de esta herramienta y de sus innumerables aplicaciones, cada vez más personas y más empresas sienten la necesidad de conectarse a este *ciberespacio*.

Las Universidades han ido incorporando sistemas informáticos para el apoyo en actividades de enseñanza académica y no académicas, ofreciendo oportunidades y beneficios, y que manejan información de uso transversal a la institución están también expuestas a los riesgos que amenazan la seguridad de la información asociados (Pires & Moreira, 2012).

Además se debe considerar que las Instituciones de Educación Superior alojan un tesoro de información para los *Hackers*, ya que se almacenan que van desde registros de recursos humanos y archivos referentes a los estudiantes, datos de investigaciones desarrolladas y en desarrollo, mayoría los cuales son propietarios, se almacenan datos financieros, tales como números de tarjetas de crédito de los estudiantes, ex alumnos, padres y visitantes. En muchas Universidades se tiene centros de enfermería y por lo general se tienen almacenados datos y registros médicos. Otros aspectos atractivos para los atacantes son los vastos y poderosos sistemas informáticos que mantienen las Universidades y la infraestructura que podrían utilizarse para sus propios fines (BELT, n.d.). En tal sentido se han venido dando varios esfuerzos por parte de las Universidades en favor de proteger estos activos de información. Para ayudar a concebir los aspectos más relevantes concernientes a la seguridad de la información en el presente Marco Teórico se toma como referencia un mapa mental ilustrado en la Figura 1.

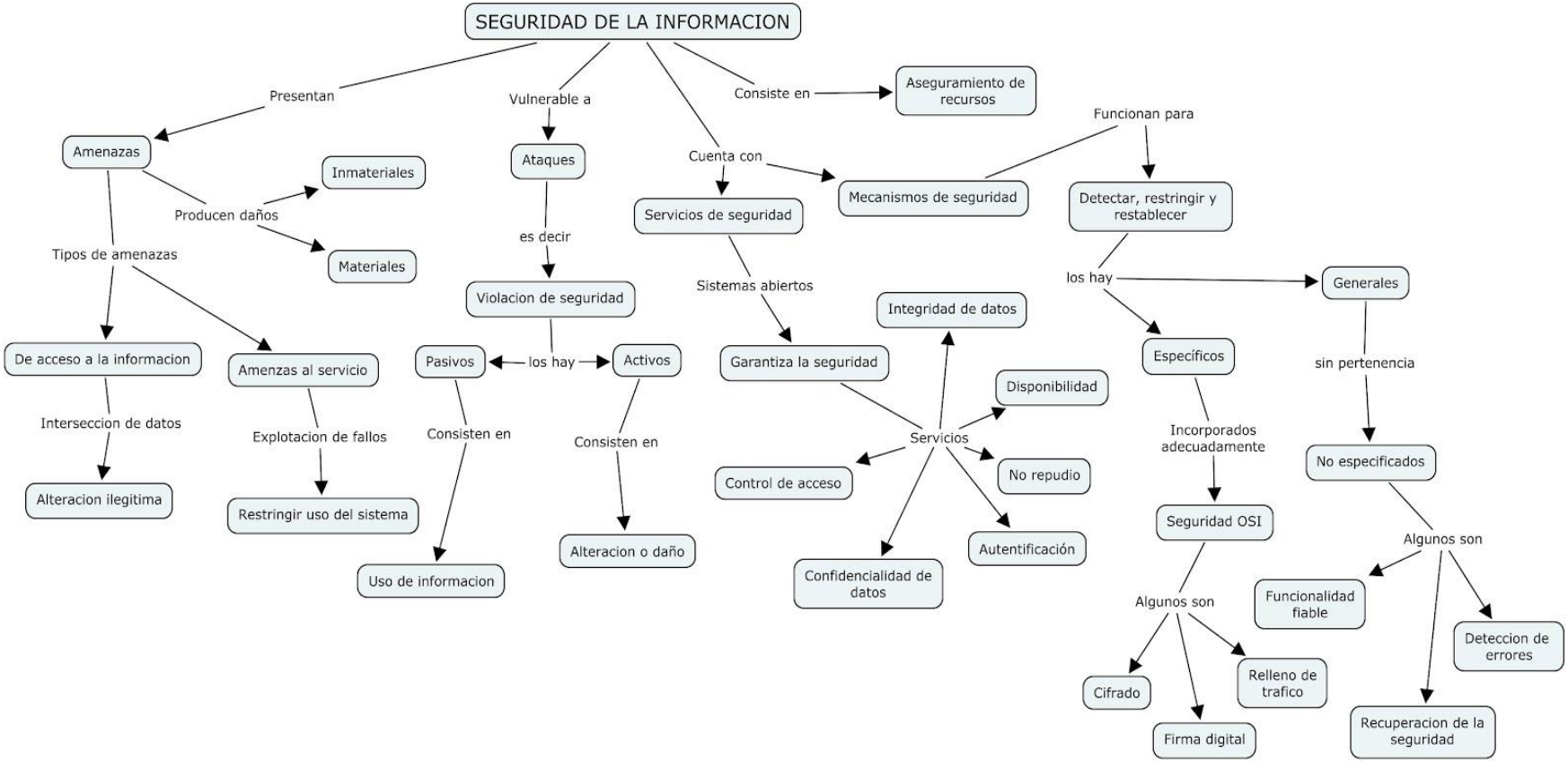


Figura 1: Mapa mental de la Seguridad de la Información

(“mapa.jpg (JPEG Image, 1600 × 743 pixels) - Scaled (45%),” n.d.)

2.3.3 Descripción de seguridad de la información

La seguridad es el conjunto de recursos, metodologías, documentos, programas y dispositivos físicos encaminados a lograr que los recursos de cómputo disponibles en un ambiente dado, sean accedidos única y exclusivamente por quienes tienen la autorización para hacerlo, cuando los requiera y se proteja de alteraciones no autorizadas. (Tanenbaum, 2003)

La seguridad de la información debe vigilar principalmente por las siguientes propiedades primarias de la información (Bertolín, 2008):

Confidencialidad.- La información debe ser vista y manipulada únicamente por quienes tienen el derecho o la autoridad de hacerlo. Un ejemplo de ataque a la confidencialidad es la divulgación de información confidencial.

Integridad.- La información debe ser consistente, fiable y no propensa a alteraciones no deseadas. Un ejemplo de ataque a la Integridad es la modificación no autorizada de las notas en un sistema académico o la modificación del estado de cuenta de una cuenta bancaria.

Disponibilidad.- La información debe estar en el momento que el usuario requiera de ella. Un ataque a la disponibilidad es la negación de servicio (En Inglés Denial of Service o DoS)

Otros aspectos a tomar cuenta para la seguridad son la trazabilidad, confiabilidad y no repudio.

2.3.4 Amenazas y ataques a la seguridad de la información

Una amenaza se da cuando existe una posibilidad de violación a la seguridad, que existe cuando se da una circunstancia, capacidad, acción o evento que pudiera romper la seguridad y causar un perjuicio, siempre en pro de explotar la vulnerabilidad de un sistema. (Stallings, 2003)

Un ataque es un asalto a la seguridad de la información derivado de un acto inteligente y deliberado para eludir los controles y violar la política de seguridad de un sistema, los ataques pueden en su sentido ser pasivos o activos. (Stallings, 2003), existen dos tipos de ataques: pasivos y activos.

Los ataques pasivos comúnmente se presentan como escucha u observaciones no autorizadas, con el objetivo principal de obtener la información que se está transmitiendo entre los emisores y receptores legítimos. Los ataques pasivos a su vez se pueden dividir en dos tipos:

Obtención de los contenidos del mensaje: en este tipo de ataque se trata de obtener información confidencial de un sistema cuando ésta se está transmitiendo por un medio dado. (Stallings, 2003)

Análisis de tráfico**:** Si el mensaje transmitido viaja encriptado, el contenido de los mensajes no se pueden descifrar para el atacante incluso habiendo capturado el mensaje y no puede obtener la información que contiene, pero aún el atacante podría observar el patrón de los mensajes, determinar la localización y la identidad de los servidores que se comunican y descubrir la frecuencia y longitud de los mensajes que se están intercambiando. Entonces este tipo de información puede ser de utilidad para averiguar la naturaleza de la comunicación que está teniendo lugar en una transmisión emisor-destino.

Los ataques pasivos son difíciles de detectar ya que no implican modificaciones en los datos, por lo que tanto el transmisor y receptor pasan por desapercibidos del ataque y no son conscientes de que una tercera persona ha leído los mensajes o que está observado el patrón de tráfico. Sin embargo, la contramedida típica para este tipo de ataques es el uso de cifrado o encripción. Entonces al tratar con los ataques pasivos, el énfasis de los encargados de la seguridad se evidencia más en la prevención que en la detección. (Instituto Tecnológico de Veracruz, n.d.-a)

Por otro lado, los ataques activos si generan una modificación del flujo de datos o la creación de un flujo falso de información. Entre las principales categorías de este tipo de ataque se pueden citar:

Suplantación de identidad: se da cuando una entidad se hace pasar por otra. Generalmente este tipo de ataque incluye unas de las otras formas de ataque pasivo, es decir que si un atacante mediante un ataque pasivo llegó determinar las secuencias de autentificación de una transmisión o comunicación, entonces luego puede obtener privilegios que no tenía para hacerse pasar por un usuario legítimo dentro de un sistema.

Repetición: implica la captura pasiva de una unidad de datos y su retrasmisión posterior para producir un efecto no autorizado.

Modificación de mensajes: significa que una parte de un mensaje original es alterada, o que los mensajes se han retrasado o reordenado, para producir un efecto no autorizado.

La interrupción de servicio: este ataque impide el uso o la gestión normal de las utilidades de comunicación. Puede tenerse como objetivo un destino particular o una red completa, ya sea inhabilitándola o sobrecargándola con mensajes para reducir su rendimiento. (Stallings, 2003)

2.3.5 Vulnerabilidad

“Vulnerabilidad es definida como un fallo en el proyecto, implementación o configuración de un software o sistema operativo que, cuando es descubierta por un atacante, resulta en la violación de la seguridad de una computadora o un sistema computacional” (Instituto Tecnológico de Veracruz, n.d.-c). Se presenta cuando la importancia y el valor que otorgado a la información, no se corresponde con las medidas de seguridad y los mecanismos de control implementados para protegerla. Una vulnerabilidad es la exposición latente a un riesgo.

En el área de informática, existen varios riesgos entre los cuales podemos citar: ataque de virus, códigos maliciosos, gusanos, caballos de Troya y hackers; así mismo con el uso de Internet como instrumento de comunicación y colaboración, los riesgos han evolucionado y las empresas también deben enfrentar ataques de DoS y amenazas combinadas, herramientas automáticas de *hackeo*, accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.

2.3.6 Riesgos

Los riesgos, en términos de seguridad se definen en función de la probabilidad e impacto de los mismos. Los riesgos tienen varias interacciones relacionadas con los activos y su valor, con las amenazas y vulnerabilidades, así como con los controles requerimientos de seguridad, tal como se muestra en la Figura 2.

2.4 Sistema de gestión de seguridad de la información

La gestión de seguridad de la información (SGSI) debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Este proceso es el que constituye un SGSI, que podría considerarse como el sistema de calidad para la seguridad de la información.

El SGSI trata de garantizar un nivel de protección aceptable, no total o que abarque el 100%, ya que es virtualmente imposible alcanzarlo incluso disponiendo de presupuesto ilimitado.

Figura 2: Relaciones de los riesgos

(ISO 27000, n.d., sec. 2b)

“El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías”. (ISO 27000, n.d., sec. 2a)

En el contexto del SGSI se debe entender por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración (ISO 27000, n.d., sec. 2a).

Para garantizar que la seguridad de la información es gestionada correctamente se debe identificar inicialmente su ciclo de vida y los aspectos relevantes adoptados, una ilustración sugerida por el sitio web oficial en español de la ISO 27000 se muestra en la Figura 3.

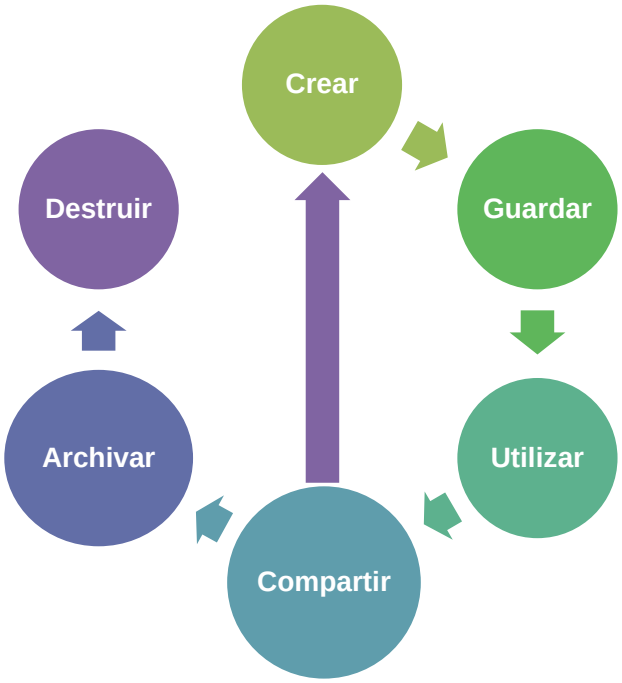


Figura 3: Ciclo de vida de la información

(ISO 27000, n.d., sec. 2a)

En base al conocimiento del ciclo de vida de cada información relevante se debe adoptar el uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

El nivel de seguridad que se puede obtener mediante la aplicación de medidas técnicas es limitado e insuficiente por sí mismo, ya que se deben como parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una

evaluación de riesgos y en una medición de la eficacia de los mismos (ISO 27000, n.d., sec. 2b).

El SGSI ayuda a establecer las políticas y procedimientos en relación a los objetivos de negocio de la organización, para mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir, ya que cuando la organización llega a conocer los riesgos a los que está sometida su información debe decidir si los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que debe ser revisada y mejorada continuamente.

Como parte del SGSI la organización debe desarrollar la documentación que se ilustra en la Figura 4.

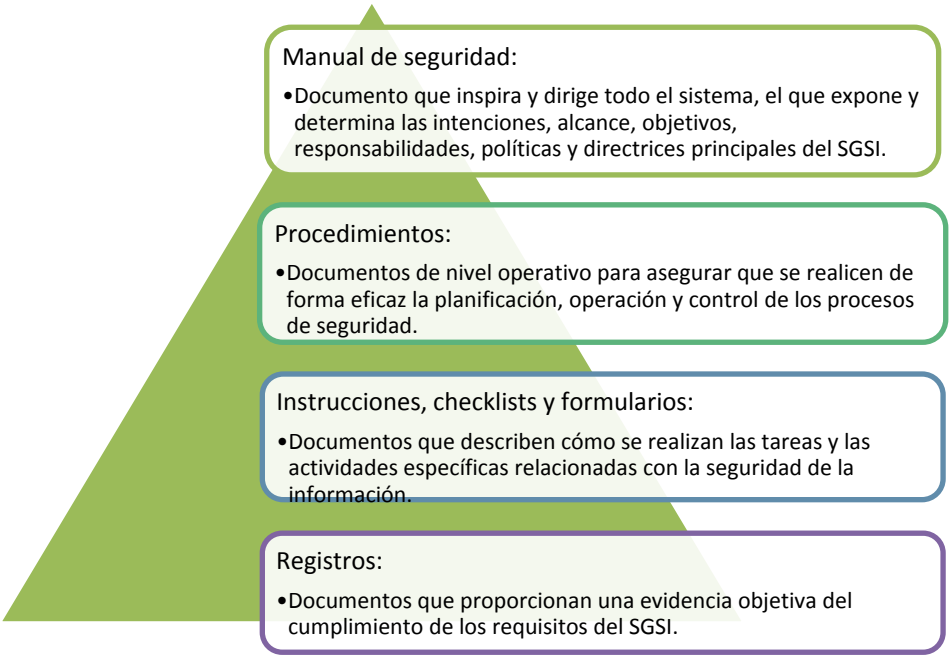


Figura 4: Documentación básica de un SGSI

(ISO 27000, n.d., sec. 2c) Además un SGSI debe estar formado por los siguientes documentos:

- Alcance del SGSI: ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas.
- Política y objetivos de seguridad: documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.
- Procedimientos y mecanismos de control que soportan al SGSI: aquellos procedimientos que regulan el propio funcionamiento del SGSI.
- Enfoque de evaluación de riesgos: descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables.
- Informe de evaluación de riesgos: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.
- Plan de tratamiento de riesgos: documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.
- Procedimientos documentados: todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.

- Declaración de aplicabilidad: (SOA -Statement of Applicability-, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.
- Todos estos documentos deben estar debidamente aprobados, revisado y actualizados cuando sea pertinente, garantizas los cambios y su estado actual, garantizar que las versiones relevantes estén disponibles, se debe garantizar la disponibilidad, la legibilidad e identificación de los documentos, entre las principales garantías para el control de la documentación

2.4.1 Normas ISO relacionadas a la gestión de seguridad de la información

Una norma es un documento cuyo uso es voluntario y que es fruto del consenso de las partes interesadas y que deben aprobarse por un organismo de Normalización reconocido.

La Organización Internacional para la Estandarización ISO (de sus siglas en inglés International Organization for Standarization), es un organismo internacional que se dedica a desarrollar reglas de normalización en diferentes ámbitos, entre los cuales está considerada la informática.

El IEC (de sus siglas en inglés International Electrotechnical Commision) es otro organismo internacional que publica normas de estandarización en el campo de la electrónica.

(PARANINFO, 2011) La serie de normas ISO/IEC 27000 se denomina “Requisitos para la especificación de sistemas de gestión de la seguridad de la información” y proporciona un marco de estandarización para la seguridad de la información para que sea aplicado por una organización o empresa y comprende un conjunto de normas sobre:

- Sistemas de gestión de la seguridad de la información
- Valoración de los riesgos
- Controles

El desarrollo de la norma ISO/IEC 27001, 27002 y 27000 en una escala de tiempo se puede visualizar en la Figura 5.

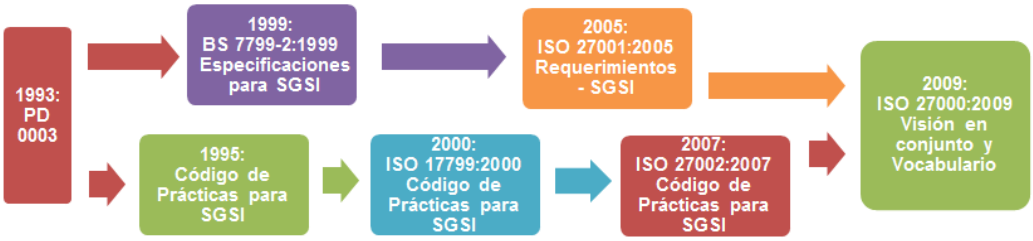


Figura 5: Línea del tiempo para el desarrollo de la norma ISO 27001, 27002 y 27000

2.4.2 Norma ISO/IEC 27001:2005

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA tradicional en los sistemas de gestión de la calidad, que aplicado a la gestión de la seguridad se aprecia en la Figura 6.

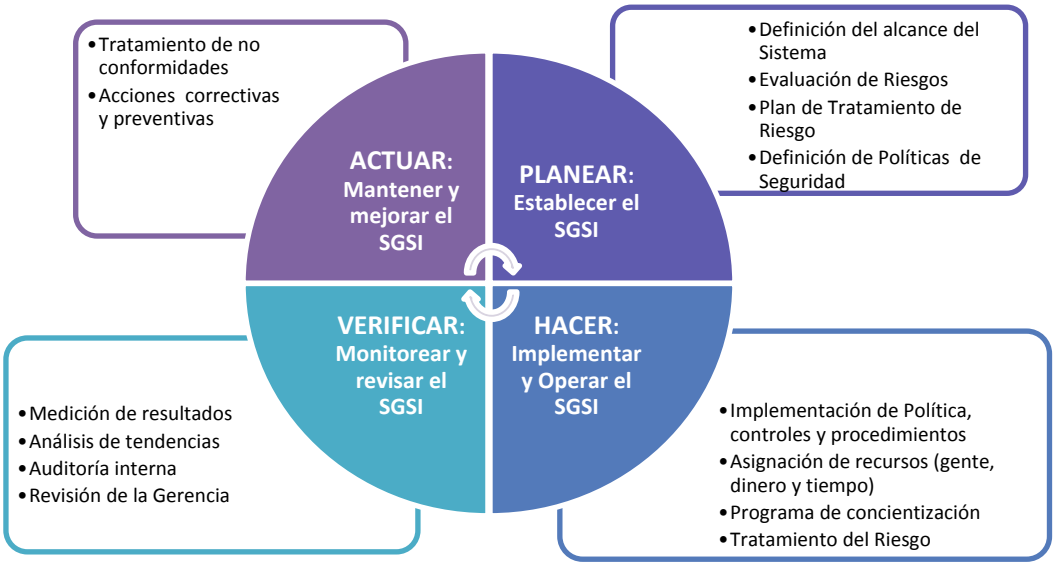


Figura 6: Ciclo continuo de PDCA para SGSI

Planificar: Establecer el SGSI

(ISO 27000, n.d., sec. 2d) En esta fase la organización debe:

- Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.
- Definir una política de seguridad que:
  - Incluya el marco general y los objetivos de seguridad de la información de la organización;
  - Considere requerimientos legales o contractuales relativos a la seguridad de la información;
  - Esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI;
  - Establezca los criterios con los que se va a evaluar el riesgo;
  - Esté aprobada por la dirección.

- Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles.

  El esquema más general de la gestión de riesgos se ilustra en la Figura 7.

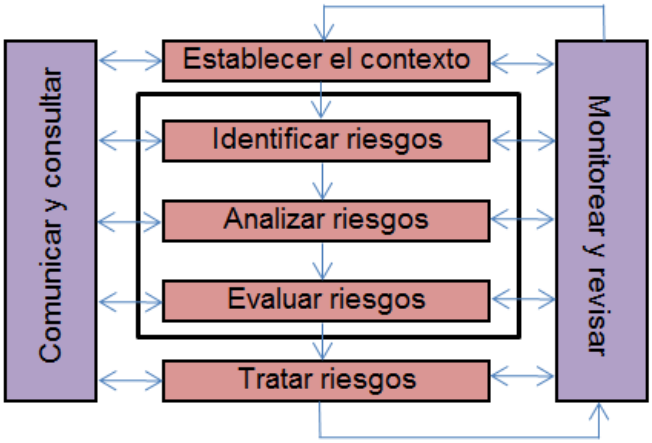


Figura 7: Esquema general de la gestión de riesgos

- Identificar los riesgos:
  - Identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios;
  - Identificar las amenazas en relación a los activos;
  - Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas;
  - Identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.
- Analizar y evaluar los riesgos:
  - Evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información;

  - Evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados;
  - Estimar los niveles de riesgo;
  - Determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.
- Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:
  - Aplicar controles adecuados;
  - Aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos;
  - Evitar el riesgo;
  - Transferir el riesgo a terceros.
- Seleccionar los objetivos de control y los controles del Anexo A de ISO 27001, que en el presente documento se detallan en el Anexo B, para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.
- Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI.
- Definir una declaración de aplicabilidad que incluya:
  - Los objetivos de control y controles seleccionados y los motivos para su elección;
  - Los objetivos de control y controles que actualmente ya están implantados;
  - Los objetivos de control y controles del Anexo A de la norma ISO/IEC 27001:2005 excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias.

Hacer: Implementar y utilizar el SGSI

(ISO 27000, n.d., sec. 2d) En esta fase la organización debe:

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.
- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.
- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.
- Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.
- Gestionar las operaciones del SGSI.
- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

Verificar: Monitorizar y Revisar el SGSI

(ISO 27000, n.d., sec. 2d) La organización deberá:

- Ejecutar procedimientos de monitorización y revisión para:
    - Detectar a tiempo los errores en los resultados generados por el procesamiento de la información;
    - Identificar brechas e incidentes de seguridad;
    - Ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la

seguridad de la información se desarrollan en relación a lo previsto;
    - Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores;
    - Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.
- Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.
- Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.
- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.
- Realizar periódicamente auditorías internas del SGSI en intervalos planificados.
- Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.
- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

Actuar: Mantener y Mejorar el SGSI

(ISO 27000, n.d., sec. 2d) La organización deberá regularmente:

- Implantar en el SGSI las mejoras identificadas.
- Realizar las acciones preventivas y correctivas adecuadas según las norma y de las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

En el ciclo de vida continuo requiere que luego de la fase de mantener y mejorar se regrese a planificar e iniciar un nuevo ciclo de las cuatro fases. Así mismo se debe disponer de una gerencia completamente comprometida en el proceso para alcanzar el éxito, para lo que la norma establece algunas de las tareas fundamentales del SGSI asignadas a la dirección se detallan en los siguientes puntos:

- Compromiso de la dirección: La dirección de la organización debe comprometerse con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.
- Formación y concienciación: La formación y la concienciación en seguridad de la información son elementos básicos para el éxito de un SGSI. Por ello, la dirección debe asegurar que todo el personal de la organización al que se le asignen responsabilidades definidas en el SGSI esté suficientemente capacitado.

2.4.3 Certificaciones de ISO/IEC ISO 27001:2005

En el ámbito de las certificaciones en normas de Seguridad, el Registro Internacional de ISMS Certificados a través de los organismos certificadores autorizados) registran que a nivel mundial se han emitido 7940 certificados a empresas que pasaron la certificación con el estándar ISO/IEC 27001, de las cuales Ecuador representa el 2.5% respecto al total de organizaciones certificadas.

A nivel mundial, 75 Universidades se han certificado en la norma ISO 27001:2005, que corresponde al 0.9% respecto al global general; 2 Universidades están ubicadas en el continente americano, 6 en Europa y 67 en Asia. De las cuales Latinoamérica y en especial Ecuador no tienen Universidades certificadas en esta norma.

Proceso de certificación ISO/IEC 27001

La ISO/IEC 27001 (Sistemas de gestión de seguridad de la Información) contiene los requisitos que deben cumplir las organizaciones y tiene un anexo que contiene los controles de la norma ISO/IEC 17799:2005 (ISO/IEC 27002).

Los expertos que forman parte del Registro Internacional de ISMS Certificados infieren que los cambios significativos en la estructura de la norma ISO/IEC 17999:2000 hacia la ISO 27001:2005 revisada el 15 de junio 2005, son la agregación de un dominio “Administración de Incidentes de Seguridad” (ver Figura 8), la definición de nombres de cada dominio, 17 nuevos controles, controles fusionados y otros eliminados; actualmente existen 11 dominios y 134 controles.

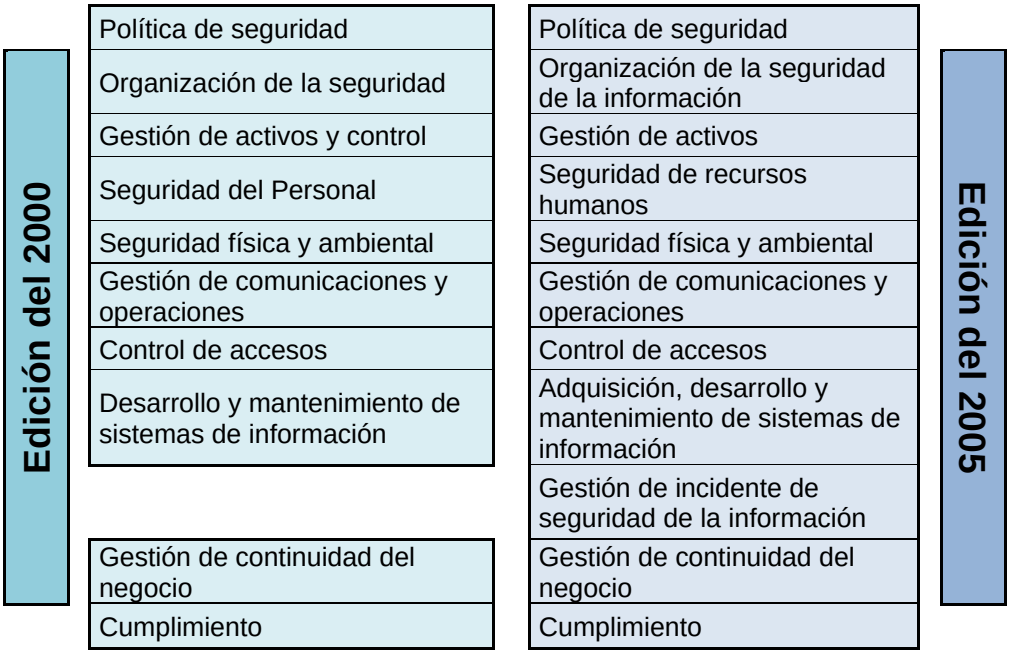


Figura 8: Comparación de los dominios de la norma ISO/IEC 17799:2000 y la norma ISO/IEC 27001:2005

Según el Registro Internacional de ISMS Certificados el proceso de certificación está constituido por tres fases:

- La primera fase del proceso consiste en la preparación de la compañía para la certificación del SGSI: desarrollar e implementar su SGSI, el uso y la integración de su SGSI a los procesos de negocio, la formación del personal y el establecimiento de un programa de mantenimiento del SGSI.
- La segunda fase consiste en el empleo de uno de los organismos de certificación acreditados para llevar a cabo una auditoría de su SGSI. El certificado otorgado por un organismos internacional tiene una duración de tres años después de este periodo el SGSI debe ser certificado nuevamente.
- La tercera fase del proceso (suponiendo que la certificación ha sido un éxito y un certificado ha sido emitido), que consiste en que el organismos de certificación visita la organización y revisa el SGSI de

forma regular (por ejemplo, cada 6-9 meses) para llevar a cabo una auditoría de seguimiento.

A pesar de que la norma ISO/IEC 27001:2005 solo es un código de prácticas para la gestión de seguridad de la información, no fue diseñado para ser aplicable en procesos de certificación. Sin embargo, se diseñó y se utiliza el complemento estándar BS 7799 Parte 2:2002 (y la nueva versión revisada de la Parte 2 de la ISO/IEC 27001, sistemas de gestión de seguridad de la información - Requisitos) para fines de la certificación de sistemas de gestión.

2.5 Análisis y gestión de riesgos

“El análisis y gestión de riesgos es un método formal para investigar los riesgos de un SI y recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos. A su vez es una salvaguarda preventiva que intenta buscar ordenadamente otras salvaguardas para proteger el SI.” (de Pablos Heredero et al., 2006)

El análisis de riesgos implica la evaluación del impacto que una violación de seguridad tendría en una empresa, señala los riesgos existentes, las amenazas que afectan al sistema y la determinación de las vulnerabilidades a dichas amenazas.

La gestión de riesgos es un proceso separado que utiliza los resultados del análisis de riesgos para seleccionar e implantar las medidas de seguridad adecuadas para controlar los riesgos identificados. Frente a estos riesgos se puede:

- Aceptar el riesgo
- Mitigar el riesgo. Conlleva a la elaboración y ejecución del plan de seguridad.
- Transferir el riesgo
- Evitar el riesgo

Para gestionar los riesgos se debe identificar y priorizar los peligros inherentes al sistema, proceso u organización. También se encarga de cuantificar la probabilidad de producirse amenazas y establecer un nivel aceptable de riesgo para la organización. (Bertolín, 2008)

Dentro de la gestión de riesgos existe un factor de incertidumbre relacionado con la probabilidad de que se dé un incidente de seguridad, así como el impacto asociado a la ocurrencia del problema.

2.5.1 Normas relacionadas a la gestión de riesgos

Las normas, metodologías y métodos principales utilizados para el análisis y gestión de riesgos se describen de manera general a continuación:

ISO/IEC 31000 – Risk Management: Establece una serie de principios y directrices de carácter genérico sobre gestión de riesgos, tiene como objetivo ayudar a las organizaciones a gestionar el riesgo con efectividad. Integra la gestión de riesgos con gobierno corporativo, planificación, gestión, procesos de información, políticas, valores y cultura. En la Figura 9 se muestran los tres elementos que conforman la norma ISO/IEC 31000: Principios de la gestión del riesgo, marco de trabajo para la gestión de riesgo y el proceso de gestión de riesgos.

ISO/IEC 27005: Es aplicable a todo tipo de organización, proporciona el estándar base para la gestión de riesgos de la seguridad de la información.

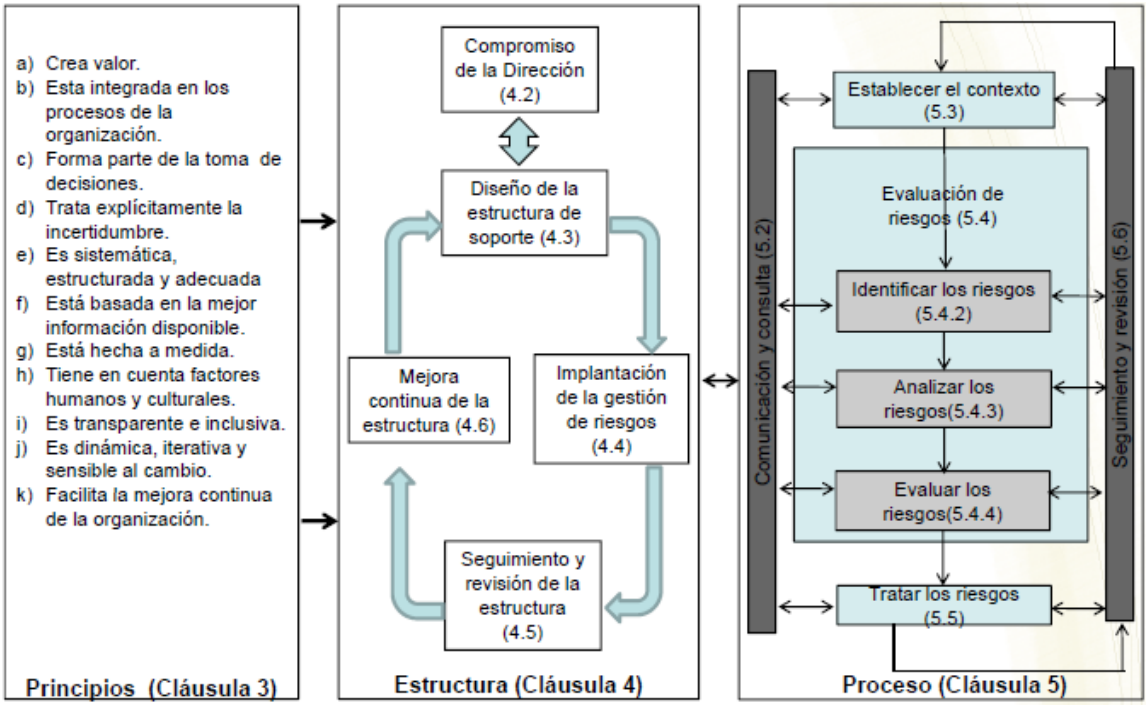


Figura 9: ISO/IEC 31000 – Descripción de los principios, marco y proceso de gestión de riesgos.

MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: Elaborada por el Consejo Superior de Administración Electrónica (CSAE) de España, reconocida por la ENISA (European Network and Information Security Agency). Está directamente relacionada con el uso de las tecnologías de información, enfatiza en dividir los activos de información en grupos para identificar los riesgos y los riesgos asociados. Consta de tres libros: “El método”, “Catálogo de elementos” y una “Guía de Técnicas”, donde se describe los pasos básicos para realizar el análisis y gestión de riesgos, tipos de activos, dimensiones, valoración de activos, criterio de valoración de activos, amenazas, salvaguardas, y las técnicas para llevar a cabo el proyecto. En la Figura 10 se muestra el proceso de gestión de riesgos de Magerit basado en la norma ISO/IEC 31000. (Ministerio de Hacienda y Administraciones Públicas, n.d.)

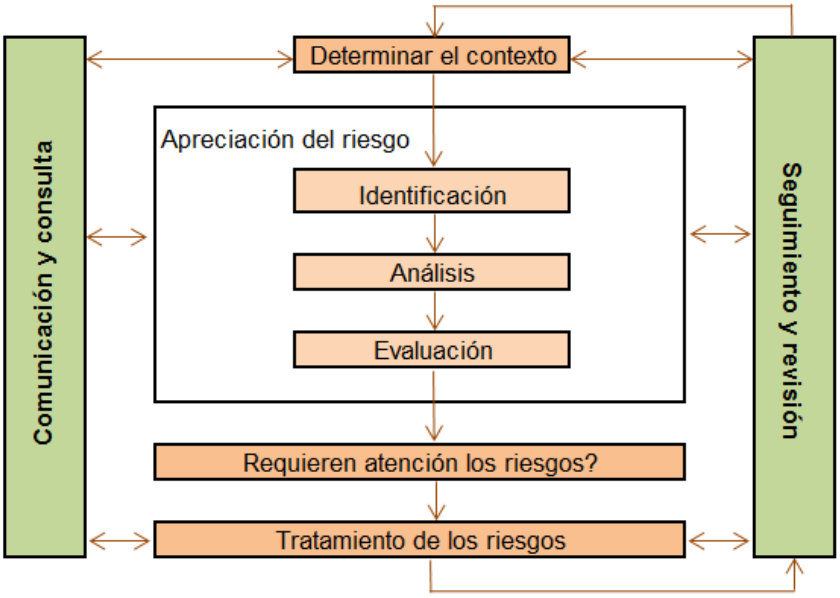


Figura 10: Magerit – proceso de gestión de riesgos

CRAMM – CCTA Risk Analysis and Management Method: Desarrollada por la Agencia Central de Computación y telecomunicaciones del Gobierno de Reino Unido, es usada principalmente en la administración pública británica. Es aplicable a todo sistema de información, organización, procesos, aplicaciones o infraestructura, utiliza técnicas cualitativas para el análisis y gestión de riesgos. En la Figura 11 se muestra el proceso de gestión de riesgos de la metodología CRAMM.

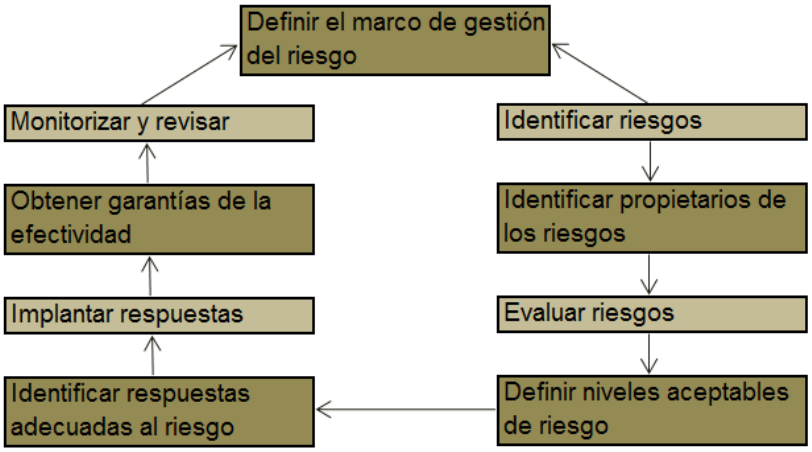


Figura 11: CRAMM – proceso de gestión de riesgos

OCTAVE - Operationally Critical Threat. Asset and Vulnerability Evaluation: Analiza los riesgos desde un punto de vista organizativo y técnico, y propone un plan de mitigación. Se enfoca en tres niveles: organizacional, operacional y de usuario final. Los procesos que forman parte del método Octave se ilustran en la Figura 12 y se describen a continuación:

- Consolidación de la información y creación de perfiles de amenazas.
- Identificación de componentes claves.
- Evaluación de los componentes seleccionados.
- Análisis de riesgos de los recursos críticos.
- Desarrollo de estrategias de protección.

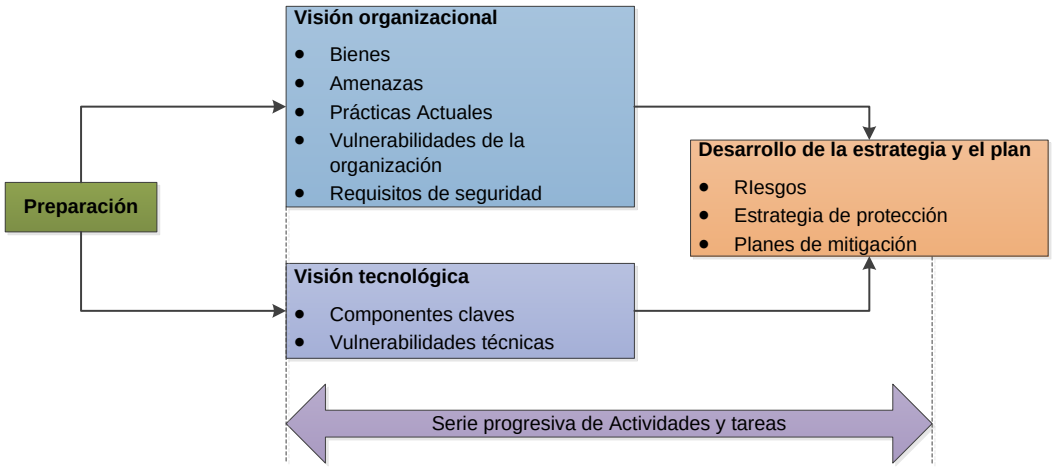


Figura 12: Octave – diagrama de análisis de riesgos

Fuente: Grafíco tomado de la presentación “Risk Assessment”, By: Ashwin Vignesh Madhu (“Blanca Rubiela Duque Ochoa - Metodologías de Gestión de Riesgos,” n.d.)

NIST SP 800-30: Creado por el National Institute Standards and Technology, US Department of Commerce. Es una guía para la evaluación de riesgos enfocada entre nivel táctico y estratégico de la organización, abarca los niveles organizacional, procesos del negocio y

sistema de información: El proceso de esta guía se basa en cuatro elementos: el contexto de riesgos, evaluación del riesgo, respuesta al riesgo y monitoreo del riesgo. Los pasos de la evaluación de riesgos se muestran en la Figura 13.

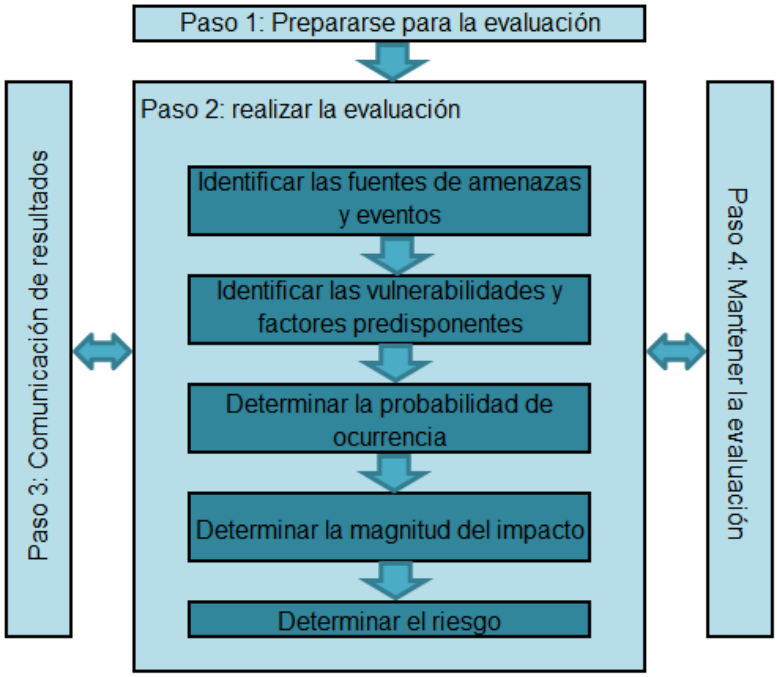


Figura 13: NIST SP 800-30 - pasos de la evaluación de riesgos

(Stouffer, Falco, & Scarfone, 2013)

BS7799-3:2006 Sistemas de Gestión de seguridad de la información: Es una norma creada por el British Standards Institution, brinda las directrices para sobre la evaluación de riesgos, tratamiento de riesgos, toma de decisiones por parte de la alta gerencia, re-evaluación de los riesgos, monitorización y revisión de los riesgos, en el contexto de gobierno corporativo y las relaciones internas con otras funciones del negocio (finanzas, informática, administración, recursos humanos, entre otros). Ofrece una guía para apoyar los requisitos dados en ISO/IEC 27001:2005. En la Figura 14 se describe el modelo del proceso de administración de riesgos.

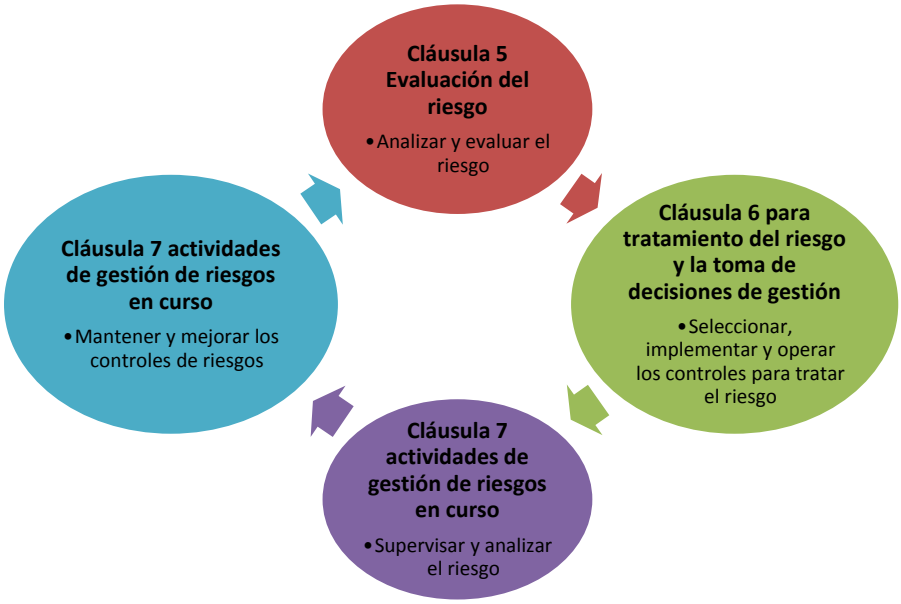


Figura 14: BS7799-3:2006 - modelo del proceso de administración de riesgos

También, existen otras normas y metodologías de gestión de riesgos utilizadas a nivel mundial, como las detalladas a continuación:

- **MARION:** método francés que se actualiza por CLUSIF (Asociación de empresas aseguradoras francesas).
- **AS/NZS 4360:**2004 Gestión de Riesgos
- **IRAM** – Information Risk Analysis Methodologies
- **CORAS** – Construct a platform for risk Analysis of Security critical systems
- **SOMAP** – Security Officers Management and Analysis Project
- **FAIR** – Factor Analysis of Information risk
- **ERM** - Enterprise Risk Management
- **SRM** - Strategic Risk Management
- **Basilea II y Solvencia II:** Evaluación de riesgos financieros

2.5.2 Norma ISO/IEC 27005:2011

La norma ISO/IEC 27005:2011 provee las guías para administrar los riesgos de seguridad de la información, describe el proceso de gestión de riesgos y brinda soporte a los conceptos generales especificados en la norma ISO/IEC 27001:2005, Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad – Requisitos. Se enlaza con el ciclo PDCA (Plan, Do, Check, Act) con el fin de revisar dichos riesgos.

La norma está alineada con la ISO 31000:2009 “Gestión de Riesgos – Principios y Directrices”, ISO/IEC 31010:2009 “Gestión de riesgos - las técnicas de evaluación de riesgos” y ISO Guide 73:2009 “Gestión del riesgo – Vocabulario” para gestionar los riesgos de seguridad de la información en las organizaciones que desean usar un marco de referencia.

"ISO/IEC 27005:2011 es una norma esencial para aquellos que quieren gestionar sus riesgos con eficacia y, en particular, para cumplir la norma ISO/IEC 27001 de sistemas de gestión de seguridad de la información. La gestión de riesgos es fundamental para el buen gobierno y esta norma ayuda a las organizaciones con consejos sobre el por qué, qué y cómo de la gestión de los riesgos de seguridad de la información en apoyo a los objetivos de su gobierno." (BSIGROUP, n.d.)

Estructura de la norma ISO/IEC 27005:2011

El proceso de gestión de riesgos de seguridad de la información se compone de seis cláusulas 7-12 y seis anexos de carácter informativo y no normativo. En la Figura 15 se muestra una visión general del proceso utilizado por la norma ISO/IEC 27005:2011.

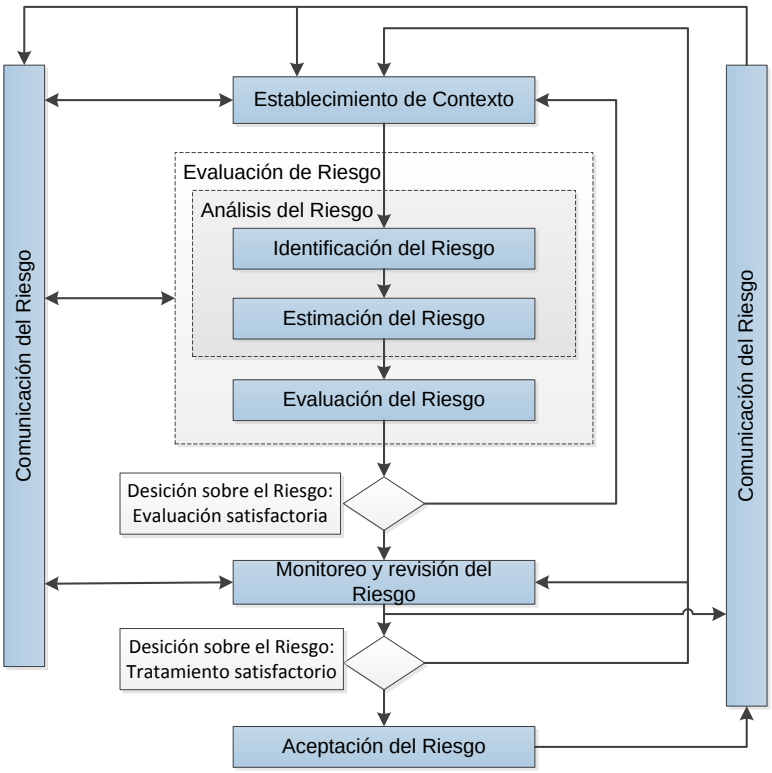


Figura 15: ISO/IEC 27005:2011- visión general del proceso

Establecimiento del contexto (Cláusula 7): Determina los contextos estratégicos, organizacionales y de gestión. Se establecen los criterios de evaluación de riesgos, criterios del impacto y criterios de aceptación de riesgos.

Evaluación del riesgo (Cláusula 8)

- Análisis de Riesgo:
  - Identificación del Riesgo
  - Identificación de los activos
  - Identificación de las amenazas
  - Identificación de los controles existentes
  - Identificación de las vulnerabilidades
  - Identificación de las consecuencias
- Estimación del Riesgo

- Metodologías para la estimación del riesgo
- Evaluación de las consecuencias
- Evaluación de la probabilidad de incidentes
- Nivel de Riesgo estimado

Evaluación del Riesgo: Se define la naturaleza de las decisiones pertinentes para evaluar el riesgo y los criterios para la toma de decisiones (determinados en el establecimiento del contexto).

Tratamiento del riesgo (Cláusula 9): Se define las opciones para el tratamiento de riesgo y se determina los riegos residuales, como se muestra en la Figura 16 y siendo estas: reducir, transferir, retener y evitar el riesgo.

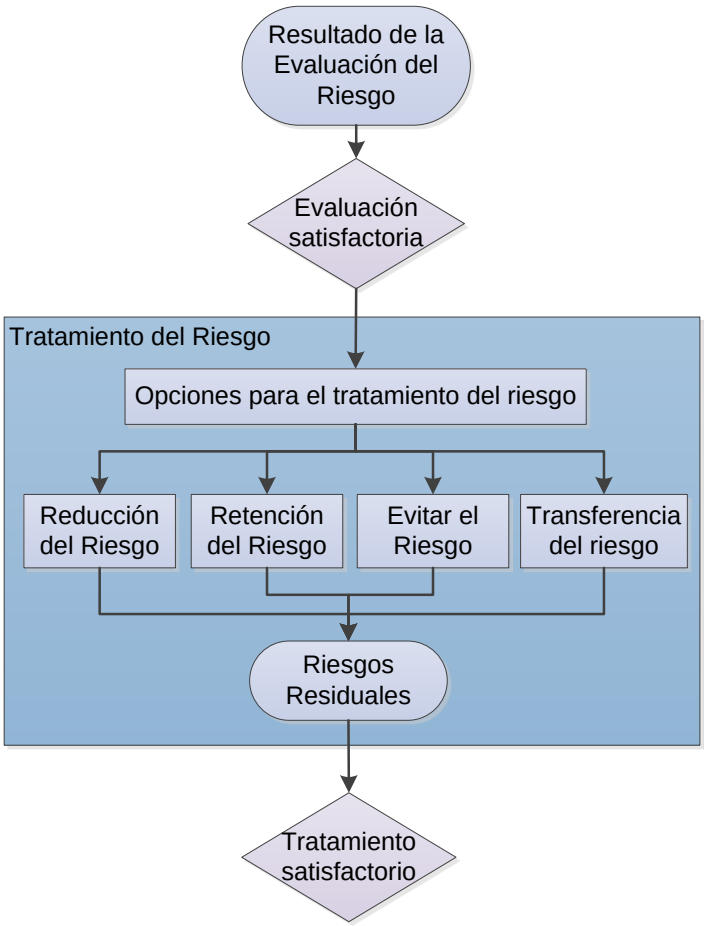


Figura 16: ISO/IEC 27005:2011 - Tratamiento del riesgo

Aceptación del riesgo (Cláusula 10): Determina si un riesgo está fuera de los límites del umbral establecido. Es posible que el nivel del riesgo residual no satisfaga los criterios de aceptación del riesgo.

Comunicación del riesgo (Cláusula 11): Es una actividad para lograr un acuerdo sobre la manera de gestionar los riesgos al intercambiar y/o compartir información de los riesgos, entre las partes interesadas y los que toman decisiones.

Monitorización y revisión del riesgo (Cláusula 12): Garantiza que el contexto, el resultado de la evaluación de riesgo y el tratamiento de riesgo continúan pertinentes y adecuados.

Los anexos de la norma describen lo siguiente:

“Anexo A” define el alcance y los límites del proceso de gestión del riesgo de seguridad de la información.

“Anexo B” trata sobre la identificación y valoración de activos y de impacto en las organizaciones.

“Anexo C” muestra ejemplos de amenazas comunes.

“Anexo D” describe varios ejemplos de vulnerabilidades comunes.

“Anexo E” presenta ejemplos para la valoración del riesgo en la seguridad de la información.

CAPÍTULO 3

3 CASO DE ESTUDIO

3.1 Universidad Tecnológica Equinoccial

3.1.1 Descripción de la Universidad

La Universidad Tecnológica Equinoccial responde a los desafíos del mundo actual, incorporando en sus labores académicas los últimos adelantos científicos y tecnológicos, con el fin de desarrollar nuevas alternativas profesionales para la juventud. En el marco de una filosofía humanista, que centra su eje de acción en el desarrollo integral del estudiante como ser humano, inculca tres principios básicos:

Excelencia: El rigor científico y el uso eficaz de todos los recursos tecnológicos disponibles, al máximo de especialización y competencia.

Visión: El poder ampliar el horizonte hacia el universo, responder como ciudadanos del mundo a las nuevas exigencias de la globalización y aportar realmente al progreso del Ecuador.

Liderazgo: La capacidad para definir objetivos propios y la decisión para emprender en ellos, firmeza para implantar derechos y para hacer cumplir obligaciones, con energía, dinamismo y creatividad, pero sobre todo con el ejemplo.

Misión

(“AutoevaluaciónUTE.pdf,” n.d.) “La Universidad Tecnológica Equinoccial es una institución particular ecuatoriana sin fines de lucro, integrada por una comunidad universitaria competente y con espíritu de superación. Está comprometida con la educación, la investigación científica y el desarrollo tecnológico mediante propuestas innovadoras y de calidad,

destinadas a la formación humanista y al progreso del país, guiada por el Código de Ética Institucional".

Visión

("AutoevaluaciónUTE.pdf," n.d) "En el año 2017 la Universidad Tecnológica Equinoccial habrá alcanzado la máxima categoría en docencia e investigación, con una oferta que incluirá nuevas profesiones y proyectos científicos centrados en el desarrollo del país.

Contaremos con estudiantes incorporados a través de un riguroso proceso de selección, quienes recibirán una formación humanista y de altos estándares académicos.

Su estructura académica y administrativa será flexible y ágil con el fin de adaptarse a los cambios del entorno.

Habrá estructurado un sistema integral de gestión del talento humano, que s se reflejará en una mayor cohesión de los estamentos que integran la comunidad universitaria.

Estará más comprometida con la sociedad, mediante programas de vinculación, orientados a la sostenibilidad económica, social y ambiental.

Su proyección intencional le permitirá establecer alianzas estratégicas que posibiliten la movilidad de profesores y estudiantes".

Objetivos institucionales

- **Docencia**

Disponer de una planta docente comprometida, con un alto perfil académico, una remuneración competitiva y mayormente a tiempo completo.

Consolidar el modelo educativo para mejorar la calidad de los procesos de enseñanza aprendizaje y la eficiencia académica.

- **Investigación**

Proporcionar a la Universidad Tecnológica Equinoccial como una entidad de investigación y docencia, mediante la producción, gestión y transferencia de nuevos conocimientos basados en las líneas de investigación institucional.

Consolidar la formación de grupos de investigación que profundicen la cultura investigativa como parte constitutiva del talento humano de la UTE.

- **Vinculación**

Incrementar servicios permanentes de asistencia técnica, consultoría, capacitación externa y apoyo comunitario a la sociedad.

Fortalecer los programas de vinculación, de cultura y deportes con la participación activa de profesores, estudiantes y egresados.

- **Gestión**

Fortalecer el modelo de desarrollo de la Universidad, mediante procesos eficientes y eficaces de gestión académica y administrativa que faciliten la adopción a los cambios del entorno.

Diseñar y aplicar políticas, estrategias y procedimientos que garanticen la diversificación de fuentes de financiamiento que coadyuven al desarrollo de la Universidad".

3.1.2 Organigrama de la UTE

La estructura orgánica de la Universidad Tecnológica Equinoccial se presenta en la Figura 17.

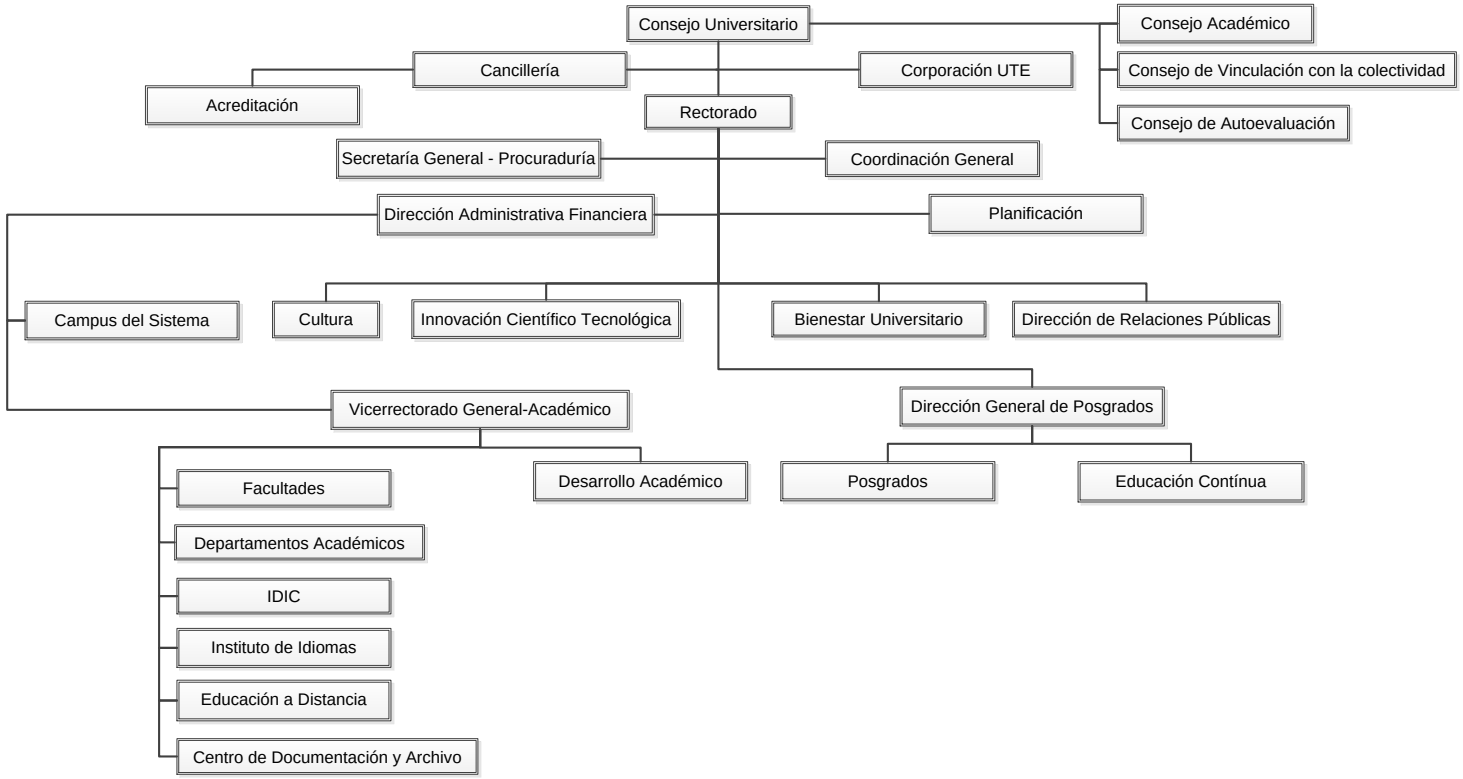


Figura 17: Organigrama Funcional de la UTE.

3.1.3 Modelo Educativo

("Unidad de Excelencia Académica y Desarrollo Curricular | UTE," n.d.) El enfoque del Modelo Educativo, desde lo filosófico es humanista, hace énfasis en el desarrollo del potencial humano, su objetivo es el desarrollo integral, el aprendizaje es centrado en el estudiante y va más allá de la información y de los datos, busca satisfacer sus necesidades físicas, psicológicas y volitivas, a través del conocimiento de sí mismo y de su entorno, adoptando una postura individual y social.

El currículo es integral y flexible, la formación es por competencias, las estrategias de aprendizaje son colaborativas y participativas y la evaluación es integral. Todos los elementos del currículo en sus diferentes momentos, ya sea diseño o actualización de carreras, deben mantener coherencia con el enfoque del Modelo.

Los procesos de cambio en el mundo también han incidido vigorosamente sobre el conocimiento, tanto en su naturaleza como en su estructura disciplinar; la amplitud y diversidad de conocimientos es ilimitada, al igual que su acelerada innovación y difusión, soportada por las tecnologías de la información y comunicación.

Desde este escenario, la Universidad Tecnológica Equinoccial, con los insumos obtenidos desde diversas fuentes: entrevistas realizadas a distintos actores de la comunidad educativa, jornadas de reflexión con varios expertos, documentos elaborados por las Facultades, sondeos de opinión sobre las competencias genéricas, involucramiento en el Proyecto Tuning[3] para América Latina entre otros, construye su Modelo Educativo.

[3] El proyecto Alfa Tuning: Es un proyecto independiente, impulsado y coordinado por Universidades de distintos países, tanto latinoamericanos como europeos su meta es identificar e intercambiar información y mejorar la colaboración entre las instituciones de educación superior para el desarrollo de la calidad, efectividad y transparencia

El Modelo Educativo UTE, se sustenta en concepciones teóricas actuales de la educación universitaria e incorpora los aspectos pertinentes del Plan Nacional de Desarrollo y las disposiciones legales vigentes y como metodología, utiliza la formación por competencias, como se ilustra en la Figura 18:

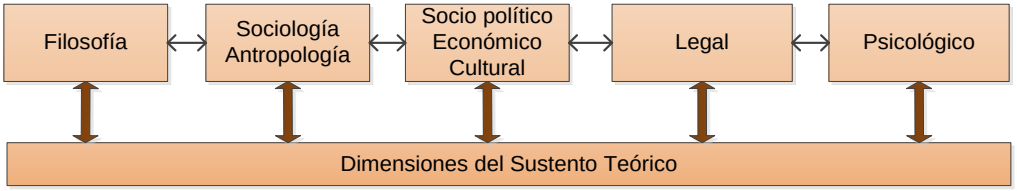


Figura 18: Dimensiones del sustento Teórico del Modelo Educativo de la UTE

(“Modelo_Educativo_new.pdf,” n.d) El modelo contribuye de forma consistente, coherente y relevante al desarrollo de los/as miembros/as de la comunidad universitaria, en el marco de la visión estratégica institucional.

El modelo propone, currículos abiertos, flexibles, dinámicos, contextualizados, inter y transdisciplinarios, desde estrategias preponderantemente participativas, experienciales y cooperativas, para el desarrollo integral del ser humano en su multidimensionalidad.

En tal sentido, el modelo educativo es el conjunto de lineamientos generales orientadores del accionar universitario y se expresa en las funciones de: docencia, investigación y vinculación con la colectividad, como se muestra en la figura 19. Entonces, la Universidad en la definición de su modelo, considera importante puntualizar los siguientes aspectos:

Un Estado que reconozca y respete: participación, derechos individuales y colectivos; apoye de manera preferente las políticas sociales, entre ellas las educativas.

Enfocarse en que la Universidad se concibe como el espacio activo de desarrollo de la sociedad, que orienta y conduce teórica y prácticamente el accionar científico/tecnológico, económico, político, cultural y ambiental de la sociedad.

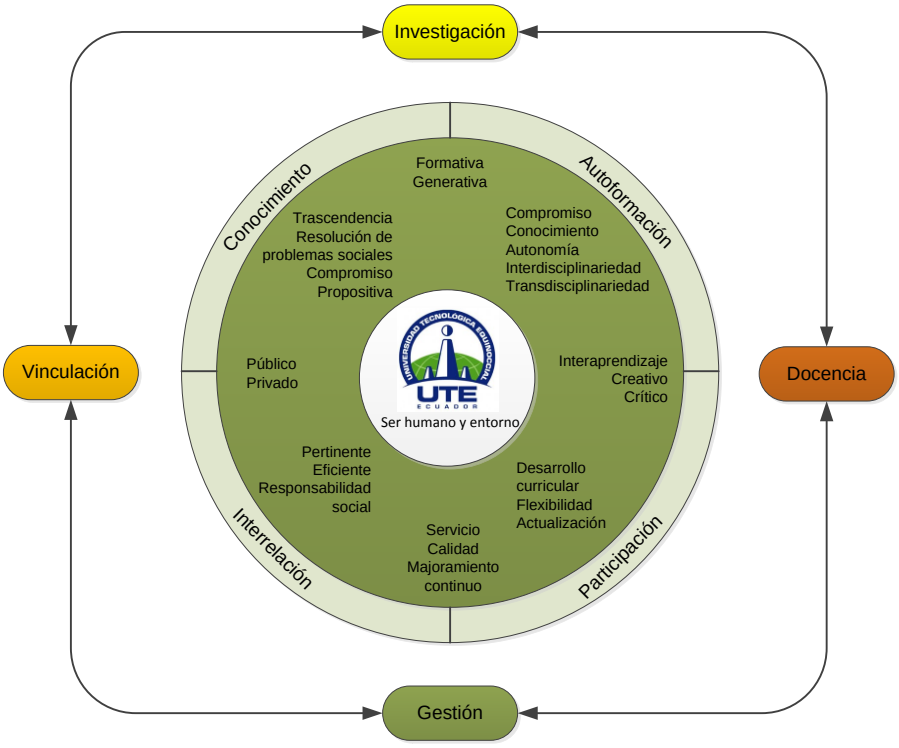


Figura 19: Esquema general del Modelo Educativo de la UTE

Contribuir a la construcción de una sociedad que:

- Funcione con principios.
- Posea identidad y soberanía.
- Sea equitativa, justa, solidaria, participativa, cooperativa y democrática.
- Propicie el diálogo y la comprensión entre todos sus miembros, sin ningún tipo de discriminación y exclusión.
- Promueva la sostenibilidad del ambiente.

(“Modelo_Educativo_new.pdf,” n.d.) La UTE concibe la educación como un proceso intencionado, complejo, sistémico, crítico, en continua construcción que propicia saberes (humanistas, éticos, estéticos, científicos y tecnológicos), busca el desarrollo humano permanente y la transformación social. Toma en cuenta los referentes locales, regionales y globales, en función de los fines de la educación pertinentes en el Ecuador, tal como lo establece la Constitución de la República, infiere que el sistema de Educación Superior tiene como finalidad:

> **“… la formación académica y profesional con visión científica y humanista; la investigación científica y humanista; la investigación científica y tecnológica; la innovación, promoción, desarrollo y difusión de los saberes y las culturas; la construcción de soluciones para los problemas del país, en relación con los objetivos del régimen de desarrollo”** (Publicado en la Sección Primera de la Constitución del Ecuador, Art. 350).

Como parte del sistema nacional de ciencia, tecnología e innovación la Universidad Ecuatoriana tiene como finalidad:

- Generar, adaptar y difundir conocimientos científicos y tecnológicos.
- Recuperar, fortalecer y potenciar los saberes ancestrales.
- Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir. (Publicado en la Sección Octava de la Constitución del Ecuador, Art. 385).

3.1.4 Enfoque del modelo UTE

(“Modelo_Educativo_new.pdf,” n.d.) A continuación se describe de forma general el enfoque del modelo educativo de la UTE.

Caracterización General

Al ser humano se lo concibe como una unidad, indivisible, irrepetible, perfectible, razón de ser de la Universidad; persona activa que construye el conocimiento de forma crítica, rigurosamente científica, responsable y cooperativa, para la integración y transformación de la sociedad.

Potencia el análisis y la praxis de los principios corporativos de la UTE en el proceso educativo. La práctica del respeto, honestidad, solidaridad, coherencia, responsabilidad, justicia, equidad, transparencia, permiten la realización humana de todos los/as actores/as de la comunidad universitaria.

La UTE es un sistema integrado que impulsa la interrelación armónica entre sus distintas unidades académicas y administrativas con la colectividad, y contribuye a la formación de una sociedad justa, equitativa, solidaria, soberana y responsable.

La metodología para operativizar el modelo es por medio de la formación por competencias, es decir por medio del desarrollo de capacidades integrales.

Características del Proceso Educativo

(“Modelo_Educativo_new.pdf,” n.d.) Propone un proceso de aprendizaje centrado en la potenciación de todas las capacidades humanas, que se desarrollan como un todo complejo, y son saberes inter y transdisciplinario.

Aprendizajes en que el conocimiento es significativo por lo que es generado, apropiado y transformado en el contexto de su aplicación e implicaciones; relacionado con los conocimientos anteriores.

Respeta las diferentes formas y ritmos de aprendizaje.

El desarrollo de la capacidad de aprender durante toda la vida, a partir del dominio de habilidades y estrategias para aprender a aprender y la necesidad de continuar en su formación con autonomía durante toda la vida.

Los objetivos de aprendizaje, incluyen contenidos que garantizan la apropiación de conocimientos y nuevas formaciones de pensamiento requeridas para la realización de diferentes tipos de actividad; a su vez, los conocimientos que se proponen tienen estrecha vinculación con otros que están en su base, según la lógica de la interrelación que se produce entre los conocimientos científicos.

Características de los protagonistas

(“Modelo_Educativo_new.pdf,” n.d.) El modelo UTE, concibe a la persona como una unidad dialógica, dentro de un contexto histórico, cultural, social, político, ético, estético; unidad que facilita los procesos educativos, para la construcción crítica permanente del conocimiento, incorporando el uso de las nuevas tecnologías; sin perder de vista las especificidades de sus roles.

Las políticas son lineamientos generales que se toman en cuenta para el diseño de cualquier carrera y éstas responden al Modelo Educativo y Pedagógico de la UTE.

El Modelo Educativo y Pedagógico de la UTE, plantea los perfiles profesionales por competencias y los ejes curriculares del pensum que se organizan de la siguiente manera:

a) Formación humana: El propósito de este eje es aportar al desarrollo de la persona, siendo coherente con lo planteado en el modelo, donde el centro del proceso de aprendizaje es el ser humano y su entorno, por lo que es común a todas las carreras y puede ubicarse en cualquier nivel de la Carrera.

b) Formación básica: El propósito es proporcionar habilidades y conocimientos de iniciación a los estudios universitarios, e introducir a los estudiantes en los contenidos de la especialidad.

c) Formación profesional: El propósito es el de proporcionar habilidades y conocimientos característicos de la especialidad.

La sugerencia del modelo educativo de la UTE acerca del peso curricular para los ejes disciplinares se presenta en la Figura 20.

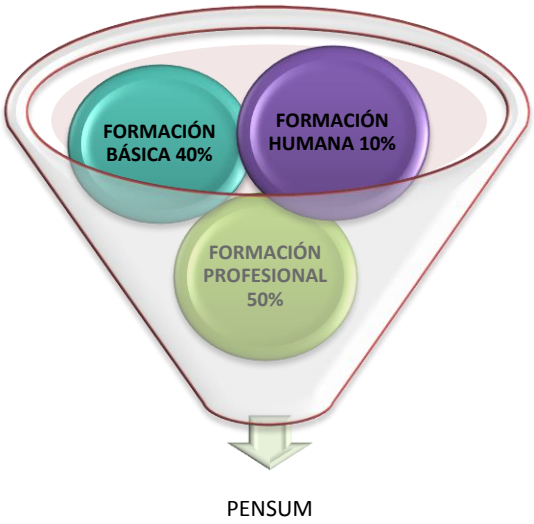


Figura 20: Sugerencia del peso curricular los tres ejes disciplinares de la UTE

3.1.5 UTE: su pensamiento e involucramiento con los sistemas de admisión y nivelación

Los cambios vertiginosos que se dan en la sociedad del siglo XXI retan a la educación y, en especial, a la Universidad a realizar análisis sobre la importancia de contar con un sistema de admisión y nivelación, científica y técnicamente válido y confiable. Un sistema que permita identificar las competencias básicas que debe tener un candidato para el ingreso a una Universidad, a fin de prevenir fracasos y frustraciones en la población

estudiantil; es por esto que se buscarán espacios para compensar las asimetrías con las que llegan los aspirantes.

Es importante destacar que los altos porcentajes de deserción y pérdida de año de los estudiantes universitarios conllevaron graves consecuencias personales, familiares, económicas y sociales. En este marco, la UTE diseña un Sistema de Admisión y Nivelación que asegura la igualdad de oportunidades para el ingreso y permanencia, sin detrimento de la calidad académica, con unas bases conceptuales que definen calidad y equidad. Equidad, como el principio ético, jurídico que controla y humaniza la justicia, para apoyar a la prudente aplicación de la ley en un caso concreto.

Se relaciona con las condiciones de igualdad, su aplicación crítica contextualizada de acuerdo con la realidad sociocultural del individuo.

La calidad de la Educación Superior está relacionada con el mejoramiento continuo, que se evidencia en los procesos y resultados de la formación profesional integral.

Un indicador de la calidad de la educación se relaciona con la permanencia de los estudiantes y, en este sentido, el Sistema de Admisión y Nivelación de la UTE además de eliminar las asimetrías en la formación de los estudiantes, garantiza el ingreso a las diferentes carreras, con una preparación integral por competencias que asegure calidad académica.

Perfil de ingreso a la UTE

Dado el carácter polivalente de los estudios ofertados en las distintas unidades de la Universidad Tecnológica Equinoccial, la formación científica básica así como los conocimientos y capacidades relacionadas con la vida social son las condiciones suficientes para asimilar la

enseñanza y desarrollar las aptitudes y facultades profesionales. En este esquema, el perfil para ingresar a la UTE requiere los siguientes rasgos:

- **Examen de aptitud**

Evalúa la capacidad para enfrentar estudios universitarios, desde el perfil de ingreso propuesto por la Universidad.

- **Examen de conocimientos generales**

Evalúa los conocimientos básicos que habilitan al postulante para el primer nivel de la Carrera seleccionada.

- **Propedéutico**

Para cubrir las exigencias de una comunidad cada vez más competitiva y alcanzar un nivel de excelencia, antes de iniciar su carrera los postulantes que no superaron el nivel requerido para ingresar a primer nivel de cualquier Carrera, deben cursar el Propedéutico, aporta para que el estudiante nivele competencias, asegurando la calidad de permanencia en su Carrera cuando ingrese a primer nivel.

Tiene un carácter general en función de que potencia las competencias básicas para ingresar a la Universidad y uno de carácter particular desde las exigencias de cada una de las Facultades.

3.2 Sistema de Admisión y Nivelación de la UTE

La Universidad Tecnológica Equinoccial es una institución cofinanciada que pertenece al Sistema de Educación Superior del Ecuador, por tal razón y en cumplimiento de la ley, dispone de un Sistema de Admisión y Nivelación denominado SIAN, que tiene como finalidad dar los lineamientos generales de las actividades que la Universidad debe realizar para garantizar la transparencia y equidad del proceso de admisión de estudiantes.

El Sistema de Admisión y Nivelación de la UTE está constituido por dos subprocesos interrelacionados: Admisión de estudiantes y Nivelación de estudiantes.

El proceso de admisión tiene como resultado una lista de aspirantes admitidos en la Universidad para primer nivel y curso de nivelación, y brinda la información requerida por los procesos de matriculación y sistemas académicos de la Universidad.

3.2.1 Descripción del proceso de Admisión de la UTE

La admisión de estudiantes es un proceso sistémico que involucra a varios departamentos de la Universidad: Vicerrectorado General Académico, Facultades, Institutos, Departamentos Académicos, Equipo Interdisciplinar y Sistema de Educación a Distancia, quienes tienen un rol importante en cada parte del proceso y generan la documentación del sistema.

El proceso de Admisión es soportado por la aplicación informática denominada “Sistema Integrado de Admisión y Nivelación (SIAN)” que permite la administración de perfiles de usuario según su nivel de autoridad, la creación y operación las preguntas de las áreas de conocimientos a evaluarse, ponderación de datos y emisión de resultados, y la aplicación denominado “Sistema de Temarios” para la publicación de los temas de las diferentes áreas de conocimientos que se evaluarán durante el proceso. Las dos aplicaciones están integradas con el Sistema Integrado Académico y Financiero correspondiente al proceso de matriculación de estudiantes.

Debido a que la Universidad no dispone de documentación formal sobre el proceso de admisión de estudiantes se presentará una descripción general del proceso desarrollada por los autores de la presente tesis en cooperación con los responsables y dueños del proceso.

Para describir ordenadamente los subprocesos, se utilizará el formato del cuadro 2, contiene los campos principales con información relevante para realizar la evaluación de riesgos.

El mapa de procesos está basado en niveles de profundidad de acuerdo a su detalle; el nivel 0 corresponde a la descripción y explicación general del proceso de Admisión de Estudiantes para pregrado en modalidad presencial para el Campus Quito, luego a medida que se describe cada subproceso se asigna un nivel de profundidad diferente, ejemplo nivel 1, nivel 2, etc.

Cuadro 2: Formato del mapa de procesos

Nombre del proceso		Nivel
Dueño del proceso		
Objetivo		
Descripción		
Recursos		
Entradas	Salidas	
Controles		
Actividades		

La descripción del proceso de admisión de aspirantes para pregrado en modalidad presencial en Campus Quito se presenta en el Cuadro 3.

Cuadro 3: Descripción del proceso de admisión de aspirantes

<table>
<tr><td colspan="2">Nombre del proceso: Admisión de aspirantes para pregrado en modalidad presencial en Campus Quito (es parte de un sistema integral para admisión y nivelación: SIAN)</td><td>Nivel: 0</td></tr>
<tr><td colspan="3">Dueño del proceso:
Vicerrectorado General Académico</td></tr>
<tr><td colspan="3">Objetivo
Dar cumplimiento a lo establecido en la constitución política del Ecuador y la LOES respecto a la Admisión de aspirantes que desean estudiar en las instituciones de Educación Superior, garantizando los principios de equidad, autonomía responsable, igualdad de oportunidades, calidad, pertinencia e integralidad en este proceso.</td></tr>
<tr><td colspan="3">Descripción

En el año se establecen dos periodos para la recepción de exámenes de aptitud y de conocimiento a los aspirantes mediante un proceso de selección y admisión, se utiliza un sistema informático desarrollado localmente y que es ejecutado en las computadoras de los laboratorios de la institución. Posteriormente, con las ponderaciones asignadas por las autoridades de la Universidad y mediante un proceso automático dentro del sistema se calculan los resultados de los exámenes y se emiten los resultados de los aspirantes admitidos. Los aspirantes pasan a primer nivel en caso de haber culminado satisfactoriamente los dos exámenes sobre el puntaje exigido, o al curso de nivelación de la UTE.</td></tr>
<tr><td>Recursos</td><td colspan="2">• Laboratorios de computación
• Sistemas computacionales de la UTE que dan soporte al macro proceso de admisión de aspirantes
• Docentes</td></tr>
</table>

	• Personal Administrativo • Alta dirección de la organización
Entradas • Personas que se inscriben en la UTE para seguir una carrera de estudios de pregrado en modalidad presencial en el campus Quito.	**Salidas** • Lista de aspirantes seleccionados por la UTE (primer nivel de carrera o curso de nivelación)
Controles Todos los controles se detallan en los niveles de profundidad nivel 1	
Actividades Todas las actividades se detallan en los niveles de profundidad nivel 1	

El diagrama del proceso de admisión de aspirantes para pregrado en modalidad presencial en Campus Quito se presenta en la Figura 21.

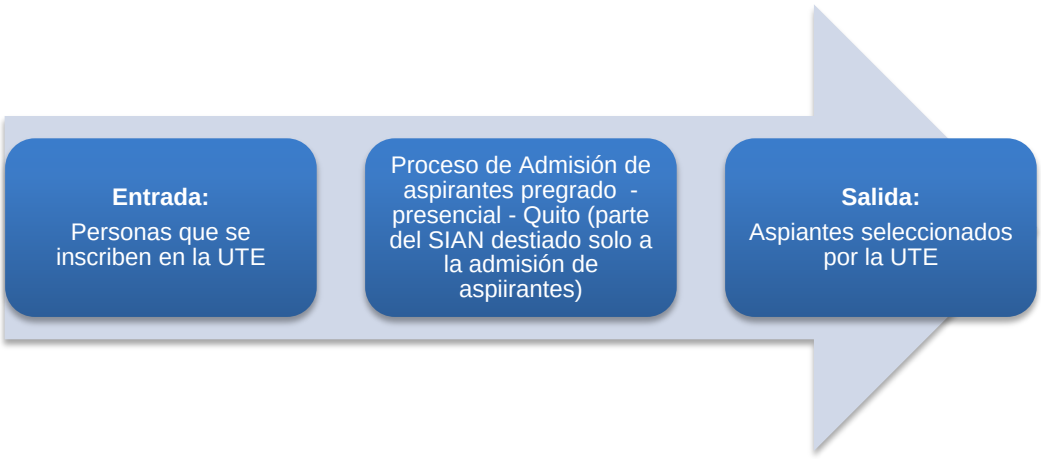


Figura 21: Diagrama de proceso de Admisión de aspirantes

El proceso de admisión está constituido por cuatro subprocesos:

- Diseño y elaboración de exámenes
- Inscripción de aspirantes
- Recepción de exámenes
- Selección de aspirantes e inducción de estudiantes

En la figura 22 se muestra el flujo completo del proceso de admisión de estudiantes.

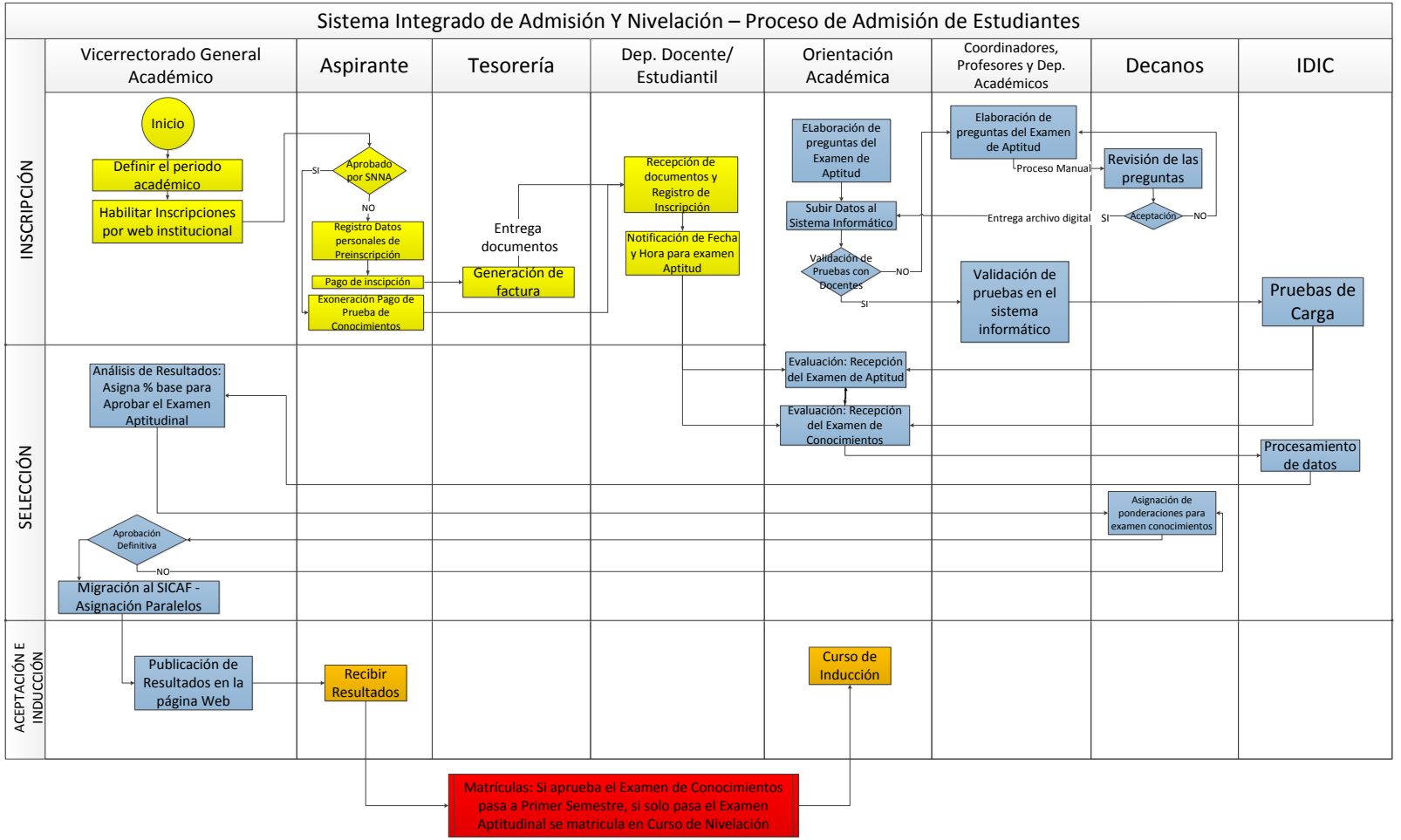


Figura 22: Diagrama de flujo del Sistema de Admisión de la UTE

3.2.2 Diseño y elaboración de exámenes

El departamento de Orientación Académica desarrolla las preguntas que formarán parte del examen de aptitud y coordina con los Departamentos Académicos, áreas de profesores, Coordinadores de Carreras y Facultades para el desarrollo de las preguntas del examen de conocimientos.

Debido a la gestión interna de la universidad, este proceso consta de dos partes complementarias entre sí:

- Diseño y elaboración de exámenes automatizado para toda la Universidad
- Diseño y elaboración de exámenes manual para la Facultad de Arquitectura y Facultad de Ciencias de la Salud.

El mapa del proceso diseño y elaboración de exámenes se describe en el Cuadro 4.

Cuadro 4: Descripción del Subproceso de Diseño y Elaboración de exámenes

Nombre del proceso: Diseño y Elaboración de exámenes	Nivel: 1.1
Dueño del proceso: Vicerrectorado General Académico **Dueño del subproceso 1:** Facultad de Arquitectura **Dueño del subproceso 2:** Facultad de Ciencias de la Salud	
Objetivo del proceso: Crear el banco de preguntas y diseñar el examen para la recepción de los exámenes que se tomarán a los aspirantes, mediante un mecanismo de asignación aleatoria de preguntas. Paralelamente, se diseña y elabora exámenes de conocimientos para la	

Facultada de Arquitectura y la Facultad de Ciencias de la Salud. En este caso, se consideran dos subprocesos complementarios en el mismo nivel que apoyan al proceso general de nivel 1.2:

- **Subproceso 1:** Diseño y elaboración de examen de conocimientos de la Facultad de Arquitectura
- **Subproceso 2:** Diseño y elaboración de examen de conocimientos de la Facultad de Ciencias de la Salud

Objetivo Subprocesos 1 y 2: Desarrollar los bancos de preguntas de los exámenes de conocimientos para los aspirantes a las Facultades de Arquitectura y Ciencias de la Salud.

Descripción

Docentes expertos de la UTE elaboran las preguntas de los exámenes de aptitud y conocimientos en computadoras personales o de la UTE, son aprobadas por jefe de cada área del departamento académico o las autoridades de la facultad, según sea el caso. Posteriormente, el jefe de los departamentos académicos entrega los bancos de las preguntas al departamento de Orientación Académica, quienes validan la información e ingresan los datos al sistema informático.

Conjuntamente con los docentes asignados por los departamentos académicos realizan las validaciones del examen; con los estudiantes de cursos de nivelación de la Universidad realizan un piloto de la recepción del examen y finalmente con el personal técnico del IDIC realizan las pruebas de carga del sistema.

En lo referente a la Facultad de Arquitectura, las preguntas del examen de admisión de aspirantes son desarrolladas por un docente de la Facultad usando una computadora asignada por la UTE. No existe validación formal de las preguntas para determinar los exámenes tipo para el periodo vigente. Los exámenes son impresos poco tiempo antes

<table>
<tr><td colspan="3">del inicio de la recepción de los exámenes.

En lo referente a la Facultad de Ciencias de la Salud, el examen de admisión es elaborado mediante reuniones periódicas de docentes expertos, validado y aprobado por los coordinadores de las carreras de la facultad. Se elabora un listado de aspirantes a la Facultad, cada aspirante está asociado a un número para rendir el examen.</td></tr>
<tr><td>Recursos</td><td colspan="2">• Docentes expertos
• Fuentes bibliográficas
• Personal Administrativo de la UTE
• Servicios web
• Sistemas informáticos internos de la UTE
• Autoridades de la UTE
• Experiencias y preguntas de pruebas de periodos anteriores
• Computadores asignados a los docentes en la Universidad
• Internet
• Bases de datos científicas</td></tr>
<tr><td colspan="2">Entradas
• Mallas curriculares de la oferta académica
• Preguntas de exámenes tomados en periodos anteriores
• Conocimientos de docentes expertos
• Base de datos de conocimientos
• Bibliografía</td><td>Salidas
• Examen de aptitud automatizado, validado y aprobado.
• Examen de conocimientos automatizado, validado y aprobado.
• Examen de conocimientos de Facultad de Arquitectura</td></tr>
</table>

• Requisitos regulatorios internos y externos	aprobado • Examen de conocimientos de Facultad de Ciencias de la Salud aprobado

Controles

- Aprobación de las preguntas
- Validación de preguntas
- Destrucción de las pruebas impresas para validación
- Lista de verificación de las preguntas ingresadas en el sistema por parte de Orientación Académica

Actividades del proceso

- Los docentes expertos de cada Facultad o área de conocimientos se reúnen periódicamente para elaborar las preguntas.
- Las preguntas se aprueban por parte del coordinador de la carrera o del área.
- Las preguntas se graban en un medio digital (comúnmente CD) y se entregan al departamento de Orientación Académica.
- El personal del Departamento de Orientación Académica ingresa las preguntas en el sistema informático SIAN.
- Un representante de los docentes realiza una validación de las preguntas subidas al sistema
- Se realiza una prueba piloto del examen para verificar la pertinencia y no ambigüedad de las preguntas del examen.
- Se realiza una prueba de carga del sistema informático en laboratorios del IDIC para minimizar los errores en la aplicación.

Actividades del subproceso 1

- Un docente experto de la Facultad de Arquitectura desarrolla y diseña los exámenes tipo en base a su experiencia y el banco de preguntas de periodos anteriores.
- El coordinador imprime y transporta los exámenes la Facultad de Arquitectura hacia las aulas asignadas.

Actividades del subproceso 2

- Los grupos de expertos de la Facultad de Ciencias de la Salud elaboran un banco de preguntas mediante reuniones periódicas y planificadas.
- Los bancos de preguntas son aprobados por los coordinadores
- Se realiza una lista de aspirantes enumerados asociados a una hoja de examen y de respuestas.

El diagrama del proceso diseño y elaboración de exámenes se presenta en la Figura 23.

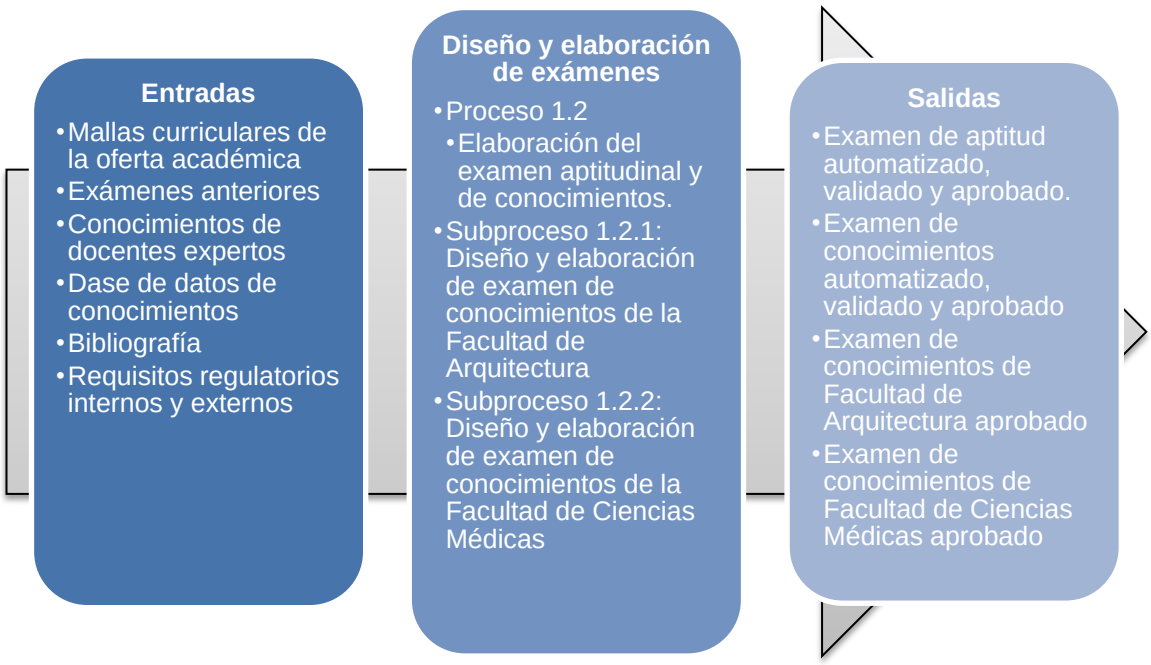


Figura 23: Diagrama del proceso diseño y elaboración de exámenes

3.2.3 Inscripción de aspirantes

La inscripción de aspirantes es un proceso de interacción entre la Universidad y los aspirantes que aspiran a una carrera universitaria, la finalidad es permitir el registro de cierta información en el sistema universitario de la UTE, sistema que posteriormente sirve como un medio para la revisión de los resultados de los puntajes obtenidos. En el Cuadro 5 se presenta el mapa de procesos de la inscripción de aspirantes.

Cuadro 5: Mapa de procesos de Inscripción de aspirantes

Nombre del proceso: Inscripción de aspirantes	Nivel: 1.2
Dueño del proceso: Orientación Académica	
Objetivo Permitir a los aspirantes inscribirse en el sistema de nivelación y admisión UTE para optar por una carrera universitaria, mediante la recepción y	

<table>
<tr><td colspan="3">validación de la información y documentación necesaria para cumplir con requisitos establecidos por la institución.</td></tr>
<tr><td colspan="3">Descripción

Las personas interesadas deben pre-inscribirse en la sección de inscripciones de la página web UTE y digitar la información requerida. Luego realizar el pago de la inscripción en la Tesorería de la UTE (en los casos pertinentes, si es aspirante es becado del SNNA no cancela ningún valor por la inscripción, pero si debe presentar documentación respectiva para rendir el examen de conocimientos) y presentar la documentación de respaldo en el Departamento Docente – Estudiantil, posteriormente se genera la fecha, horario y laboratorio asignado para rendir el examen.</td></tr>
<tr><td>Recursos</td><td colspan="2">• Personas que se inscriben
• Personal Administrativo de la UTE
• Servicios web
• Sistemas informáticos internos de la UTE
• Computadoras</td></tr>
<tr><td colspan="2">Entradas

• Personas que se inscriben en la UTE para seguir una carrera de estudios de pregrado en modalidad presencial en el campus Quito.
• Listado de personas becadas por el SNNA
• Oferta académica de la UTE</td><td>Salidas

• Lista de personas inscritas y validadas para rendir en el examen aptitudinal y de conocimientos en las fechas, horarios y laboratorios establecidos.
• Información ingresada por los aspirantes
• Listado de correos electrónicos de los aspirantes.</td></tr>
</table>

Controles

- Verificación de documentos habilitantes por el SNNA.
- Verificación de documentación que son requisitos en la UTE.

Actividades

- Vicerrectorado General Académico establece un periodo para inscripciones de los aspirantes.
- Se habilita el acceso a enlace de la página web institucional.
- Los aspirantes deben ingresar sus datos personales (número de cédula, nombres, los correos electrónicos personales) en el Sistema de Temarios, el acceso se realiza utilizando el número de cédula. Los aspirantes deben realizar un pago de la inscripción en la Tesorería de la Universidad. Si las personas son becados por el SNNA, únicamente requieren presentar el documento habilitante para la exoneración del pago.
- El Departamento Docente-Estudiantil valida la información ingresada al sistema utilizando los documentos físicos. Para los aspirantes nuevos habilita en el sistema el horario, fecha y laboratorio para rendir los dos exámenes, en el caso de los becados por el SNNA únicamente el examen de conocimientos.
- La información del aspirante es utilizada por el Departamento de Orientación académica para enviar notificaciones y directrices sobre el examen y su preparación.

El diagrama del subproceso de Inscripción de Aspirantes se presenta en la Figura 24.

Figura 24: Diagrama del proceso de inscripción de aspirantes

3.2.4 Recepción de exámenes

La Universidad evalúa a los aspirantes mediante dos exámenes: conocimientos generales y específicos de los aspirantes. Si el estudiante aprueba el examen de aptitud, será admitido en la Universidad y estará apto para matricularse en el curso de nivelación. Si el estudiante aprueba el examen de conocimientos puede matricularse en el primer nivel de carrera.

Durante la recepción de exámenes, el aspirante debe acudir a las instalaciones de la Universidad, un funcionario organiza los grupos de aspirantes en los exteriores de los edificios, como se visualiza en la figura 25.

Figura 25: Estudiantes formados, según el aula asignada listos para revisar autenticación.

Posteriormente, el personal de seguridad verifica las credenciales de los aspirantes y la hoja de inscripción durante el ingreso a los laboratorios de computación (IDIC) según los datos en la inscripción, como se visualiza en la Figura 26.

En las aulas asignadas, un docente tutor imparte las indicaciones generales, verifica la lista y la identidad de cada aspirante, Al finalizar el turno del examen notifica al departamento de Orientación Académica los incidentes que se presentaron durante el examen.

Figura 26: Ingreso de los aspirantes al edificio del IDIC

Los aspirantes ingresan sus credenciales en la aplicación informática, validan sus datos personales y el sistema les presenta preguntas aleatorias originadas de los bancos de preguntas elaboradas en el proceso de “Diseño y elaboración de exámenes”. El examen de aptitud tiene una duración de 45 min (becados del SNNA no rinden este examen) y el examen de conocimientos de 40 min, tiempo en el cual el docente tutor mantiene un control de la aula, como se muestra en la Figura 27.

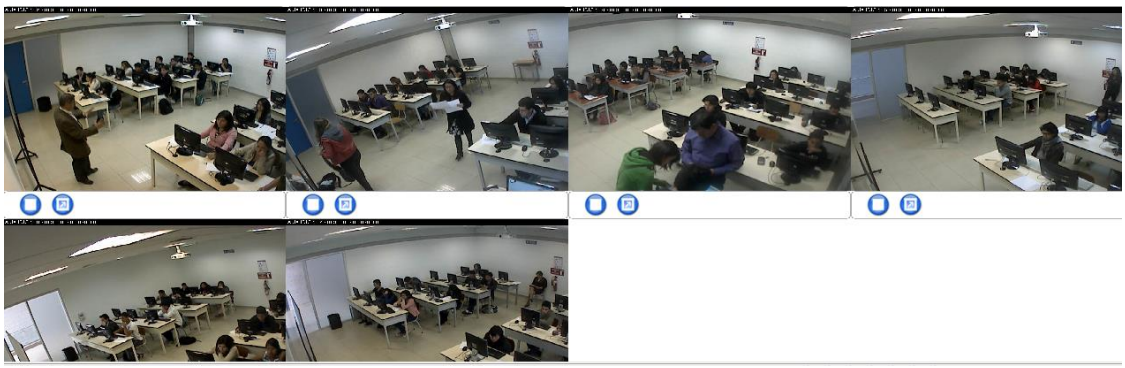


Figura 27: Aspirantes rindiendo examen de ingreso

El mapa del proceso de recepción de exámenes se detalla en el Cuadro 6, está dividido en dos partes:

- Recepción de exámenes utilizando un sistema informático, aplicado a toda la Universidad.
- Recepción y calificación de exámenes de conocimientos de forma manual para la Facultad de Arquitectura y Facultad de Ciencias de la Salud.

Cuadro 6: Descripción del proceso de recepción de exámenes

Nombre del proceso: Recepción de exámenes	Nivel 1.3
Dueño del proceso: Orientación Académica **Dueño del subproceso 1:** Facultad de Arquitectura **Dueño del subproceso 2:** Facultad de Ciencias de la Salud	

Objetivo del proceso: Receptar los exámenes de aptitud y de conocimientos de los aspirantes para el ingreso a la Universidad.

Objetivo de los subprocesos 1 y 2: Realizar la toma de los exámenes de conocimientos para los aspirantes de la Facultad de Arquitectura y de la Facultad de Ciencias de la Salud, calificar y subir las notas al sistema informático.

Descripción

La recepción de exámenes se realiza en las instalaciones de la Universidad, de acuerdo a los horarios, fechas y aulas asignadas en el subproceso de inscripción.
Los exámenes automatizados son tomados en los laboratorios de computación de la Universidad utilizando el sistema informático SIAN y son vigilados por docentes tutores asignados por cada facultad. Los resultados por aspirante se muestran al finaliza el proceso de nivel 0.

En el caso de la Facultad de Arquitectura y la Facultad de Ciencias de la Salud, los exámenes de conocimientos se toman manualmente, los docentes califican los exámenes y luego las notas se ingresan al sistema informático SIAN.

Recursos	• Docentes tutores responsables de las aulas • Laboratorios computacionales • Instalaciones de la UTE • Personal Administrativo de la UTE • Servicios web • Sistemas informáticos internos de la UTE • Autoridades de la UTE • Redes computacionales, Intranet e Internet

<table>
<tr><td></td><td colspan="2">• Bases de datos</td></tr>
<tr><td colspan="2">Entradas
• Lista de aspirantes habilitados para rendir los exámenes de aptitud y de conocimientos
• Examen de aptitud automatizado validado y aprobado
• Examen de conocimientos validado y aprobado.
• Examen de conocimientos de Facultad de Arquitectura aprobado
• Examen de conocimientos de Facultad de Ciencias de la Salud aprobado</td><td>Salidas
• Lista de aspirantes que rindieron sus exámenes
• Exámenes de aptitud resueltos por los aspirantes
• Base de datos de exámenes de aptitud calificados
• Base de datos de exámenes de conocimientos calificados
• Exámenes de conocimientos de aspirantes a la Facultad de Arquitectura tomados y calificados
• Exámenes de conocimientos de aspirantes a la Facultad de Ciencias de la Salud tomados y calificados</td></tr>
<tr><td colspan="3">Controles
• Verificación de identidad de los aspirantes
• Firma de las hojas de dibujo por parte del docente encargado antes de entregarlas a los aspirantes
• Numeración de hojas de exámenes y hojas de respuestas (Fac. Ciencias de la Salud)
• Conteo de grupos de exámenes y comparación con las listas de asistentes a rendir los exámenes firmadas. (Fac. Ciencias de la Salud)</td></tr>
</table>

Actividades del proceso

- El personal de seguridad y tutores de aula validan la identidad de los aspirantes durante el ingreso a los laboratorios del IDIC, verifican la hoja de inscripción y la cédula de ciudadanía.
- El docente tutor de aula informa la modalidad del examen a los aspirantes de cada laboratorio.
- El docente tutor de aula verifica la identidad de cada aspirante.
- El docente tutor de aula controla el desarrollo del examen y gestiona los problemas que se presenten durante el examen.
- Los aspirantes firman la hoja de asistencia al finaliza el examen y retira del aula.
- Los resultados son almacenados en la Base de datos del sistema informático.

Actividades del subproceso 1

- El coordinador entrega los exámenes a los docentes tutores de aula.
- El docente tutor de aula verifica la identidad de los aspirantes que asisten a rendir el examen de conocimientos de la Facultad de Arquitectura.
- El docente tutor de aula entrega los exámenes impresos a los aspirantes.
- Los docentes tutores reciben los exámenes resueltos y un grupo de 3 docentes califican al finalizar cada día.
- Se ingresan manualmente las notas al sistema informático.

Actividades del subproceso 2

- La coordinación entrega los exámenes y hojas de respuestas a los docentes encargados del control de las aulas, según el listado de alumnos.

- El personal de seguridad verifica la identidad de los aspirantes que asisten a rendir el examen de conocimientos de la Faculta de Ciencias de la Salud.
- El docente tutor de aula verifica la identidad de los aspirantes, reparte los exámenes impresos a todos los aspirantes.
- El docente tutor recibe los exámenes y hojas de respuestas, posteriormente en una sala restringida califica los exámenes utilizando las plantillas entregadas por la coordinadora de la facultad. Al finalizar esta actividad, los docentes entregan a los coordinadores de la facultad: los exámenes, las hojas de respuestas y un resumen del número de respuestas correctas por cada bloque de preguntas según el área de conocimiento evaluada en el examen.
- La secretaria verifica el número de exámenes y hojas de respuesta, ingresa los datos en una hoja de Excel y la envía para aprobación de la coordinadora y decano de la facultad.
- Las secretarias ingresan las notas de cada aspirante al sistema informático.

El diagrama del subproceso de recepción de exámenes se presenta en la Figura 28.

Figura 28: Diagrama del proceso de recepción de exámenes

Exámenes de conocimientos para aspirantes a la Facultad de Arquitectura, Artes y Diseño.

El proceso de la Facultad de Arquitectura para el diseño, elaboración y recepción de exámenes de conocimientos se muestra en la figura 29. Un docente designado por la facultad prepara los exámenes de dibujo técnico y artístico, dependiendo de la cantidad de aspirantes se elabora un examen para cada turno de examen, por lo general son 3 por cada día. Los exámenes de dibujo técnico se imprimen horas antes de la recepción del examen, el coordinador los transporta desde la Facultad de Arquitectura ubicado en la matriz hacia la Av. Occidental, entrega a los docentes tutores de aula de acuerdo al listado de aspirantes.

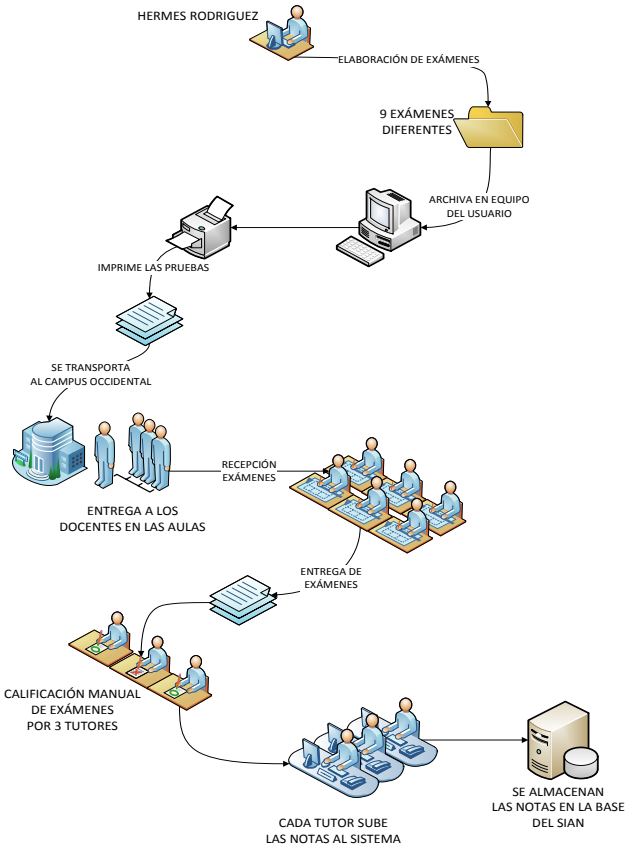


Figura 29: Descripción del desarrollo y evaluación del examen de conocimientos de la Facultad de Arquitectura

El primero examen es “dibujo técnico”, debido a su naturaleza dispone de menores controles que el examen de aptitud, evalúan los conocimientos y destrezas de los aspirantes para poder realizar dibujos y son menos propensos a copias. La Figura 30 muestra un grupo de estudiantes rindiendo el examen de dibujo técnico.

Figura 30: Rendición de examen de conocimientos – Arquitectura

El segundo examen “dibujo artístico” para los aspirantes a la Facultad de Arquitectura, Artes y Diseño es rendido en diferentes áreas del edificio con la custodia del tutor.

Luego de la rendición del examen un grupo de profesores de la facultad se encargan de evaluar e ingresar los datos en la aplicación SIAN.

Examen de conocimientos para aspirantes a la Facultad de Ciencias de la Salud.

El proceso de la Facultad de Ciencias de la Salud para el diseño, elaboración y recepción de exámenes de conocimientos, realizado por los autores de la presente tesis se muestra en la figura 31.

El examen evalúa los conocimientos previos de los aspirantes respecto a diversas áreas del conocimiento: anatomía, biología y física.

Se generan dos turnos para el examen, distribuidos en grupos de 20 por cada aula, se asigna un examen numerado y una hoja de respuestas numerada y ligada al examen para cada aspirante.

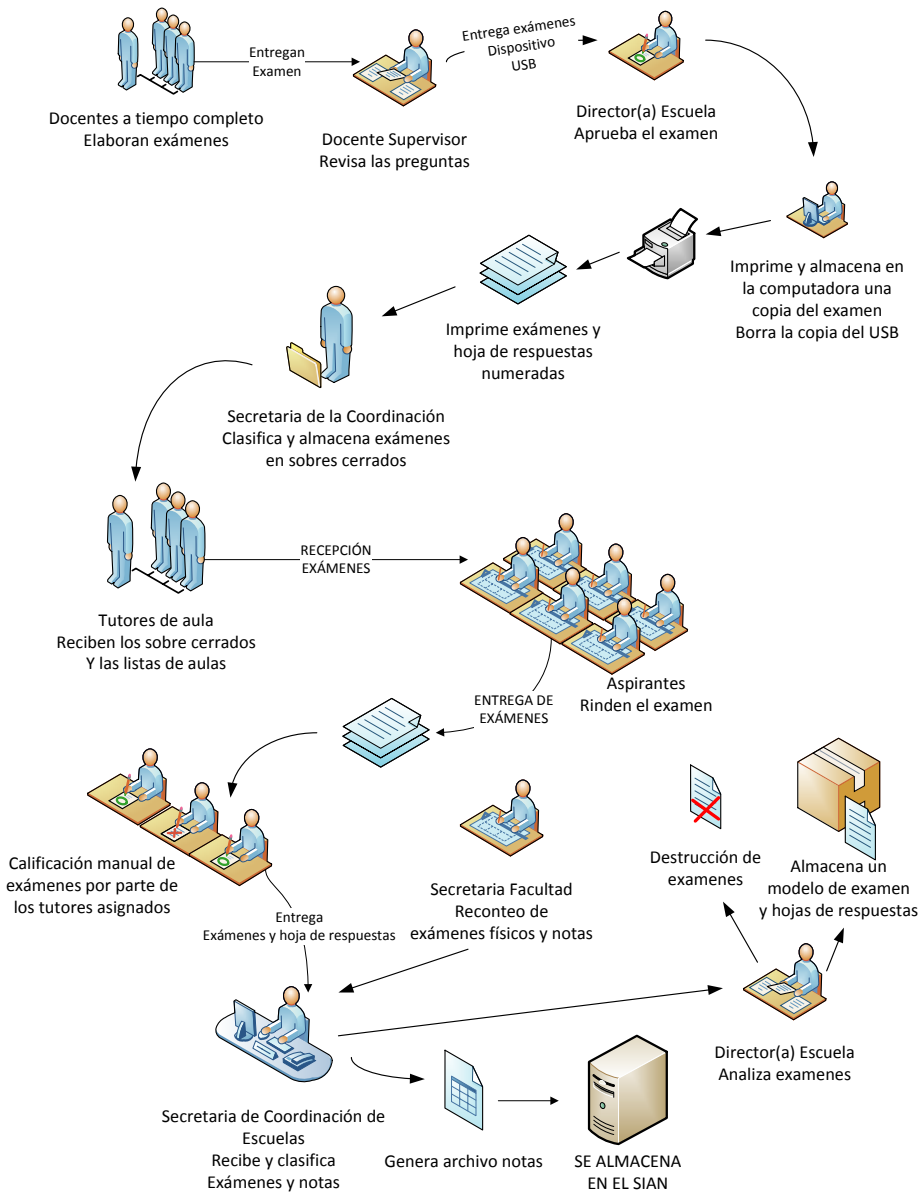


Figura 31: Descripción del desarrollo y evaluación del examen de conocimientos de la Facultad de Ciencias de la Salud

Durante el ingreso a las aulas se verifica la documentación de los aspirantes, son ubicados en diferentes aulas de acuerdo a listados publicados por la Facultad.

En cada aula, el docente tutor, verifica identidad de los aspirantes, explica las reglas para rendición del examen (uso de esfero, las pertenencias personales deben estar en la parte frontal del aula), distribuye los exámenes según la correspondencia entre el número de examen, la hoja de respuestas y la cédula, tal como se muestra en la Figura 32.

Figura 32: Verificación de identidad del examen de Medicina

Al finalizar el examen de cada turno, los aspirantes salen por la parte posterior del edificio, inmediatamente ingresa el siguiente grupo de aspirantes.

Al finalizar la recepción de los exámenes, los docentes tutores proceden a calificar los exámenes en una sala de acceso restringido, como se muestra en la Figura 33. La coordinadora de la Facultad explica la forma de calificar de los exámenes.

Figura 33: Calificación de exámenes – Facultad Ciencias de la Salud

Posteriormente, los docentes realizan la sumatoria de las preguntas correctas y entregan los exámenes calificados a las coordinaciones de Medicina y Odontología. Las secretarias de la Facultad verifican los exámenes físicos, preparan el archivo de información consolidada, el decano de la facultad autoriza el ingreso y se registran los datos en la aplicación SIAN.

3.2.5 Selección de aspirantes

En la selección de aspirantes, las autoridades (Vicerrectorado General Académico y Facultades) establecen los valores de ponderaciones del examen de aptitud y examen de conocimientos.

El mapa del proceso de asignación de ponderaciones se describe en el Cuadro 7.

Cuadro 7: Descripción del proceso de selección de aspirantes

Nombre del proceso: Selección de aspirantes	Nivel: 1
Dueño del proceso: Orientación Académica y Decanos de todas las Facultades	

<table>
<tr><td colspan="3">Objetivo
Establecer las ponderaciones y los puntajes mínimos que deben obtener los aspirantes para aprobar los exámenes de aptitud y de conocimientos.</td></tr>
<tr><td colspan="3">Descripción

Vicerrectorado General Académico de la UTE establece e ingresa la ponderación del examen de aptitud.

Los decanos establecen la ponderación para el examen de conocimientos, valores que son aprobados por Vicerrectorado General Académico.

Posteriormente, el sistema informático procesa los datos según los parámetros ingresados, emite resultados.

Vicerrectorado General Académico cierra el proceso y se migran los datos del sistema informático SIAN al sistema académico SICAF para establecer el periodo de matriculación y preparar horarios.</td></tr>
<tr><td>Recursos</td><td colspan="2">• Autoridades de la UTE
• Equipos de computación utilizados
• Servicios web
• Sistemas informáticos internos de la UTE
• Redes computacionales, Intranet e Internet
• Bases de datos</td></tr>
<tr><td colspan="2">Entradas
• Criterios de ponderación para la selección
• Ponderaciones de Vicerrectorado</td><td>Salidas
• Lista de aspirantes seleccionados para primer nivel o curso de nivelación en</td></tr>
</table>

<table>
<tr><td>y Decanos.
• Base de datos con las calificaciones de cada aspirante que rindió sus exámenes de aptitud y conocimientos según le correspondía</td><td>cada carrera.</td></tr>
<tr><td colspan="2">Controles
• Las ponderaciones establecidas por los Decanos de las diferentes Facultades
• Vicerrectorado General Académico aprueba las ponderaciones.</td></tr>
<tr><td colspan="2">Actividades
• Vicerrectorado General Académico establece la ponderación para el examen de aptitud.
• Los decanos de cada facultad establecen la ponderación para el examen de conocimientos.
• Vicerrectorado General Académico aprueba la ponderación para el examen de conocimientos de cada Facultad.
• Migran los resultados al SICAF para la matriculación.</td></tr>
</table>

El diagrama del proceso de asignación de ponderaciones se presenta en la Figura 34.

Figura 34: Diagrama del proceso de selección de aspirantes

3.2.6 Inducción

La inducción es un proceso posterior a la matriculación de los estudiantes, consiste en brindar charlas presenciales sobre las políticas, reglamentos de la Universidad y manejo de la plataforma informática.

CAPÍTULO 4

4 EVALUACIÓN DE RIESGOS Y BRECHA DE SEGURIDAD DE LA INFORMACIÓN

4.1 Metodología de evaluación de seguridad de la información

Se puede entender por metodología a la reunión de técnicas basadas sobre una filosofía común o esquema de trabajo, que se establecen en una plataforma conocida ciclo de vida.

La metodología a describirse es formulada por los autores de la presente tesis, está conformada por un conjunto de pasos a seguir en forma ordenada, necesarios para la evaluación de riesgos de seguridad y la determinación de la brecha respecto a la norma ISO/IEC 27001:2005.

Las etapas de la metodología son de carácter obligatorio, no se debe excluir ningún paso, en caso de hacerlo debe documentar el motivo de la exclusión.

La metodología está basada en las normas de gestión de riesgos de riesgos de seguridad de la información NTE INEN-ISO/IEC 27005:2012 y MAGERIT.

En la figura 35 se muestra la “Metodología de evaluación de seguridad”, describe los pasos a seguir durante la evaluación en la presente tesis, se debe cumplir con todas la etapas empezando desde RECOPILACION DE INFORMACIÓN.

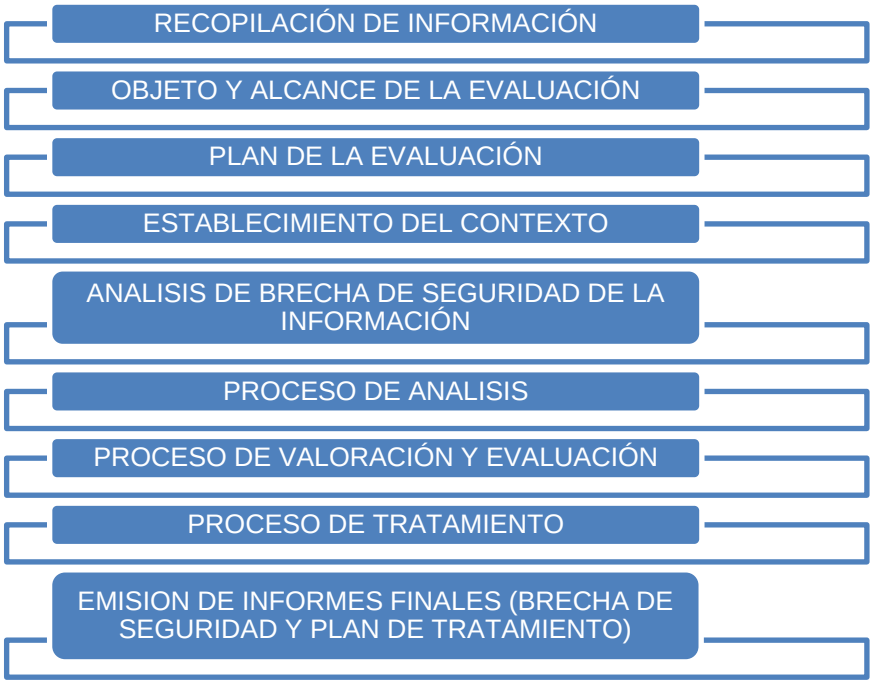


Figura 35: Metodología de evaluación de seguridad

4.1.1 Recopilación de información

Esta etapa se realiza la observación inicial del entorno de la organización a evaluar, consiste en recopilar información sobre los procesos de la organización, conocer las relaciones entre procesos y cuáles son los responsables de cada proceso.

En esta etapa los evaluadores tendrán un acercamiento general a la documentación, registros y recursos que se utilizan en los procesos.

El resultado de esta etapa se evidencia de la siguiente manera:

- Descripción general de la organización
- Lista de procesos de la organización
- Lista de responsables de cada proceso.
- Diagrama de relaciones entre procesos.

4.1.2 Objeto y alcance de la evaluación

En esta etapa se define cual será el objeto de la evaluación de seguridad y sobre qué procesos de la organización se aplicará.

El objeto es el motivo que conduce a la realización de la evaluación de seguridad de una organización.

El establecimiento del alcance permite enfocar la evaluación de riesgos a los requerimientos de la organización, con el fin de garantizar que todos los activos de información más importantes se toman en cuenta durante la evaluación de seguridad.

Esta etapa debe ser aprobada por la alta dirección de la organización para facilitar la evaluación de todos los procesos involucrados.

4.1.3 Plan de la evaluación

En etapa se realiza la planificación de la evaluación de seguridad, se evalúa la viabilidad de alcanzar los objetivos del proyecto con los recursos disponibles y las limitaciones existentes; la planificación se realizará en función de las etapas de la metodología propuesta.

En la planificación del proyecto se detallan las actividades a realizar durante la evaluación, la estimación de recursos y tiempos requeridos para la ejecución de cada actividad. El plan es un instrumento de apoyo para el evaluador puesto que ayuda a planificar y coordinar con los usuarios las actividades que se realizarán durante la evaluación, contiene las actividades que se van a realizar, el centro donde se realizará la evaluación, el día y hora previstos para la evaluación, el evaluador asignado y los departamentos responsables del proceso, el formato se presenta en el cuadro 8.

El plan de evaluación de seguridad se notificará previamente a los usuarios para acordar los tiempos de entrevistas y observaciones sobre el proceso.

Cuadro 8: Plan de evaluación de seguridad

Evaluación basada en ISO/IEC 27001 e ISO/IEC 27005				Departamento / proceso 1	Departamento / proceso 2	Departamento / proceso 3	.....	.....	.....	.....
ACTIVIDAD	**CENTRO**	**EVALUADOR**	**HORARIO**							
				X	**X**					
						X	**X**			
									X	**X**

Los documentos de salida de esta etapa son: el cronograma del proyecto y el plan de evaluación de seguridad.

4.1.4 Establecimiento del contexto

En esta etapa se especifica el contexto general de la evaluación, consiste en establecer los criterios básicos definidos por la alta dirección de la organización. Los criterios son:

- **Criterios de evaluación del riesgo:** Determina el riesgo de la seguridad de la información de la organización, teniendo en cuenta: el valor estratégico, criticidad de los activos, requisitos legales y reglamentarios, importancia de la disponibilidad, confidencialidad e integridad y las expectativas de las partes interesadas.
- **Criterios de impacto:** Se especifica en términos del daño o costo para la organización causados por un evento de seguridad

- **Criterios de aceptación del riesgo:** Especifica bajo qué criterios se aceptarán los riesgos, dependerán de las políticas, objetivos organizacionales y de las partes interesadas.

4.1.5 Análisis de brecha de seguridad de la información

En esta etapa se determina donde los déficits pueden estar ocurriendo y que pueden afectar al cumplimiento de los objetivos de seguridad institucionales.

El proceso de análisis de brechas propuesto en la presente metodología consiste en determinar el nivel de cumplimiento de los requisitos obligatorios de la norma ISO/IEC 27001:2005 y los controles especificados en el anexo de la norma.

La evaluación de los procesos se realiza mediante la investigación de campo e investigación documental-bibliográfica, utilizando técnicas de recolección de datos (entrevista, observación, empleo de documentos, entre otros) para registrar los la información más relevante del proceso, el formato se muestra en el cuadro 10.

El análisis cualitativo consiste en asignar un valor y porcentaje de cumplimiento por cada requisito y control de la norma ISO/IEC 27001:2005, en función la escala de cumplimiento. Para el presente trabajo se propone la escala de 4 niveles: 0,1, 2 y 3, como se muestra en el cuadro 9.

Cuadro 9: Escala de cumplimiento

Nivel	Cumplimiento	Porcentaje
0	No está definido ningún control	0%
1	No existen controles efectivos - Deficiencias considerables respecto a lo esperado	25%
2	Controles Básicos – Deficiencias menores con respecto a lo esperado para el requerimiento	50%
3	El requerimiento se cumple de manera efectiva	100%

Para la interpretación de los datos se debe hacer referencia a la norma ISO/IEC 27001:2005 y validar su cumplimiento. Los datos se registran en el formato que se muestra en el cuadro 10.

Cuadro 10: Formato de registro de cumplimiento normativo

Requisito normativo	Descripción	Aplica S/N	% Actual	Estado Actual	Cumplimiento			
					0	1	2	3

Siendo que en el cuadro 10:

- El “requisito normativo” corresponde al requisito o control especificado en la norma ISO/IEC 27001:2005
- El campo “descripción” corresponde a la explicación detallada del requisito normativo.
- El campo “Aplica”, especifica si un requisito o control normativo aplica al proceso evaluado, dependerá de la naturaleza de la organización y del alcance de la evaluación.
- El campo “% Actual” indica el porcentaje obtenido durante la evaluación, tiene correspondencia al nivel alcanzado respecto a la escala de cumplimiento.
- El campo “Estado Actual” describe en qué estado se encuentra el proceso evaluado respecto a un requisito o control específico.
- El campo “cumplimiento” especifica el nivel alcanzado (0, 1, 2 y 3) respecto a la escala de cumplimiento, la valoración dependerá de los evaluadores asignados al proceso.

La determinación del nivel de cumplimiento de cada capítulo, dominio de control y del sistema se obtiene a través del cálculo promedio de los valores parciales de cada requisito normativo. Por ejemplo, los valores de sistema de gestión de seguridad de la información, responsabilidad de la

dirección, auditorías del SGSI, revisión SGSI por la dirección y mejora del SGSI permiten obtener el porcentaje de cumplimiento total del proceso evaluado.

4.1.6 Proceso de análisis

En esta etapa la evaluación de seguridad se basa en riesgos, permite identificar los posibles riesgos que pueden afectar o causar daño a la organización.

La información obtenida en este proceso es valiosa para la gestión adecuada de los incidentes y eventos inesperados, y reducir los daños potenciales sobre las áreas de interés de la organización.

Los formatos y matrices desarrolladas en la presente metodología tratan de cumplir con los requerimientos de la información necesaria para cubrir la Norma NTE INEN-ISO/IEC 27005:2012.

El proceso de análisis y evaluación se compone de tres fases:

Identificación del riesgo

En esta etapa se determina que podría suceder y causar una pérdida potencial, comprender cómo, dónde y por qué podría causar esta pérdida.

Esta fase esta se compone de 4 actividades principales:

- **Identificación de activos**

Esta fase consiste en identificar todos los activos relevantes que forman parte del proceso evaluado y que requieren protección.

La identificación de activos se debe realizar con un nivel adecuado de detalle a fin de obtener información suficiente para la valoración de los riesgos.

La presente metodología, proporciona un listado de categorías de activos sugeridos por los autores, se basa en el Anexo B de la norma NTE INEN-ISO/IEC 27005:2012 y el Libro II de Catálogos de elementos de Magerit. Se han definido dos tipos: activos principales y activos de apoyo; cada activo con su categoría y subcategoría según se corresponda. En el Cuadro 11 y 12 se muestran las definiciones de los activos.

Cuadro 11: Definición de activos principales

Activos principales	
Categoría	**Subcategoría**
Procesos	
Información	Digital Físico Log

Cuadro 12: Definición de activos de apoyo

Activos de apoyo	
Categoría	**Subcategoría**
Servicios	
Software-aplicaciones	Aplicación del negocio Software Estándar
Hardware	Equipo Fijo – PC Equipo Fijo – Servidor Medios electrónico Equipo auxiliar
Red	Medios y Soportes Transmisión pasiva -activa
Personal	Personal de Toma decisiones Usuarios Desarrolladores Personal de operación/mantenimiento
Sitios	Zona
Organización	Proveedores

El evaluador de seguridad debe seleccionar los activos relacionados al proceso y registrarlos en el formato descrito en el cuadro 13.

Adicionalmente, se registra con una “x” los requerimientos de seguridad de la información (confidencialidad, integridad y disponibilidad) especificado por los dueños del proceso y la valoración inicial en escala

alto medio y bajo asignado por la alta dirección, el formato se muestra en el cuadro 14.

En el caso de los activos de información, se debe clasificar al activo en función de su nivel de:

a) Sensibilidad (confidencialidad):

- **“Uso público”:** Información puesta a disposición del público.
- **“Uso Interno”:** Información que está restringida al personal de la Universidad o de terceros a los que ha sido otorgado acceso a la información de la Universidad
- **“Confidencial”:** Información que está restringida a un conjunto de personas, unidad organizacional o funcional, cuya divulgación no controlada afectaría los recursos de la Universidad; y que es de interés para el desarrollo de sus funciones

b) Criticidad (disponibilidad)

- **“Crítico”:** Referencia a los sistemas de producción y que puede afectar directamente al normal funcionamiento de la Universidad.
- **“Necesario”:** Aquello que no afecta directamente al normal funcionamiento de la Universidad pero que se considera importante para trabajo normal de un grupo de personas.
- **“Opcional”:** Aquello que es totalmente opcional para las operaciones en ejecución y el logro de objetivos.

c) Integridad

- **“Integro”:** Aquello que hace referencia a los sistemas de producción y que puede afectar directamente al normal funcionamiento de la Universidad.
- **“No integro”:** Aquello que no afecta directamente al normal funcionamiento de la Universidad pero que se considera importante para trabajo normal de un grupo de personas.

Cuadro 13: Formato de registro de activos

				Custodio		Responsable			
ID Activo	**Nombre Activo**	**Sub categoría**	**Propietario**	**Funcionario**	**Cargo**	**Funcionario**	**Cargo**	**Ubicación**	**Dependencia**

Cuadro 14: Formato de clasificación y valoración inicial de activos

				Clasificación			Requerimientos SI			Valoración Inicial		
Categoría	**Sub categoría**	**ID Activo**	**Descripción**	**Sensibilidad**	**Criticidad**	**Integridad**	**C**	I	**D**	**C**	**I**	**D**

- **Identificación de amenazas**

Esta fase consiste en identificar las amenazas que potencialmente pueden causar daño a los activos, tales como información, procesos y sistemas.

Como parte de la metodología se debe identificar el tipo de amenaza, la amenaza en sí y el origen de la misma: Deliberada (D), Accidental (A) y Ambientales (E).

En función del anexo C de la norma NTE INEN-ISO/IEC 27005:2012 se sugiere utilizar los siguientes tipos de amenazas:

- Fallas técnicas
- Daño físico
- Perturbación debida a la radiación
- Compromiso de las funciones
- Pérdida de los servicios esenciales
- Eventos naturales
- Compromiso de la información
- Acciones no autorizadas

El registro de las amenazas se puede realizar en el formato del cuadro 15.

Cuadro 15: Formato de registro de amenazas

Categoría	Subcategoría	ID Activo	Activo	Descripción	Tipo	Amenaza	D	A	E

- **Identificación de controles**

De la evaluación de los controles existentes se puede identificar que vulnerabilidades y tomar acciones para determinar si eliminar, reemplazar por otro control más adecuado para mitigar los riesgos identificados o mantener el control.

En esta fase se deben identificar los controles existentes para evitar trabajo o costos innecesarios, y los controles planificados por la organización.

La identificación se basa en revisión de documentos, verificación con las personas responsables, revisiones en el sitio y observaciones.

El registro de los controles se debe realizar en el formato del cuadro 16.

Cuadro 16: Formato de registro de controles

				Amenazas				Controles (existentes)	
Categoría	Subcategoría	ID Activo	Activo	Amenaza	D	A	E	Tipo	Estado

- **Identificación de vulnerabilidades**

En esta fase se deben identificar todas las vulnerabilidades que pueden ser explotadas por las amenazas y pueden afectar a los activos.

Por cada amenaza se debe identificar las vulnerabilidades a nivel organizacional, en los procesos y procedimientos, gestión, personal, ambiente físico, configuraciones, hardware software e interacción con las partes externas, y registrarlas en el formato del cuadro 17.

Cuadro 17: Formato de registro de vulnerabilidades

			Amenazas				Controles (existentes)		Vulnerabilidades
Categoría	Subcategoría	Activo	Amenaza	D	A	E	Tipo	Estado	

Es importante mencionar que una vulnerabilidad por sí sola no presenta riesgo para la organización, dado que es necesaria la explotación de una amenaza.

4.1.7 Proceso de valoración y evaluación

En esta etapa se define la metodología de análisis que se va utilizará para estimar el riesgo, siendo: cualitativa, cuantitativa o una combinación de las dos.

Por lo general, la metodología cualitativa es menos compleja y costosa, utiliza calificativos cualitativos (alto, medio y bajo) para describir la magnitud de las consecuencias potenciales y la probabilidad de que ocurra. Se la utiliza para obtener una indicación general del nivel del riesgo y revelar los riesgos más importantes.

La metodología cuantitativa utiliza una escala de valores numéricos para calificar las consecuencias y probabilidades, es usada para realizar un análisis profundo de riesgos más importantes.

En la estimación del riesgo se realizan las siguientes fases:

Valoración de los activos

La valoración de los activos se realiza mediante métodos diferentes, dependerá del tipo de activo: procesos, información y activos de apoyo; a cada activo se asigna un valor según la Tabla 1.

Tabla 1: Referencia de valoración de activos

Valor del activo	**0**
	1
	2
	3
	4

a) Método de valoración de los activos primarios: “procesos”

El método consiste en seleccionar el valor más alto del activo de apoyo o de información que lo conforma.

b) Método de valoración de los activos primarios: “información”

El método consiste en calcular los datos en función de la clasificación de la información, criterios de seguridad especificados por usuarios en las entrevistas y la valoración inicial por parte de la alta dirección.

En el Cuadro 18 se muestran los valores de la clasificación de la información.

Cuadro 18: Criterios de clasificación de la información

Criterio	Clasificación	Valor
Sensibilidad	Público	1
	Interno	2
	Confidencial	3
Criticidad	Opcional	1
	Necesario	2
	Crítico	3
Integridad	No Integro	1
	Integro	2

Los requerimientos de seguridad de la información están detallados en la Tabla 2.

Tabla 2: Escala de valoración de los criterios de seguridad

Criterio	Si requiere	No requiere
Confidencialidad	1	0
Integridad	1	0
Disponibilidad	1	0

Los valores asignados por la alta dirección para la escala de Alto, Medio y Bajo se muestran en la Tabla 3.

Tabla 3: Escala de valoración inicial

Criterio	Alta (H)	Media (M)	Baja (L)
Confidencialidad	3	2	1
Integridad	3	2	1
Disponibilidad	3	2	1

El Valor del activo (VA) se obtiene de la sumatoria de los valores asignados en cada parámetro del activo de información. Posteriormente, se compara el valor resultante con el rango del valor descrito en el Cuadro 18, según las consideraciones siguientes:

$$\sum = 6\text{-}8 \rightarrow VA = 0$$

$$\sum = 9\text{-}11 \rightarrow VA = 1$$

$$\sum = 12\text{-}14 \rightarrow VA = 2$$

$$\sum = 15\text{-}17 \rightarrow VA = 3$$

$$\sum = 18\text{-}20 \rightarrow VA = 4$$

c) Método de valoración de los activos de apoyo: “servicios”

El valor de activos la categoría “servicios” se determina a partir del valor más alto las dos opciones siguientes:

- El valor más alto heredado de los activos dependientes.
- La sumatoria de los valores de los requisitos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad) especificada por los usuarios y la valoración inicial realizada por la alta dirección.

d) Método de valoración de los activos de apoyo

El método utiliza los requerimientos de seguridad de la información y los valores de la escala (Alto, medio y bajo) descritos en los Cuadros 20 y 21 para valorar los activos de apoyo.

El Valor del activo (VA') se obtiene de la sumatoria de los valores asignados en cada parámetro del activo de información. Posteriormente, se compara el valor resultante con el rango del valor descrito en el Cuadro 18, según las consideraciones siguientes:

$$\sum = 3\text{-}4 \rightarrow VA' = 0$$

$$\sum = 5\text{-}6 \rightarrow VA' = 1$$

$$\sum = 7\text{-}8 \rightarrow VA' = 2$$

$$\sum = 9\text{-}10 \rightarrow VA' = 3$$

$$\sum = 11\text{-}12 \rightarrow VA' = 4$$

e) Método de valoración de los activos de apoyo: "Hardware, Software, Red, Personas, Sitios y Organización"

Para los activos de categorías: Hardware, Software, Red, Personas, Sitios y Organización se considera el valor de acuerdo a las siguientes consideraciones: monetario de reposición del activo, de reconfiguración, pérdida, valor invertido en capacitación anual de personas, los sueldos por año, entre otros.

El estado financiero está clasificado en una escala de “Bajo” si el costo es menor a $5000, “Medio” si se encuentra entre $5000 y $50000, y “Alto” si supera $50000; los valores se muestran en la Tabla 4.

Tabla 4: Criterios para valoración monetaria de los activos

Criterio	Estado Financiero	Valor
Alto	> $50000	3
Medio	entre $5000 y $50000	2
Bajo	< $5000	1

También, se considera la sumatoria de los valores correspondiente a los requisitos de seguridad de la información y la valoración inicial (Confidencialidad, Integridad y Disponibilidad) realizada por las autoridades descritos en los Cuadros 20 y 21.

El Valor del activo (VA) se obtiene de la sumatoria de los valores asignados en cada parámetro del activo de información. Posteriormente, se compara el valor resultante con el rango del valor descrito en el Cuadro 18, según las consideraciones siguientes:

$$\sum = 4\text{-}6 \rightarrow VA = 0$$

$$\sum = 7\text{-}9 \rightarrow VA = 1$$

$$\sum = 10\text{-}11 \rightarrow VA = 2$$

$$\sum = 12\text{-}13 \rightarrow VA = 3$$

$$\sum = 14\text{-}15 \rightarrow VA = 4$$

Valoración de las consecuencias

La valoración de consecuencias permite determinar las acciones negativas que pueden producirse si se materializa una amenaza, en

relación a los objetivos y requerimientos institucionales de la seguridad de la información. Es decir, las consecuencias definen el riesgo real de producirse una amenaza.

Por cada activo se debe especificar describir el impacto en función de la pérdida de confidencialidad, pérdida de disponibilidad, pérdida de integridad, en el aspecto legal o reglamentario y las pérdidas económicas.

El valor del impacto se asigna de acuerdo a los criterios de afectación que se muestran en el Cuadro 19.

Cuadro 19: Definición de activos de apoyo

En Alta	**H**	Afecta directamente a la consecución de los objetivos, reponerse es muy costoso o llevaría mucho tiempo y esfuerzo
Media	**M**	Afecta a la consecución de los objetivos, sin embargo la recuperación es no es muy costosa o no requiere mucho esfuerzo
Baja	**L**	No afecta a la consecución de los objetivos

El evaluador debe registrar los datos en el formulario del cuadro 20.

Cuadro 20: Valoración de las consecuencias (impacto)

Activo	Valor del Activo	Código Riesgo	Consecuencias (Riesgo)					Valoración del Impacto
			CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO LEGAL	PERDIDAS ECONOMICAS / CONFIABILIDAD	
Activo1	4	R1	Consecuencia 1					H
Activo2	3	R2	Consecuencia 2					M
Activo3	3	R3		Consecuencia 3				H
Activo4	2	R4			Consecuencia 4		Consecuencia 5	B

Valoración de los incidentes

La valoración de los incidentes se basa en la facilidad de explotación de las vulnerabilidades y la probabilidad que una amenaza se materialice y afecte negativamente a las operaciones de la organización.

El valor se asigna de acuerdo a las escalas cualitativas descritas en los Cuadros 21 y 22.

Cuadro 21: Probabilidad de ocurrencia de una amenaza

Alta	**H**	<2 meses
Media	**M**	2-6 meses
Baja	**L**	> 6 meses

Cuadro 22: Facilidad de explotación de vulnerabilidad

Alta	**H**	Conocimientos avanzados en informática
Media	**M**	Conocimientos medios en informática
Baja	**L**	Conocimiento básicos en informática

El evaluador debe registrar los datos en el formato descrito en el Cuadro 23.

Cuadro 23: Definición de activos de apoyo

ID Activo	Activo	Valor del Activo	Código Riesgo	Probabilidad Amenaza	Facilidad de explotación
	Activo1	**3**	R1	H	M
	Activo2	**4**	R2	H	H
	Activo3	**2**	R3	M	B

Nivel de estimación

La estimación del riesgo de la metodología se basa en el segundo método propuesto en el Ejemplo E.2.1 del anexo E de la norma NTE INEN-ISO/IEC 27005:2012, propone realizar la valoración detallada de los

riesgos de la seguridad de la información en función del impacto y probabilidad.

El nivel de riesgo, se obtiene en función de la amenaza, vulnerabilidad y del impacto (consecuencia) en la organización descrita en la Tabla 5, corresponde a la Tabla E1.b) del anexo E de la norma NTE INEN-ISO/IEC 27005:2012.

Por ejemplo, si el impacto es alto (H), la probabilidad de una amenaza es media (M) y la facilidad de explotación de una vulnerabilidad es alta (H), entonces el nivel de riesgo es 5.

Tabla 5: Matriz de valoración detallada de los riesgos de seguridad de la información

	Probabilidad de ocurrencia - Amenazas	**L**			**M**			**H**		
	Facilidad de explotación vulnerabilidades	**L**	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**
Impacto en el negocio	L	0	1	2	1	2	3	2	3	4
	M	1	2	3	2	3	4	3	4	5
	H	2	3	4	3	4	5	4	5	6

El registro del nivel de cada riesgo se debe realizar en el formulario que se muestra en el cuadro 24.

Cuadro 24: Definición de activos de apoyo

ID Activo	Activo	Código Riesgo	Probabilidad Amenaza	Facilidad de explotación	Valoración Impacto	Nivel Riesgo
DAT-05	Activo1	R020	H	H	H	6
DAT-06	Activo2	R025	L	L	L	0
DAT-07	Activo3	R026	M	M	M	3
DAT-08	Activo4	R035	H	L	M	3
DAT-09	Activo5	R040	H	M	H	5

Evaluación del riesgo

En esta fase se compara los riesgos estimados con los criterios de evaluación del riesgo que se definieron en el establecimiento del contexto.

La evaluación del riesgo provee de la información necesaria para tomar decisiones sobre las acciones futuras.

4.1.8 Proceso de tratamiento

En conformidad con la norma NTE INEN-ISO/IEC 27005:2012, en esta etapa se seleccionan los controles para reducir, retener, evitar o transferir el riesgo y se presenta un plan de tratamiento del riesgo.

Las opciones consideradas para el tratamiento del riesgo que se utilizarán en esta etapa son:

Reducir el riesgo: Se deben seleccionar y proponer controles adecuados que satisfagan los requisitos identificados en la valoración y tratamiento del riesgo. Se deben tomar en cuenta los criterios de aceptación del riesgo, requisitos legales, reglamentarios y contractuales.

Retención del riesgo: No es necesario implementar controles adicionales si el nivel de riesgo satisface los criterios para su aceptación.

Evitación del riesgo: Si los riesgos identificados se consideran muy altos o los costos de implementar controles que los minimicen exceden los beneficios, se debe analizar la opción de retirar alguna actividad o modificar las condiciones en las cuales se desarrolla tal actividad.

Transferencia del riesgo: Se trata de compartir algunos riesgos con partes externas a la organización, tomando en cuenta que pueden generarse nuevos riesgos o modificar los existentes en su impacto o probabilidad.

En esta etapa, se deben priorizar los riesgos en función del valor y nivel de riesgo, como se muestra en la Tabla 6.

Tabla 6: Definición de activos de apoyo

Nivel Riesgo	Valor Riesgo
Prioritario	6
	5
Medio	4
	3
Bajo	2
	1
	0

Las opciones de tratamiento de riesgo se deben seleccionar con base en el resultado de la valoración, los costos y los beneficios esperados en cada opción.

A partir de la decisión organizacional se deberá elaborar el plan de tratamiento de riesgos con claridad en el orden de prioridad para implementar las acciones recomendadas.

El plan de tratamiento puede ser no valorado o valorado, dependerá del alcance de la evaluación; en el primero se describe las acciones a tomar y los responsables de ejecutarlas, en el segundo se incluye además, los costos y tiempos requeridos para ejecutar dichas acciones.

4.1.9 Emisión de Informes Finales: Brecha de seguridad de la información y Plan de tratamiento de los riesgos

Los informes finales lo constituyen dos entregables: el informe del análisis de la brecha de seguridad de la información y el plan de tratamientos de riesgos de seguridad de la información priorizado. Cada informe final se entrega a la alta dirección de la organización, debe ser claro, conciso y

ordenado, emitir recomendaciones fundamentadas en las mejores prácticas y dentro del contexto de la evaluación.

Los informes finales son vitales para la toma de decisiones, puesto que se registran los resultados de la evaluación y las recomendaciones para tomar acciones correctivas.

4.2 Aplicación de la metodología de evaluación de los riesgos de seguridad de la información

En la evaluación de seguridad se realizará en función de la metodología descrita en el numeral 4.1, con el objetivo presentar un plan de acción que permita alinear la gestión de seguridad con la norma ISO/IEC 27001:2005.

A fin de mantener la confidencialidad de la información solicitada por las autoridades de la Universidad Tecnológica Equinoccial, en la aplicación de la metodología se presentarán muestras de los resultados obtenidos de la evaluación.

4.2.1 Recopilación de información

En la recolección de información se realizaron entrevistas iniciales con las autoridades de la universidad, observación del funcionamiento de los procesos universitarios y revisión de documentación, registros y recursos que se utilizan en cada proceso.

Como resultado de esta etapa se desarrolló el capítulo 3 “Caso de Estudio”, describe la Universidad y el proceso completo de la Admisión de Estudiantes.

La universidad ha considerado importante la evaluación de seguridad para:

- Dar cumplimiento legal y dar muestra de la debida diligencia en el proceso de admisión de estudiantes.
- Mantener una buena reputación y confianza hacia la sociedad en general.
- Demostrar un proceso transparente y seguro que garantice igualdad de oportunidades a todos los aspirantes, seleccionarlos adecuadamente y que sea reflejo de sus conocimientos y aptitudes.

4.2.2 Objetivo y alcance de la evaluación

Las autoridades de la UTE han establecido que la evaluación de seguridad de la información se realice sobre proceso de Admisión de estudiantes de Pregrado Campus Quito, modalidad educación presencial, subprocesos: inscripción de aspirantes, diseño y elaboración de exámenes, recepción de exámenes y selección de aspirantes. No se incluirá la etapa de inducción de estudiantes considerando que no es un aspecto relevante para el objetivo del estudio.

La Universidad requiere garantizar el cumplimiento de los siguientes objetivos institucionales:

a) Estratégico

- Garantizar la igualdad de oportunidades a todos los aspirantes a través de un proceso de Admisión transparente y seguro.
- Asegurar que los resultados del proceso de admisión de estudiantes de pregrado muestren el fiel reflejo de los conocimientos y aptitudes de cada aspirante.
- Preservar la confianza de la sociedad y mantener la imagen de la Universidad

b) Cumplimiento

- Dar cumplimiento a lo establecido en la constitución política del Ecuador y la LOES respecto a la Admisión de aspirantes que desean estudiar en las instituciones de Educación Superior.
- Respetar los lineamientos institucionales especificados en la misión, visión y objetivos de la Universidad

En consenso con las autoridades de la Universidad y en alineación a los objetivos de la Universidad se determinaron los siguientes requerimientos de seguridad de la información:

- Garantizar que la información sea accesible solo a las personas autorizadas.
- Evitar la fuga de información, principalmente de las preguntas y respuesta de los exámenes de admisión que entran en el banco de preguntas del sistema informático.
- Garantizar que la información de los exámenes resueltos no se alterada en beneficio de ningún aspirante.
- Establecer los lineamientos necesarios para evitar la existencia de fraude en el proceso de admisión.
- Preservar la información durante el tiempo estipulado en la LOES.
- Proteger los derechos legales, incluyendo la privacidad.

Estos requerimientos de seguridad servirán de punto de partida para realizar análisis de gestión de riesgos del proceso de admisión y obtener un resultado enfocado a las necesidades de la Universidad.

El documento oficial firmado por el Rector se detalla en el Anexo A.

4.2.3 Plan de la evaluación

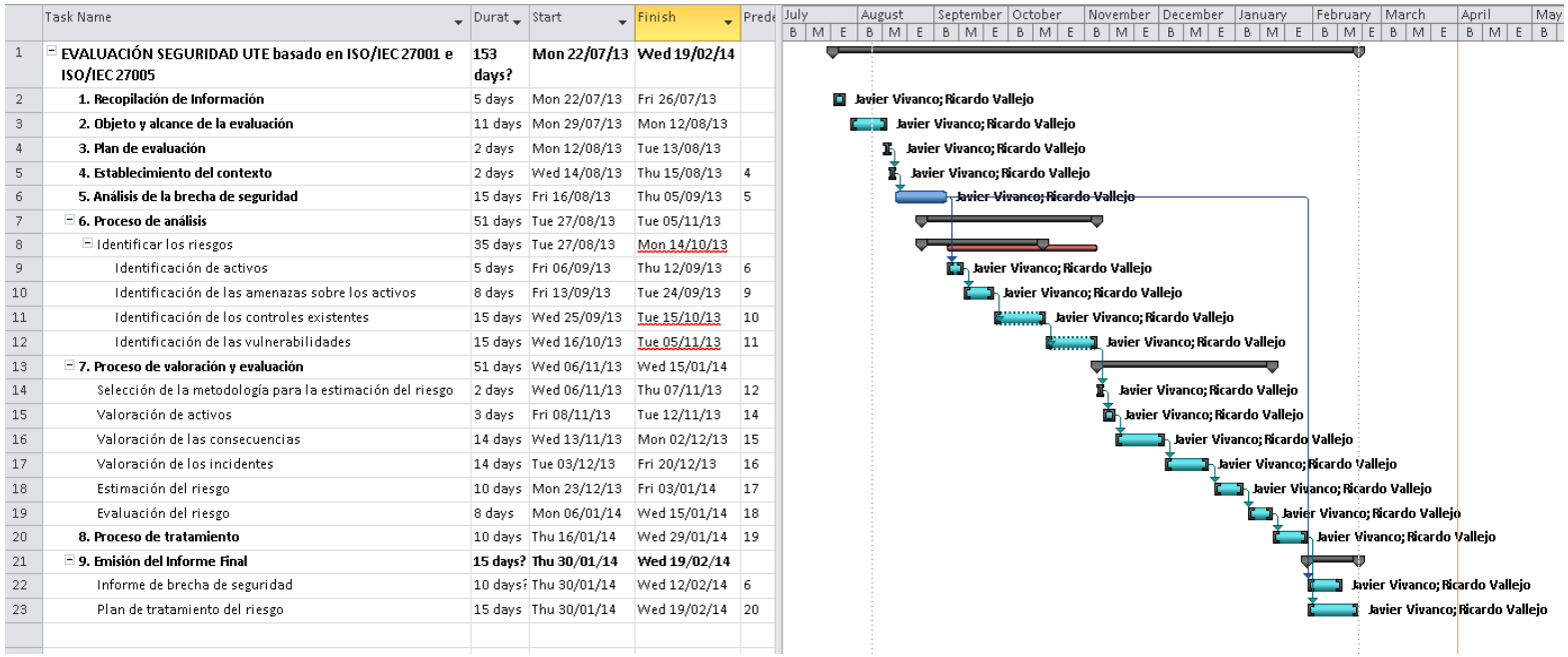
En esta etapa se realiza la planificación general del proyecto y el plan de evaluación de seguridad.

La planificación del proyecto se muestra en la Figura 36, contiene las actividades, tiempo requerido para la ejecución y los responsables asignados.

Para la elaboración del plan de evaluación de seguridad es necesario identificar al personal que está involucrado en el proceso para planificar las visitas, entrevistas, observaciones y pruebas de manera ordenada. La lista de funcionarios se presenta en el Cuadro 25.

El plan de evaluación de seguridad se muestra que se utilizará para la evaluación de seguridad se muestra en el Cuadro 26.

Figura 36: Planificación de la evaluación de seguridad



	Task Name	Durat	Start	Finish	Prede
1	**EVALUACIÓN SEGURIDAD UTE basado en ISO/IEC 27001 e ISO/IEC 27005**	**153 days?**	**Mon 22/07/13**	**Wed 19/02/14**	
2	**1. Recopilación de Información**	5 days	Mon 22/07/13	Fri 26/07/13	
3	**2. Objeto y alcance de la evaluación**	11 days	Mon 29/07/13	Mon 12/08/13	
4	**3. Plan de evaluación**	2 days	Mon 12/08/13	Tue 13/08/13	
5	**4. Establecimiento del contexto**	2 days	Wed 14/08/13	Thu 15/08/13	4
6	**5. Análisis de la brecha de seguridad**	15 days	Fri 16/08/13	Thu 05/09/13	5
7	**6. Proceso de análisis**	51 days	Tue 27/08/13	Tue 05/11/13	
8	Identificar los riesgos	35 days	Tue 27/08/13	Mon 14/10/13	
9	Identificación de activos	5 days	Fri 06/09/13	Thu 12/09/13	6
10	Identificación de las amenazas sobre los activos	8 days	Fri 13/09/13	Tue 24/09/13	9
11	Identificación de los controles existentes	15 days	Wed 25/09/13	Tue 15/10/13	10
12	Identificación de las vulnerabilidades	15 days	Wed 16/10/13	Tue 05/11/13	11
13	**7. Proceso de valoración y evaluación**	51 days	Wed 06/11/13	Wed 15/01/14	
14	Selección de la metodología para la estimación del riesgo	2 days	Wed 06/11/13	Thu 07/11/13	12
15	Valoración de activos	3 days	Fri 08/11/13	Tue 12/11/13	14
16	Valoración de las consecuencias	14 days	Wed 13/11/13	Mon 02/12/13	15
17	Valoración de los incidentes	14 days	Tue 03/12/13	Fri 20/12/13	16
18	Estimación del riesgo	10 days	Mon 23/12/13	Fri 03/01/14	17
19	Evaluación del riesgo	8 days	Mon 06/01/14	Wed 15/01/14	18
20	**8. Proceso de tratamiento**	10 days	Thu 16/01/14	Wed 29/01/14	19
21	**9. Emisión del Informe Final**	**15 days?**	**Thu 30/01/14**	**Wed 19/02/14**	
22	Informe de brecha de seguridad	10 days?	Thu 30/01/14	Wed 12/02/14	6
23	Plan de tratamiento del riesgo	15 days	Thu 30/01/14	Wed 19/02/14	20

Cuadro 25: Formulario de registro de personas involucradas en el proceso de Admisión de Estudiantes

Personal				
ID	**Departamento**	**Nombre**	**Cargo**	**Ubicación**
1	Vicerrectorado General Académico	Confidencial	Vicerrectora	Vicerrectorado – Rumipamba
2	Orientación Académica	Confidencial	Directora Dep. Orientación Académica	Orientación Académica – Rumipamba
3		Confidencial	Asistente Dep. Orientación Académica	Orientación Académica – Rumipamba
4		Confidencial	Secretaria Dep. Orientación Académica	Orientación Académica – Rumipamba
5	Facultades	Confidencial	Decano Fac. Arquitectura, Artes y Diseño	Decanato Fac. Arquitectura – Rumipamba
6		Confidencial	Decano Fac. Ingeniería	Decanato Fac. Ingeniería – Occidental
7		Confidencial	Decano Fac. Ciencias de la Salud	Decanato Fac. Ciencias de la Salud – Occidental
8		Confidencial	Decano Fac. Ciencias Económicas y Negocios	Decanato Fac. Ciencia Económicas – Occidental
9		Confidencial	Decano Fac. Ciencias Sociales	Decanato Fac. Ciencias Sociales – Occidental
10		Confidencial	Decano Fac. Turismo, Hotelería y Gastronomía	Decanato Fac. Turismo – Rumipamba
11	Fac. Ciencias de la Salud	Confidencial	Coordinadora Esc. Medicina	Coordinación Medicina – Occidental
12		Confidencial	Secretaria Coordinación	Secretaría Medicina – Occidental
13	Fac. Arquitectura	Confidencial	Coordinador Fac. Arquitectura	Oficina Doc. Tiempo Completo Arq. – Rumipamba
14	Departamentos Académicos	Confidencial	Jefe Departamento Ciencias Exactas - Ciencias Exactas: Química, Física, Matemática	Occidental, Bloque B, 4to piso
15		Confidencial	Jefe Departamento Humanística - Lingüística, sociología y psicología	Occidental, Bloque A
16		Confidencial	Fundamentos Matemáticas	Occidental, Biblioteca , Deparatamentos
18		Confidencial	Inglés Básico	Occidental, Idiomas, Coordinación
19		Confidencial	Fundamentos de Física	Occidental, Biblioteca , Deparatamentos
20		Confidencial	Fundamentos de Química	Occidental, Biblioteca , Deparatamentos
21		Confidencial	Introducción a la Economía	Rumipamba, Distancia
22		Confidencial	Introducción a la Sociología	Rumipamba
23		Confidencial	Introducción a la psicología	occidental, Biblioteca , Orientación académica
24	Instituto de Informática y Computación (IDIC)	Confidencial	Ingeniero de Sistemas	Edificio del IDIC - Occidental
25		Confidencial	Ingeniero de Sistemas	Edificio del IDIC - Occidental
26		Confidencial	Ingeniero de Sistemas	Edificio del IDIC - Occidental
27		Confidencial	Administrador Bdd	Edificio del IDIC - Occidental
28		Confidencial	Ingeniero de Manten. - Redes	Edificio del IDIC - Occidental
29		Confidencial	Ingeniero de Manten. - Hardware	Edificio del IDIC - Occidental

Cuadro 26: Plan de evaluación de seguridad de la información en el proceso de Admisión de Estudiantes de la UTE

Plan de Evaluación de Seguridad de la Información

Organización:	Universidad Tecnológica Equinoccial	**Fecha Actualización:** 02 Agosto 2013 **Rev 0.0**
Evaluadores:	Ing. Javier Vivanco R. (JV) Ing. Ricardo Vallejo (RV)	
Estándar:	ISO/IEC 27001:2005/ NTE INEN-ISO/IEC 27005:2012	
Lenguaje de la evaluación:	Español	

Objetivo	Evaluar la seguridad de la información del proceso de Admisión de estudiantes en la Universidad Tecnológica Equinoccial basado en la norma internacional ISO/IEC 27000 para determinar el nivel de seguridad y elaborar un plan de tratamiento de riesgos que permita dar respuesta a los riesgos de seguridad de la información asociados a este proceso.
Alcance	Evaluación del proceso de Admisión de estudiantes para las carreras de Pregrado, campus Matriz Quito, modalidad Presencial, no incluye al proceso de admisión de Posgrado, proceso de matrícula y nivelación de estudiantes.
Proceso	Sistema Integrado de Admisión y Nivelación: Admisión de Estudiantes
Documentos de referencia	Soportes del proceso de admisión de estudiantes

Evaluación basada en ISO/IEC 27001:2005 e ISO/IEC 27005										
ACTIVIDAD	**CENTRO**	**EVALUADOR(ES)**	**HORARIO**	Rectorado	Vicerrectorado General Académico	Orientación Académica	Departamentos Académicos	Facultad de Ciencias de la Salud	Facultad de Arquitectura	Instituto de Informática y Computación

Establecimiento del contexto	Quito	JV, RV	16h00-17h00	14/08/2013						
Análisis de la brecha de seguridad	Quito	JV, RV	08h00-18h00		16/08/2013	20/08/2013	22-23/08/2013	21/08/2013	21/08/2013	27/08/2013
Proceso de Análisis										
Identificación de activos	Quito	JV, RV	08h00-18h00		06/09/2013	07/09/2013	08-09/09/2013	10/09/2013	10/09/2013	11-12/09/2013
Identificación de amenazas	Quito	JV, RV	08h00-18h00		13/09/2013	16/09/2013	17-18/09/2013	19/09/2013	20/09/2013	23-24/09/2013
Identificaciòn de controles existentes	Quito	JV, RV	08h00-18h00		25/09/2013	26-27/09/2013	30/09-02/10/2013	03-04/10/2013	07-08/10/2013	14-15/10/2013
Identificaciòn de vulnerabilidades	Quito	JV, RV	08h00-18h00		16/10/2013	17-18/10/2013	21-23/10/2013	24-25/10/2013	28-29/10/2013	30-31/10/2013
Proceso de valoración y evaluación										
Valoraciòn de activos	Quito	JV, RV	08h00-18h00			08-11/11/2013	12/11/2013			
Valoraciòn de consecuencias	Quito	JV, RV	08h00-18h00							
Valoraciòn de incidentes	Quito	JV, RV	08h00-18h00							
Estimación del riesgo	Quito	JV, RV	08h00-18h00							
Evaluaciòn del riesgo	Quito	JV, RV	08h00-18h00							
Proceso de tratamiento	Quito	JV, RV	09h00-13h00	16-21/01/2014		22-29/01/2014				
Emisión de informes finales										
Informe de becha de seguridad	Quito	JV, RV	08h00-18h00	16/01/2014						
Plan de tratamiento de riesgos	Quito	JV, RV	08h00-18h00	24/02/2014						

Elaborado por: Javier Vivanco y Ricardo Vallejo

4.2.4 Establecimiento del contexto

Actualmente la UTE no ha implementado la gestión de riesgos de la seguridad de la información sobre a ningún proceso, por tal motivo los autores han realizado reuniones con las autoridades para definir ciertos aspectos y criterios básicos que delinearán los resultados del presente trabajo de tesis.

Criterios básicos

- **Criterios de evaluación del riesgo**

Los criterios de evaluación del riesgo para determinar el riesgo de la seguridad de la información en el proceso de admisión de estudiantes de la UTE están constituidos por los siguientes aspectos:

- El valor estratégico del proceso de información en la organización es muy importante, así como los requisitos legales y reglamentarios, la ley que ampara al funcionamiento de las Universidades especifica que se debe contar con un proceso de selección para el ingreso a las instituciones de Educación Superior públicas y privadas, que garantice equidad de oportunidades y transparencia.
- Las expectativas de la sociedad respecto a la buena reputación que tiene la institución es muy importante.
- El valor de los activos es importante para la UTE, ya que normalmente utilizan información sensible y crítica en todo el proceso de admisión que reflejan las aptitudes y conocimientos de los aspirantes.

- **Criterios de impacto**

Los criterios de impacto están constituidos por los siguientes aspectos:

- La brecha de la seguridad de la información que afecta directamente a la pérdida de confidencialidad, integridad y disponibilidad de los

activos involucrados en el proceso y que pongan en riesgo la confianza del proceso, el cumplimiento legal y los resultados de la selección de aspirantes.

- Las pérdidas económicas de los activos en función del coste de compra para los activos tangibles y el valor de recuperación, pérdida, incumplimiento, pérdida de buen nombre y multas para el caso de los activos intangibles.

- **Criterios de aceptación del riesgo**

En reuniones mantenidas con las autoridades de la Universidad de ha definido el apetito del riesgo del proceso de Admisión de Estudiantes, en donde, se acepta los riesgos del proceso que no afecten directamente y en gran medida a la confianza de la sociedad, imagen, el cumplimiento legal y ni a los resultados de la selección de aspirantes en beneficio de partes interesadas.

En evaluación de seguridad se gestionarán los riesgos en dos etapas: la primera corresponde a los riesgos prioritarios mediante las acciones descritas plan de tratamientos propuesto, y la segunda relacionada a los riesgos de nivel medio y bajo que a futuro se analizarán y se tomarán las acciones pertinentes.

4.2.5 Análisis de brecha de Seguridad de la Información

El análisis de la brecha de seguridad se enfoca a realizar la evaluación del estado actual respecto a los requisitos obligatorios de la norma ISO/IEC 27001:2005 y los controles especificados en el anexo A.

Esta etapa es importante porque identifica los riesgos más relevantes a los que está expuesto el proceso analizado, y se constituye en un insumo valioso para iniciar la evaluación de los riesgos de seguridad.

Para determinar la brecha de seguridad se realizó una investigación de campo mediante observaciones al proceso, validación de controles, revisión de documentos y entrevistas al personal involucrado.

Por cada requisito o control de la norma se asignó un nivel de cumplimento en base a la escala especificada en la metodología y se analizó los datos para obtener el valor final individual.

La obtención del porcentaje de cumplimiento final se obtiene del cálculo promedio de los porcentajes individuales de cada elemento analizado. En el cuadro 27 se presenta una muestra de los registros, por su confidencialidad para la publicación se modificado los valores cualitativos por cuantitativos. Por su confidencialidad para la publicación se modificado los valores cuantitativos por cualitativos en el Cuadro 34.

Los resultados de la brecha de seguridad se entregaran a las autoridades en la etapa de emisión del informe final.

En el Cuadro 28 se puede visualizar a su vez el formato de la matriz con algunos valores que demuestran del análisis para el cumplimiento de los controles de la norma ISO/IEC 27002 en la UTE. Por su confidencialidad para la publicación se modificado los valores cualitativos por cuantitativos en el Cuadro 34.

Cuadro 27: Formato para el análisis de brecha respecto a la norma ISO/IEC 27001:2005

PROCESO DE ADMISIÓN: Estándar ISO/IEC 27001:2005

Fecha: 28 de noviembre del 2013

	REQUISITO NORMATIVO	% Actual	Estado actual	0	1	2	3
	CUMPLIMIENTO GENERAL ISO 27001:2005	**Bajo**					
4	**SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN**	**Bajo**	**La Universidad dispone de controles de seguridad implantados pero fuera del contexto de un SGSI**				
4,1	**REQUERIMIENTOS GENERALES**	**Bajo**	La Universidad no dispone de un SGSI	x			
4,2	**ESTABLECIMIENTO Y GESTIÓN DEL SGSI**	**Bajo**	La Universidad no dispone de un SGSI				
4.2.1	Establecer el SGSI	**Bajo**	La Universidad no dispone de un SGSI				
a)	Definir el alcance y límites del SGSI	**Bajo**	La Universidad no dispone de un SGSI	x			
b)	Definir una política del SGSI	**Bajo**	NO existe una política de seguridad de la información				
1.-	Incluya el marco general y los objetivos de seguridad de la información de la organización	**Bajo**	No se realiza esta actividad	x			
2.-	Considere requerimientos legales o contractuales relativos a la seguridad de la información	**Bajo**	No se realiza esta actividad	x			
3.-	Esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI	**Bajo**	No se realiza esta actividad	x			
4.-	Establezca los criterios con los que se va a evaluar el riesgo	**Bajo**	No se realiza esta actividad	x			

5.-	Esté aprobada por la dirección	**Bajo**	No se realiza esta actividad	x			
c)	Definir el enfoque organizacional hacia la valoración del riesgo	**Bajo**					
1.-	*Definir una metodología de evaluación del riesgo apropiada para el SGSI* y los requerimientos del negocio	**Bajo**	No existe una metodología establecida en la Universidad	x			
2.-	Establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable	**Bajo**	No existen criterios de aceptación del riesgo	x			
d)	Identificar los riesgos	**Bajo**					
1.-	Identificar los activos que están dentro del alcance del SGSI y a sus responsables directos	**Bajo**	Se identifican algunos activos sin considerar un SGSI		x		
2.-	Identificar las amenazas en relación a los activos	**Bajo**	Se identifican amenazas para ciertos activos, fuera del contexto de un SGSI		x		
3.-	Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas	**Bajo**	Se identifican vulnerabilidades para ciertos activos, fuera del contexto de un SGSI		x		
4.-	Identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos	**Bajo**	Los impactos son identificados por los administradores de los sistemas, bdd y redes, fuera del contexto de un SGSI		x		
e)	*Analizar y evaluar los riesgos*	**Bajo**					
1.-	Evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información	**Bajo**	Los impactos son identificados por los administradores de los sistemas, bdd y redes, fuera del contexto de un SGSI		x		
2.-	Evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados	**Bajo**	No se realiza esta actividad	x			
3.-	Estimar los niveles de riesgo	**Bajo**	No se realiza esta actividad	x			

Cuadro 28: Formato para el análisis de la brecha respecto a los controles del Anexo A

PROCESO DE ADMISIÓN: Estándar ISO/IEC 27001:2005 - Anexo A

REQUISITO NORMATIVO	DESCRIPCIÓN	Aplica (Si/No)	% Actual	% Objetivo	Estado actual	Cumplimiento			
						0	1	2	3
A.5 Política de seguridad		**Si**	**Bajo**	**100%**		**2**	**0**	**0**	**0**
A.5.1 Política de seguridad de la información	Objetivo: Dirigir y dar soporte a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y reglamentos pertinentes.		**Bajo**	**100%**		**2**	**0**	**0**	**0**
A.5.1.1 Documento de la política de seguridad de la información	Un documento de política de seguridad de información será aprobado por la dirección, publicado y comunicado a todos los empleados y partes externas pertinentes.	Si	Bajo	100%	No existe una política de seguridad de la información.	x			
A.5.1.2 Revisión de la política de seguridad de la información	La política de seguridad de la información debe revisarse a intervalos planificados o si ocurren cambios significativos asegurar su conveniencia, adecuación y eficacia continua.	Si	Bajo	100%	Al no existir una política de seguridad, no se realizan las revisiones	x			

4.2.6 Proceso de análisis

4.2.6.1Identificación de activos

La identificación de los activos está basada en el levantamiento del mapa de procesos de la Universidad, la observación de las actividades relacionadas, las entrevistas con el personal involucrado y las necesidades de las autoridades. Las entradas utilizadas para esta etapa son:

a) Mapa de procesos de la Universidad determinados en el numeral 3.2.1
b) Listado de personas descrito en el numeral 4.2.3

Las listas de activos más relevantes del proceso de admisión UTE se presentan en el Cuadro 29, 30 y 31.

a) Activos principales: Procesos

Cuadro 29: Activos principales - Procesos

Categoría	ID Activo	Activo
Procesos		
	APP-01	Inscripción de aspirantes
	APP-02	Diseño y elaboración de exámenes
	APP-03	Recepción de exámenes
	APP-04	Selección de aspirantes

b) Activos principales: Información

Cuadro 30: Activos principales - Información

Categoría	Subcategoría	ID Activo	Activo
Información			
	Digital	DAT-01	Información ingresada por las personas en la inscripción
	Digital	DAT-02	Lista de estudiantes becados por el SNNA

Digital	DAT-03	Lista de correos electrónicos de los inscritos por periodo
Físico	DAT-04	Turnos del examen
Digital	DAT-05	Banco de preguntas del examen de aptitud y conocimientos de periodos anteriores
Digital / Físico	DAT-06	Bases de datos científicas y bibliografía digital o física accesible por los docentes
Digital	DAT-07	Banco de preguntas del examen de aptitud y conocimientos automatizado. (solo se genera un nuevo banco de preguntas para el examen aptitudinal si hay necesidad de actualización, sino no se actualiza en el banco existente)
Digital / Físico	DAT-08	Exámenes tipo para los aspirantes a la Facultad de Arquitectura
Digital / Físico	DAT-09	Examen de conocimientos para los aspirantes a la Facultad de Ciencias de la Salud
Físico	DAT-10	Listado de los aspirantes que rindieron sus exámenes en un determinado periodo
Físico	DAT-11	Listas de docentes tutores por aulas que tomaron o tomarán los exámenes
Digital	DAT-12	Respuesta seleccionadas por los aspirantes en los exámenes tomados en el proceso de recepción de exámenes
Log	DAT-13	Logs del sistema
Físico	DAT-14	Exámenes de conocimientos resueltos por los aspirantes a la Facultad de Arquitectura
Físico	DAT-15	Hojas de respuestas llenadas por los aspirantes a la Facultad de Ciencias de la Salud
Digital	DAT-16	Archivo que contienen las notas obtenidas por los aspirantes a la Fac. Ciencias de la Salud
Digital	DAT-17	Ponderación # de cupos de aspirantes admitidos por UTE y por carreras. Definición de notas mínimas para ser seleccionados
Digital	DAT-18	Listado de aspirantes admitidos.
Digital	DAT-19	Código fuente del Sistema Integrado de Admisión y Nivelación
Digital	DAT-20	Código fuente del Sistema de Temarios y Resultados
Físico	DAT-21	Documentos de aprobaciones de exámenes retrasados y tomar nuevamente, personas con discapacidad.

c) Activos de apoyo

Cuadro 31: Activos de apoyo

Categoría	Subcategoría	ID Activo	Activo
Servicios			
	Servicio	SER-01	Web
	Servicio	SER-02	Correo electrónico
	Servicio	SER-03	Almacenamiento de ficheros
	Servicio	SER-04	Almacenamiento en base de datos

	Servicio	SER-05	Gestión de identidades
	Servicio	SER-06	Control de acceso de usuarios
	Servicio	SER-07	Soporte a usuarios
	Servicio	SER-08	Respaldos de información
Software-Aplicaciones			
	Aplicaciones del negocio	SW-01	Sistema Integrado de Admisión y Nivelación SIAN
	Aplicaciones del negocio	SW-02	Sistema de Admisión: Temarios y Resultados
	Sistema Operativo	SW-04	Windows Server 2008
	Software estándar	SW-05	Internet Information Server 6,0
	Software estándar	SW-06	Microsoft Exchange Server 2007
	Software estándar	SW-07	Sql Sever 2008 R2 SP2
	Software estándar	SW-08	Microsoft Office 2007/2010/2013
	Software estándar	SW-09	Symantec End Point Antivirus
	Software estándar	SW-10	Kaspersky Antivirus
	Software estándar	SW-11	Vsphere 4.0 / 5.0
	Software estándar	SW-12	Windows 7
	Software estándar	SW-13	Terminal Services
	Software estándar	SW-14	Backup Exec 2010
	Software estándar	SW-15	Internet Explorer
	Software estándar	SW-16	Software de acceso remoto: VNC, PCAnywhere
Hardware			
	Equipo Fijo - móvil	HW-01	Computadora Vicerrectora General Académica
	Equipo Fijo - PC	HW-02	Computadora Departamento Orientación Académica
	Equipo Fijo - PC	HW-03	Computadora de la Coordinadora de Esc. Medicina
	Equipo Fijo - PC	HW-04	Computadora del Coordinador de la Fac. Arquitectura
	Equipo Fijo - PC	HW-05	Computadora del Departamentos Académicos
	Equipo Fijo - PC	HW-06	Computadora del Desarrollador de Aplicación SIAN
	Equipo Fijo - Servidor	HW-07	Base de datos: svrquito43, svrquito44
	Equipo Fijo - Servidor	HW-08	Aplicaciones: svrquito36, svrquito60
	Equipo Fijo - Servidor	HW-09	Controladores de dominio: Quito01, quito02, quito03, quito07, quito08

	Equipo Fijo - Servidor	HW-10	Servidor de Archivos: svrquito09, svrquito07
	Equipo Fijo - Servidor	HW-11	Correo electrónico
	Equipo Fijo - Servidor	HW-12	Librería MLS4048 / MSL2024
	Equipo Fijo - Servidor	HW-13	HP Storage P6300
	Equipo Fijo - Servidor	HW-14	HP Enclousure C7000
	Medios electrónico	HW-15	Dispositivos USB
	Medios electrónico	HW-16	DVD
	Medios electrónico	HW-17	Cintas magnéticas
	Equipo auxiliar	HW-18	Sistema de alarmas
	Equipo auxiliar	HW-19	Generador eléctrico
	Equipo auxiliar	HW-20	Equipo de destrucción de papeles
Red			
	Medios y Soportes	NET-01	Red telefónica
	Medios y Soportes	NET-02	Red inalámbrica
	Medios y Soportes	NET-03	LAN / cableado
	Medios y Soportes	NET-04	Internet
	Transmisión pasiva -activa	NET-05	switch cisco 6500
	Transmisión pasiva -activa	NET-06	switch cisco 4503
	Transmisión pasiva -activa	NET-07	switch cisco 2960
	Transmisión pasiva -activa	NET-08	router cisco 7500
	Transmisión pasiva -activa	NET-09	Fortigate 1240B
Personal			
	Personal de Toma decisiones	PRS-01	Vicerrectora General Académico
	Usuarios	PRS-02	Personal de Orientación Académica
	Personal de Toma decisiones	PRS-03	Decanos
	Usuarios	PRS-04	Departamentos Académicos
	Usuarios	PRS-05	Personal de Coordinación Fac. Medicina
	Usuarios	PRS-06	Personal de Coordinación Fac. Arquitectura, Artes y Diseño
	Usuarios	PRS-07	Docentes tutores de aula
	Desarrolladores	PRS-08	Desarrollador de aplicación.
	Personal de operación/mantenimiento	PRS-09	Ingenieros del Área de Redes

	Personal de operación/mantenimiento	PRS-10	Administrador de bdd
	Usuarios	PRS-11	Administrador del SIAN
	Personal de operación/mantenimiento	PRS-12	Ingenieros de Mantenimiento - Hardware
Sitios			
	Zona	ST-01	IDIC
	Zona	ST-02	Patio de la Virgen - orientación Académica
	Zona	ST-03	Patio de la Virgen - Vicerrectorado
	Zona	ST-04	Patio de la Virgen - Departamentos Académicos
	Zona	ST-05	Oficinas de Coordinaciones Facultades
	Zona	ST-06	Rack Comunicaciones
	Zona	ST-07	Bloque C - Posterior
Organización			
	Proveedores	ORG-01	SNNA
	Proveedores	ORG-02	Telconet
	Proveedores	ORG-03	Level3

Una muestra del registro detallado de cada activo: categoría y subcategoría del activo, propietario, custodio, la ubicación, dependencia de activos, se presenta en la Cuadro 32.

En cuadro 33 se presenta una muestra de los activos de información clasificados en función de su nivel de sensibilidad, criticidad e integridad, y la valoración inicial respecto a los requerimientos de seguridad.

Cuadro 32: Muestra de activos del proceso de admisión

Activos de apoyo: servicios										
				Custodio		Responsable				
ID Activo	Nombre Activo	Subcategoría	Propietario	Funcionario	Cargo	Funcionario	Cargo	Ubicación		Dependencia
SER-01	Web	Servicio	IDIC	Confidencial	Ingeniero de Sistemas	Confidencial	Ingeniero de Sistemas	IDIC		HW08, HW14, SW4, SW5,SW09, NET03, NET04, NET05, NET08, NET09, PSR08, PSR09, ST01, ORG02
SER-02	Correo electrónico	Servicio	IDIC	Confidencial	Ingeniero de Manten. - Redes	Confidencial	Ingeniero de Manten. - Redes	IDIC		HW11, HW14, SW4, SW6, SW09, NET03, NET04, NET05, NET08, NET09, PSR09, ST01, ORG02, ORG03
SER-03	Almacenamiento de ficheros	Servicio	IDIC	Confidencial	Ingeniero de Manten. - Redes	Confidencial	Ingeniero de Manten. - Redes	IDIC		HW10, HW14, SW4, SW09, SW11, NET03, NET05, NET08, PSR09, ST01
SER-04	Almacenamiento en base de datos	Servicio	IDIC	Confidencial	Administrador Bdd	Confidencial	Administrador Bdd	IDIC		HW07, HW14, SW04, SW07, SW09, NET03, NET05, PSR10, ST01
SER-05	Gestión de identidades	Servicio	IDIC	Confidencial	Ingeniero de Manten. - Redes	Confidencial	Ingeniero de Manten. - Redes	IDIC		HW09, HW14, SW04, SW09, NET03, NET05, PSR09, ST01
SER-06	Control de acceso de usuarios	Servicio	IDIC	Confidencial	Ingeniero de Manten. - Redes	Confidencial	Ingeniero de Manten. - Redes	IDIC		HW07, HW09, HW10, HW11, HW14, SW01, SW02, SW04, SW05, SW06, SW07, SW11, SW13, PSR08, PSR09, PSR10, PSR11, ST01
SER-07	Soporte a usuarios	Servicio	IDIC	Confidencial	Ingeniero de Manten. - Hardware	Confidencial	Ingeniero de Manten. - Hardware	IDIC		SW16, NET03, PRS12
SER-08	Respaldos de información	Servicio	IDIC	Confidencial	Ingeniero de Manten. - Redes	Confidencial	Ingeniero de Manten. - Redes	IDIC		HW12, SW14, PS09, ST01

Cuadro 33: Muestra de activos del proceso de admisión

ACTIVOS PRINCIPALES														
				Clasificación			Requerimientos SI			Valoración Inicial		
Categoría	Subcat.	ID Activo	Descripción	Sensibilidad	Criticidad	Integridad	C	I	D	C	I	D
Información												
	Digital	DAT-01	Las personas interesadas en un periodo habilitado pueden inscribirse desde la página web institucional, para lo que se le pide que ingres información relacionada con: Nombres, dirección, colegio de donde proviene, teléfono de contacto, nivel de socioeconómico, correo electrónico, etc.	Interno	Opcional	Integro			x	L	M	M
	Digital	DAT-02	El SSNA proporciona un documento en Excel a Vicerrectorado General Académico de la UTE con los nombres y puntajes de los estudiantes becados por el SNNA	Interno	Opcional	Integro		x	x	L	M	L
	Digital	DAT-03	Luego de inscribirse y llenar la información requerida por el sistema web, se genera un listado con los correos personales de los inscritos	Interno	Opcional	No integro			x	L	L	M
	Físico	DAT-04	Documentos que contiene la información del estudiante y el turno para rendir el examen	Interno	Opcional	Integro			x	L	M	M
	Digital / Físico	DAT-06	Toda la información que por convenios institucionales los docentes pueden tener acceso desde la UTE	Público	Opcional	No integro			x	L	L	L

4.2.6.2 Identificación de las amenazas

La identificación de las amenazas está desarrollada en función de las entrevistas con los usuarios, autoridades y propietarios de los activos establecidos en el numeral 4.2.6.1, así como el reconocimiento de las amenazas genéricas que se indican en la metodología. Las entradas utilizadas en esta fase son:

a) Listado de activos de información del proceso de Admisión
b) Listado de las amenazas comunes del anexo C de la norma NTE INEN-ISO/IEC 27005:2012.
c) Matriz de entrevistas con usuarios, autoridades y propietarios de los activos.
d) Informe de brecha de seguridad de la información.

Como resultado de esta etapa se obtiene la matriz que contiene un listado de activos de información junto con las amenazas a las que está expuesto cada activo, tipo y el origen de amenaza, tal como se puede visualizar en el cuadro 34 una muestra de los datos.

Cuadro 34: Identificación de amenazas de los activos de información

Categoría	Subcat.	ID Activo	Activo	Descripción	Tipo	Amenaza	D	A	E
Información									
	Digital	DAT-01	Información ingresada por las personas en la inscripción	Las personas interesadas en un periodo habilitado pueden inscribirse desde la página web institucional, para lo que se le pide que ingres información relacionada con: Nombres, dirección, colegio de donde proviene, teléfono de contacto, nivel de socioeconómico, correo electrónico, etc.	Compromiso con la información	Manipulación con software	x	x	
					Pérdida de los servicios esenciales	Falla en el equipo de telecomunicaciones		x	
					Fallas técnicas	Falla de equipo		x	
					Fallas técnicas	Mal funcionamiento de equipo		x	
	Digital	DAT-02	Lista de estudiantes becados por el SNNA	El SNNA proporciona un documento en Excel a Vicerrectorado General Académico de la UTE con los nombres y puntajes de los estudiantes becados por el SNNA	Compromiso con la información	Datos provenientes de fuentes no confiables	x	x	
					Compromiso con la información	Manipulación con software	x	x	
					Fallas técnicas	Falla del equipo		x	
					Acciones no autorizadas	Uso no autorizado del equipo			x
					Acciones no autorizadas	Corrupción de los datos			x
	Digital	DAT-03	Lista de correos electrónicos de los inscritos por periodo	Luego de inscribirse y llenar la información requerida por el sistema web, se genera un listado con los correos personales de los inscritos	Fallas técnicas	Falla del equipo		x	
					Fallas técnicas	Mal funcionamiento de equipo		x	
					Compromiso con las funciones	Abuso de derechos	x	x	

4.2.6.3 Identificación de los controles existentes

La identificación de los controles existentes se desarrolló en función de las entrevistas con los usuarios, autoridades y propietarios de los activos establecidos en el numeral 4.2.6.1, así como, las observaciones a las actividades de los subprocesos como parte de la presente evaluación del riesgo. Las entradas utilizadas en esta fase son:

a) Listado de activos de información del proceso de Admisión con sus respectivas amenazas.
b) Hojas de trabajo de las observaciones de las actividades de los subprocesos.
c) Hojas de trabajo de entrevistas con usuarios, autoridades y propietarios de los activos.
d) Informe de brecha de seguridad de la información.

Como parte de esta fase se realiza la verificación del funcionamiento de los sistemas informáticos utilizados.

El resultado de esta etapa es la matriz de los controles asociados a los activos. Una muestra se de este resultado se especifica en el Cuadro 35.

Cuadro 35: Identificación de controles y su estado

Identificación de Amenazas, Controles existentes, Vulnerabildiades y Consecuencias									
				Amenazas				Controles (existentes)	
Categoría	Subcat.	ID Activo	Activo	Amenaza	D	A	E	Tipo	Estado
Información									
	Digital	DAT-01	Información ingresada por las personas en la inscripción	Manipulación con software	x	x		1) Acceso restringido 2) Validación de datos de entrada en el sistema web 3) Respaldos de información 4) Control de acceso a la información mediante perfiles de usuario 5) Control de acceso externo mediante un firewall perimetral	1) Implementado 2) Implementado 3) Implementado 4) Implementado 5) Implementado
		DAT-01	Información ingresada por las personas en la inscripción	Falla en el equipo de telecomunicaciones	x	x		1) Contratación de servicios de garantía 2) Respaldos de configuraciones 3) Plan de contingencia de TI	1) implementado 2) Implementado 3) Implementado
		DAT-01	Información ingresada por las personas en la inscripción	Falla de equipo		x		1) Mantenimiento correctivo	1) Implementado
		DAT-01	Información ingresada por las personas en la inscripción	Mal funcionamiento de equipo		x		1) Mantenimiento correctivo	1) Implementado

4.2.6.4 Identificación de las vulnerabilidades

La identificación de las vulnerabilidades existentes se desarrolló en función de las entrevistas con los usuarios, autoridades y propietarios de los activos establecidos en el numeral 4.2.6.1, las observaciones y pruebas realizadas en el desarrollo de los subprocesos como parte de la presente evaluación del riesgo y el reconocimiento de las vulnerabilidades comunes que se indican como ejemplo en el anexo D de la norma NTE INEN-ISO/IEC 27005:2012. Las entradas para esta fase son:

a) Listado de activos de información del proceso de Admisión con sus respectivas amenazas y controles.
b) Listado de las vulnerabilidades comunes del anexo D de la norma NTE INEN-ISO/IEC 27005:2012.
c) Hojas de trabajo de las observaciones y pruebas realizadas a los subprocesos.
d) Hojas de trabajo de entrevistas con usuarios, autoridades y propietarios de los activos.
e) Informe de brecha de seguridad de la información.

Para la determinación de las vulnerabilidades de los activos se realizaron pruebas de los controles implementados y la verificación de las vulnerabilidades del anexo D de la norma NTE INEN-ISO/IEC 27005:2012 aplicables al proceso.

El resultado es una matriz de las vulnerabilidades que tienen los activos, una muestra se presenta en el cuadro 36.

Cuadro 36: Identificación de las vulnerabilidades

Identificación de Amenazas, Controles existentes, Vulnerabildiades y Consecuencias

				Amenazas				Controles (existentes)		Vulnerabilidades
Categoría	Subcat.	ID Activo	Activo	Amenaza	D	A	E	Tipo	Estado	
Información										
	Digital	DAT-01	Información ingresada por las personas en la inscripción	Manipulación con software	x	x		1) Acceso restringido 2) Validación de datos de entrada en el sistema web 3) Respaldos de información 4) Control de acceso a la información mediante perfiles de usuario 5) Control de acceso externo mediante un firewall perimetral	1) Implementado 2) Implementado 3) Implementado 4) Implementado 5) Implementado	Cualquier persona puede modificar los datos si conoce el número de cédula El sistema no dispone de un sistema de verificación de cédula o pasaporte El aspirante puede ingresar datos erróneos
		DAT-01	Información ingresada por las personas en la inscripción	Falla en el equipo de telecomunicaciones	x	x		1) Contratación de servicios de garantía 2) Respaldos de configuraciones 3) Plan de contingencia de TI	1) implementado 2) Implementado 3) Implementado	Explotación de vulnerabilidades de IOS de equipos de telecomunicaciones
		DAT-01	Información ingresada por las personas en la inscripción	Falla de equipo		x		1) Mantenimiento correctivo	1) Implementado	No se difunde la política de respaldos de información No existen mecanismos de respaldos implementados
		DAT-01	Información ingresada por las personas en la inscripción	Mal funcionamiento de equipo		x		1) Mantenimiento correctivo	1) Implementado	No existen mecanismos de respaldos implementados

4.2.7 Proceso de Valoración y Evaluación

El análisis de riesgos se realiza con diferentes grados de detalle dependiendo de la criticidad y esfuerzos de la institución.

Al ser la primera ocasión que se realiza una evaluación de riesgos en la universidad y por recomendación de la norma NTE INEN-ISO/IEC 27005:2012 especificada en el literal 8.2.2.1 “Metodología para la estimación del riesgo”, en el presente trabajo se utilizará una metodología de estimación cualitativa para obtener una indicación general del nivel del riesgo e identificar los riesgos más importantes.

Al finalizar la presente tesis, se deja abierta la posibilidad para que a futuro se realice un análisis detallado de los riesgos más importantes con una metodología cuantitativa.

Para determinar la estimación del riesgo, los autores utilizarán atributos calificativos para describir las consecuencias potenciales: Alta (H), Media (M) y Baja (L), con el fin de facilitar las entrevistas, la comprensión por parte de los entrevistados y obtener los resultados más óptimos de estimación del riesgo.

4.2.7.1 Valoración de los activos

La valoración del impacto es determinada en función a los posibles incidentes ocasionados por las amenazas, vulnerabilidades, la deficiencia de los controles implementados y los requerimientos de seguridad definidos por las autoridades de la Universidad. Las entradas de esta fase son:

a) Listado de activos de información del proceso de Admisión con sus respectivas amenazas, controles y vulnerabilidades.

b) Valoración de los activos en función de sus costo de reposición, costo de reconfiguración, tiempo de suspensión del servicio, brechas de seguridad, falta de cumplimientos legales, imagen y reputación.
c) Hojas de trabajo de entrevistas con usuarios, autoridades y propietarios de los activos.

a) Método de valoración de los activos primarios: "procesos"

Por la criticidad de los activos todos los procesos obtuvieron una valoración de 4 como se indica en el Cuadro 37.

b) Método de valoración de los activos primarios: "información"

El método considera los datos de clasificación de la información en función de su Criticidad, Sensibilidad e Integridad especificados por los dueños del proceso, los datos de Confidencialidad, Integridad y Disponibilidad especificados por usuarios en las entrevistas y la percepción de las autoridades del nivel de seguridad.

Una muestra de la matriz de valoración de los activos resultante del análisis de los riesgos del proceso de admisión de la UTE se presenta en el Cuadro 38.

c) Método de valoración de los activos de apoyo: "servicios"

El valor de activos la categoría "servicios" se determina a partir del valor más alto heredado de los activos dependientes o del valor total de la sumatoria de los requisitos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad)

d) Método de valoración de los activos de apoyo

Una muestra de la matriz de valoración de los activos resultante del análisis de los riesgos del proceso de admisión de la UTE se presenta en el Cuadro 39.

Cuadro 37: Valoración de activos primarios – Procesos

Categoría	ID Activo	Activo	Valor según dependencias		Valor del activo METODOLOGIA APLICADA PARA PROCESOS Valor mas alto de los activos dependientes o involucrados
			Dependencia	Valor más alto	
A **Procesos**					**VA**
	APP-01	Inscripción de aspirantes	DAT-01, DAT-02, DAT-03, DAT-04, DAT-13,DAT-19, DAT-20, SER-01, SER-02, SER-04, SER-05, SER-06	3	**3**
	APP-02	Diseño y elaboración de exámenes	DAT-05, DAT-06, DAT-07, DAT-08, DAT-09, DAT-13,DAT-19, DAT-20, SER-01, SER-02, SER-03, SER-04, SER-05, SER-06, SER-07, SER-08	4	**4**
	APP-03	Recepción de exámenes	DAT-10, DAT-11, DAT-12, DAT-13, DAT-14, DAT-15, DAT-16, DAT-19, SER-01, SER-04, SER-05, SER-06, SER-07, SER-08	4	**4**
	APP-04	Selección de aspirantes	DAT-13, DAT-17, DAT-18, DAT-19, SER-01, SER-04, SER-05, SER-06, SER-08	3	**3**

Cuadro 38: Valoración de activos primarios – Información

Categoría	Sub categoría	Activo	Valor según dependencias			Requerimientos de SI			Valoración			Suma de factores	VA
			sensibilidad	Criticidad	Integridad	C	I	D	C	I	D		
Información													
	Digital	Información ingresada por las personas en la inscripción	Interno	Opcional	Integro			x	L	M	M	11	1
	Digital	Lista de estudiantes becados por el SNNA	Interno	Opcional	Integro		x	x	L	M	L	11	1
	Digital	Lista de correos electrónicos de los inscritos por periodo	Interno	Opcional	No integro			x	L	L	M	9	1
	Físico	Turnos del examen	Interno	Opcional	Integro			x	L	M	M	11	1
	Digital	Banco de preguntas del examen de aptitud y conocimientos de periodos anteriores	Confidencial	Crítico	Integro	x	x	x	H	H	H	20	4
	Digital / Físico	Bases de datos científicas y bibliografía digital o física accesible por los docentes	Público	Opcional	No integro			x	L	L	L	7	0
	Digital	Banco de preguntas del examen de aptitud y conocimientos automatizado.	Confidencial	Crítico	Integro	x	x	x	H	H	H	20	4

Cuadro 39: Valoración de activos de apoyo – Servicios

Categoría	ID Activo	Activo	Valor segun dependencias		Requerimientos			Valoración					
			Dependencia	Valor más alto (Y")	C	I	D	C	I	D	Suma de factores	VA'	VA
Servicios													
	SER-01	Web	HW08, HW14, SW4, SW5,SW09, NET03, NET04, NET05, NET08, NET09, PSR08, PSR09	4		x	x	L	H	H	9	3	4
	SER-02	Correo electrónico	HW11, HW14, SW4, SW6, SW09, NET03, NET04, NET05, NET08, NET09, PSR09, ST01	4			x	L	L	M	5	1	4
	SER-03	Almacenamiento de ficheros	HW10, HW14, SW4, SW09, SW11, NET03, NET05, NET08, PSR09, ST01	4	x	x	x	H	H	H	12	4	4
	SER-04	Almacenamiento en base de datos	HW07, HW14, SW04, SW07, SW09, NET03, NET05, PSR10, ST01	4	x	x	x	H	H	H	12	4	4
	SER-05	Gestión de identidades	HW09, HW14, SW04, SW09, NET03, NET05, PSR09, ST01	4		x	x	M	H	H	10	3	4
	SER-06	Control de acceso de usuarios	HW07, HW09, HW10, HW11, HW14, SW01, SW02, SW04, SW05, SW06, SW07, SW11, SW13, PSR08, PSR09, PSR10. PSR11. ST01	4		x	x	H	H	H	11	4	4
	SER-07	Soporte a usuarios	SW16, NET03, PRS12	2			x	L	L	M	5	1	2
	SER-08	Respaldos de información	HW12, SW14, PS09,	4	x	x	x	H	H	M	11	4	4

e) Método de valoración de los activos de apoyo: "Hardware, Software, Red, Personas, Sitios y Organización"

Una muestra de la matriz de valoración de los activos de las categorías: Hardware, Software, Red, Personas, Sitios y Organización resultante del análisis de los riesgos se presenta en el Cuadro 41.

4.2.7.2 Valoración de las consecuencias

Para la valoración de las consecuencias se utilizaron los siguientes documentos: Listado de activos del proceso de admisión con sus respectivas amenazas, controles y vulnerabilidades, activos valorados cualitativamente, hoja de entrevistas con usuarios, autoridades y propietarios de los activos, y el informe de brecha de seguridad.

En el cuadro 40 se presenta la lista de consecuencias en función de los requerimientos de seguridad establecidos por las autoridades de la universidad y lo requerido en la metodología.

Cuadro 40: Detalle considerado en las consecuencias para el caso de materializarse una amenaza

Consecuencias				
CONFIDENCIALIDAD • Garantizar que la información sea accesible solo a las personas autorizadas. • Evitar la fuga de información, principalmente de las preguntas y respuesta de los exámenes de admisión que entran en el banco de preguntas del sistema informático.	**INTEGRIDAD** • Garantizar que la información de los exámenes resueltos no se alterada en beneficio de ningún aspirante.	**DISPONIBILIDAD** • Preservar la información durante el tiempo estipulado en la LOES.	**CUMPLIMIENTO LEGAL** • Establecer los lineamientos de seguridad de la información necesarios para evitar la existencia de fraude en el proceso de admisión.	**PÉRDIDAS ECONÓMICAS / CONFIABILIDAD** • Valor de los activos • Pérdida de imagen y reputación

El resultado es la matriz de valoración de las consecuencias de los riesgos, una muestra de la matriz resultante se presenta en al Cuadro 42.

Cuadro 41: Valoración de activos de apoyo restantes

Categoría	ID Activo	Activo	Valor Monetario/reposición/pérdida/invertido en capacitación*año/sueldos*año/ec			Requerimientos de SI			Valoración			Sumatoria	VA
			Bajo (L): 0-5000	Medio (M): 5000-50000	Alto (H): 50000 en adelante	C	I	D	C	I	D		
Hardware													
	HW-01	Computadora Vicerrectora General Académica	x			x		x	M	L	M	8	1
	HW-02	Computadora Departamento Orientación Académica	x			x		x	H	L	M	9	1
	HW-03	Computadora de la Coordinadora de Esc. Medicina	x			x		x	H	L	M	9	1
	HW-04	Computadora del Coordinador de la Fac. Arquitectura	x			x		x	H	L	M	9	1
	HW-05	Computadora del Departamentos Académicos	x			x		x	H	L	M	9	1
	HW-06	Computadora del Desarrollador de Aplicación SIAN	x			x		x	H	L	M	9	1
	HW-07	Base de datos: svrquito43, svrquito44		x			x	x	H	H	H	13	3
	HW-08	Aplicaciones: svrquito36, svrquito60		x			x	x	L	H	H	11	2
	HW-09	Controladores de dominio: Quito01, quito02, quito03, quito07, quito08		x		x	x	x	L	H	H	12	3
	HW-10	Servidor de Archivos: svrquito09, svrquito07		x			x	x	H	H	H	13	3
	HW-11	Correo electrónico		x				x	L	L	M	7	1
	HW-12	Librería MLS4048 / MSL2024		x				x	L	L	L	6	0
	HW-13	HP Storage P6300			x		x	x	H	H	H	14	4

Cuadro 42: Valoración de las consecuencias

Activo	VA	Código Riesgo	Amenazas		Controles (existentes)	Vulnerabilidades	Consecuencias (Riesgo)					Valoración del Impacto
			Tipo	Amenaza	Tipo		CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO LEGAL	PERDIDAS ECONOMICAS / CONFIABILIDAD	
Sistema Integrado de Admisión y Nivelación SIAN	2	R163	Compromiso de las funciones	Abuso de los derechos	1) Realización de pruebas de calidad de software	Las pruebas de software se realizan con datos exportados de la base de datos de producción	• Fuga de información • Mala utilización de la información • Acceso a información personal					L
Sistema Integrado de Admisión y Nivelación SIAN	2	R164	Compromiso de las funciones	Abuso de los derechos	1) Etiquetado de la información en medios digitales	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	• Fuga de información • Mala utilización de la información • Acceso a información personal	• Alteración de las terceras partes que tienen transacciones con la organización.	• Pérdida de información	• Incumplimiento de las obligaciones legales o reglamentarias • Procesos judiciales y castigos	• Pérdida del valor financiero del activo	H
Sistema Integrado de Admisión y Nivelación SIAN	2	R165	Compromiso de las funciones	Abuso de los derechos	1) Logs de auditoría en el sistema	Los logs del sistema se encuentran administrados por el programador de la aplicación	• Mala utilización de la información	• Alteración de las terceras partes que tienen transacciones con la organización.				M
Sistema Integrado de Admisión y Nivelación SIAN	2	R166	Compromiso de las funciones	Abuso de los derechos	1) Administración de perfiles de uso del sistema	Asignación errada de los derechos de acceso Creación de usuarios del sistema genéricos con permisos de administración	• Mala utilización de la información • Acceso a información personal	• Alteración de las terceras partes que tienen transacciones con la organización. • Uso de datos no confiables	• Costo de operaciones interrumpidas • Incapacidad para prestar el servicio • Pérdida de información			M

4.2.7.3 Valoración de los incidentes

En esta etapa se asignó un valor de probabilidad de la ocurrencia de cada amenaza y la facilidad de explotar las vulnerabilidades sobre el activo evaluado. Los documentos utilizados son:

a) Listado de activos del proceso de Admisión con sus respectivas amenazas, controles y vulnerabilidades.
b) Activos valorados cualitativamente.
c) Hojas de entrevistas con usuarios, autoridades y propietarios de los activos.
d) Escalas cualitativas definidas en esta fase de la metodología
e) Informe de brecha de seguridad.

El resultado es la matriz de probabilidad de la explotación de vulnerabilidades y la probabilidad de ocurrencia de una amenaza sobre los activos, una muestra se presenta en el Cuadro 43.

Cuadro 43: Facilidad de explotación y Probabilidad de que se produzca la amenaza

ACTIVOS PRINCIPALES			Amenazas						
Categoría	Activo	VALOR DEL ACTIVO	Tipo	Amenaza	D	A	E	Probabilidad Amenaxa	Facilidad de explotación
Información									
	Información ingresada por las personas en la inscripción	4	Compromiso con la información	Manipulación con software	x	x		M	H
	Información ingresada por las personas en la inscripción	4	Pérdida de los servicios escenciales	Falla en el equipo de telecomunicaciones	x	x		L	L
	Información ingresada por las personas en la inscripción	4	Fallas técnicas	Falla de equipo		x		L	M
	Información ingresada por las personas en la inscripción	4	Fallas técnicas	Mal funcionamiento de equipo		x		M	M

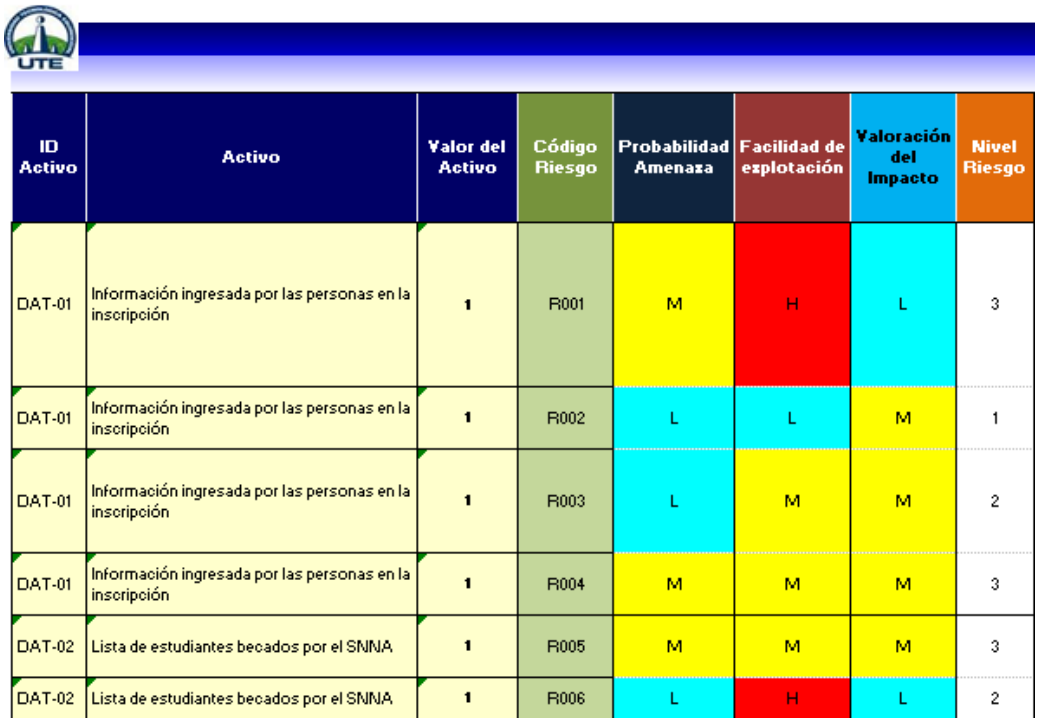
4.2.7.4Nivel de estimación

Para la ejecución de esta fase se utilizaron los siguientes documentos:

a) Identificación del impacto en el negocio en términos cualitativos, tomando como base las consecuencias ligadas a los requerimientos institucionales de seguridad de la información para el proceso de admisión de estudiantes.
b) Listado de las amenazas, controles, vulnerabilidades, facilidad de explotación y probabilidad de ocurrencia de la amenaza.

En función de la probabilidad de ocurrencia de amenaza, facilidad de explotación, la valoración de las consecuencias (impacto) y la referencia la matriz de valoración especificada en esta metodología se asignó el nivel de riesgo. Una muestra de la matriz de estimación se presenta en el Cuadro 44.

Cuadro 44: Matriz de estimación de los riesgos de seguridad



ID Activo	Activo	Valor del Activo	Código Riesgo	Probabilidad Amenaza	Facilidad de explotación	Valoración del Impacto	Nivel Riesgo
DAT-01	Información ingresada por las personas en la inscripción	1	R001	M	H	L	3
DAT-01	Información ingresada por las personas en la inscripción	1	R002	L	L	M	1
DAT-01	Información ingresada por las personas en la inscripción	1	R003	L	M	M	2
DAT-01	Información ingresada por las personas en la inscripción	1	R004	M	M	M	3
DAT-02	Lista de estudiantes becados por el SNNA	1	R005	M	M	M	3
DAT-02	Lista de estudiantes becados por el SNNA	1	R006	L	H	L	2

4.2.7.5Evaluación del riesgo

En la evaluación del riesgo se comparó los riesgos con los criterios de evaluación descritos en la etapa del establecimiento del contexto.

De la evaluación se determinó que 22 (22.2%) de los 99 activos están expuestos a riesgos de nivel alto y pueden afectar al servicio que presta la Universidad.

Se identificaron 524 riesgos, el 58.6% de los riesgos son de nivel bajo, el 32.1% tiene una afectación media y el 9.4% de riesgos pueden considerar impacto alto en la institución, el detalle se muestra en la Tabla 7.

Tabla 7: Matriz de estimación de los riesgos de seguridad

Nivel Riesgo	Valor Riesgo	Cantidad	Porcentaje
Alto	6	12	2,3%
	5	37	7,1%
Medio	4	56	10,7%
	3	112	21,4%
Bajo	2	146	27,9%
	1	105	20,0%
	0	56	10,7%
	Total	**524**	

Es importante mencionar que los riesgos identificados pueden afectar al cumplimiento de los requisitos legales y reglamentarios, el buen nombre de la universidad y la confianza de los aspirantes en el proceso de admisión.

4.2.8 Proceso de tratamiento

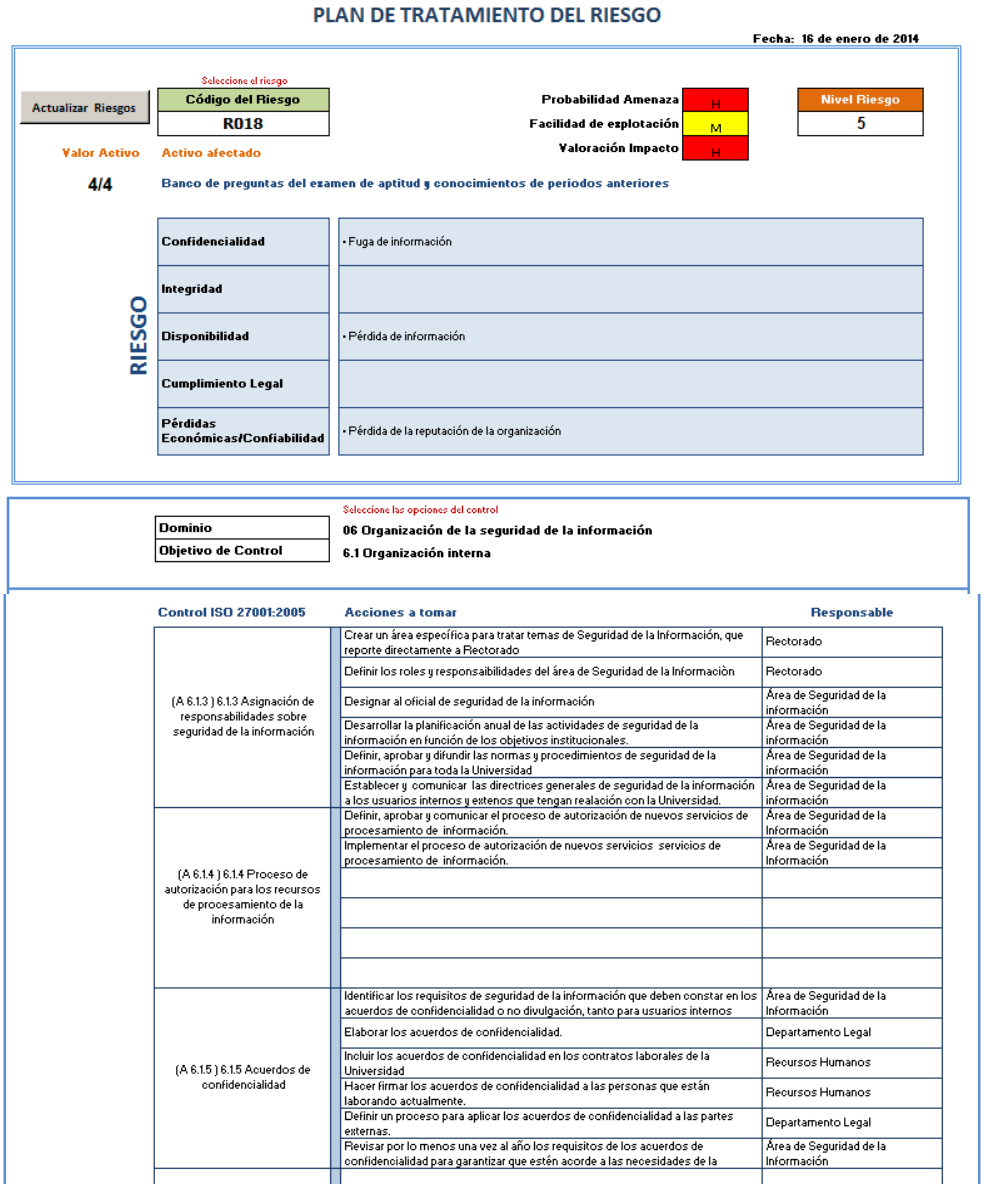
Las autoridades de la Universidad han definido tres niveles de prioridad para la identificación de los riesgos más importantes:

- Nivel prioritario: los riesgos de nivel 5 y 6
- Nivel medio: los riesgos de nivel 3 y 4,
- Nivel bajo: los riesgos de nivel 0, 1 y 2.

En acuerdo con las autoridades, en función de los criterios de aceptación del riesgo y los requerimientos de seguridad de la información se determinó las siguientes consideraciones:

- Por ser la primera ocasión que se realiza la evaluación de riesgos en la institución se aceptarán los riesgos de nivel medio y bajo.
- En el caso de los riesgos prioritarios, se seleccionarán los controles del Anexo A de la norma ISO/IEC 27001:2005 para mitigar los riesgos.
- Los evaluadores presentarán un plan de tratamiento no valorado con las acciones necesarias para mitigar los riesgos encontrados.

Las acciones a tomar sobre cada riesgo identificado se registran en el formato de la Figura 37.



PLAN DE TRATAMIENTO DEL RIESGO

Fecha: 16 de enero de 2014

Actualizar Riesgos | Seleccione el riesgo | Código del Riesgo: R018 | Probabilidad Amenaza: H | Facilidad de explotación: M | Valoración Impacto: H | Nivel Riesgo: 5

Valor Activo: 4/4 | Activo afectado: Banco de preguntas del examen de aptitud y conocimientos de periodos anteriores

RIESGO	
Confidencialidad	• Fuga de información
Integridad	
Disponibilidad	• Pérdida de información
Cumplimiento Legal	
Pérdidas Económicas/Confiabilidad	• Pérdida de la reputación de la organización

Seleccione las opciones del control

Dominio	06 Organización de la seguridad de la información
Objetivo de Control	6.1 Organización interna

Control ISO 27001:2005	Acciones a tomar	Responsable
(A 6.1.3) 6.1.3 Asignación de responsabilidades sobre seguridad de la información	Crear un área específica para tratar temas de Seguridad de la Información, que reporte directamente a Rectorado	Rectorado
	Definir los roles y responsaibilidades del área de Seguridad de la Informaciòn	Rectorado
	Designar al oficial de seguridad de la información	Área de Seguridad de la información
	Desarrollar la planificación anual de las actividades de seguridad de la información en función de los objetivos institucionales.	Área de Seguridad de la información
	Definir, aprobar y difundir las normas y procedimientos de seguridad de la información para toda la Universidad	Área de Seguridad de la información
	Establecer y comunicar las directrices generales de seguridad de la información a los usuarios internos y externos que tengan realación con la Universidad.	Área de Seguridad de la información
(A 6.1.4) 6.1.4 Proceso de autorización para los recursos de procesamiento de la información	Definir, aprobar y comunicar el proceso de autorización de nuevos servicios de procesamiento de información.	Área de Seguridad de la Información
	Implementar el proceso de autorización de nuevos servicios servicios de procesamiento de información.	Área de Seguridad de la Información
(A 6.1.5) 6.1.5 Acuerdos de confidencialidad	Identificar los requisitos de seguridad de la información que deben constar en los acuerdos de confidencialidad o no divulgación, tanto para usuarios internos	Área de Seguridad de la Información
	Elaborar los acuerdos de confidencialidad.	Departamento Legal
	Incluir los acuerdos de confidencialidad en los contratos laborales de la Universidad	Recursos Humanos
	Hacer firmar los acuerdos de confidencialidad a las personas que están laborando actualmente.	Recursos Humanos
	Definir un proceso para aplicar los acuerdos de confidencialidad a las partes externas.	Departamento Legal
	Revisar por lo menos una vez al año los requisitos de los acuerdos de confidencialidad para garantizar que estén acorde a las necesidades de la	Área de Seguridad de la Información

Figura 37: Muestra de acciones por riesgo

En lo posterior, la Universidad realizará un análisis de factibilidad para determinar los beneficios que se obtienen al implantar las acciones del plan de tratamiento y los costos asociados.

4.2.9 Emisión de informes finales

Una vez finalizada la metodología de evaluación se ha determinado que la Universidad no dispone de un sistema de gestión de seguridad de la

información implantado y que el nivel de cumplimiento de los requisitos exigidos por la norma es bajo.

La mayoría de los controles sugeridos en el anexo A de la norma se aplican de manera parcial, generando una brecha de seguridad muy considerable.

En el proceso de admisión de han identificado riesgos de diferente nivel, sin embargo, existen riesgos nivel alto que podrían afectar a la universidad y que requieren una acción inmediata.

En esta etapa se presentarán dos informes relacionados al nivel de seguridad de la información:

- Brecha de seguridad respecto a la norma ISO/IEC 27001:2005.
- Plan de tratamiento para mitigar los riesgos.

Por pedido de las autoridades de la universidad, a continuación se describirán los resultados de manera general salvaguardando la confidencialidad de la información, los informes completos reposan en las instalaciones de la Universidad.

4.2.9.1.1 Informe: Brecha de seguridad de la información respecto a la norma ISO/IEC 27001:2005

El informe consta de dos partes, la primera describe el nivel de cumplimiento de requisitos obligatorios de la norma ISO/IEC 27001:2005, y la segunda muestra el nivel de cumplimiento de los controles implementados respecto a las mejores prácticas del Anexo A.

Requisitos obligatorios de la norma

En el presente informe se describen los porcentajes de cumplimiento de la gestión de seguridad de la información respecto a la norma internacional ISO/IEC 27001:2005, que surge de la evaluación realizada

al proceso de admisión de estudiantes de la Universidad Tecnológica Equinoccial. A pesar de que la evaluación se realizó a un proceso específico “Admisión”, los resultados abarcan a toda la Gestión de Seguridad de la Información que se realiza en la Universidad, por lo tanto, se acerca a la realidad de la institución en un contexto general.

Establecimiento y Gestión del SGSI

La Universidad cumple en un nivel bajo, se evidencia que implícitamente la Universidad ha iniciado las actividades para tener un Sistema de gestión de seguridad de la información, sin embargo, aún debe mejorar en muchos aspectos. Se requiere mayores esfuerzos para implantar, poner en funcionamiento el sistema y crear conciencia de seguridad en toda la institución. Los resultados y gráficos obtenidos de la evaluación no se incluirán en la presente tesis con la finalidad de preservar la confidencialidad de los datos.

Establecer el SGSI: La Universidad cumple con un nivel bajo, se evidencia que los riesgos de seguridad son identificados y evaluados parcialmente por el personal del Instituto de Informática y Computación, bajo criterios definidos en cada área de trabajo. También, como medida para mitigar los riesgos se aplican ciertos controles del Anexo A de la norma. ISO/IEC 27001:2005.

Sin embargo, la gestión no está alineada a lo establecido en la norma ISO/IEC 27001:2005, se requiere: una política de seguridad de la información global que brinde las directrices en la Universidad, establecer los criterios de seguridad de la información por parte de las autoridades, implementar una metodología de gestión de riesgos formalmente implementada, evaluar los riesgos de todos los activos principales del proceso, implementar acciones y controles en base a los riesgos prioritarios, y establecer una declaración de aplicabilidad establecida en función de la realidad de la institución. Los resultados y gráficos obtenidos

de la evaluación no se incluirán en la presente tesis con la finalidad de preservar la confidencialidad de los datos.

Requisitos de documentación: La Universidad lleva un control de los documentos y registros de las actividades de gestión de seguridad de la información, sin embargo, no existen procedimientos formales implementados para realizar esta actividad y se encuentran fuera del contexto del SGSI. Los resultados y gráficos obtenidos de la evaluación no se incluirán en la presente tesis con la finalidad de preservar la confidencialidad de los datos.

Responsabilidad de la Dirección

La Universidad cumple con un nivel bajo. La institución provee recursos para proteger los activos acorde a los requerimientos puntuales de seguridad informática pero no se realiza en todo el contexto del SGSI, y recursos para la formación y capacitación en seguridad de la información a personal del Instituto de Informática y Computación. Sin embargo, se requiere de una planificación para capacitar y concientizar a todos los involucrados en el proceso en temas de seguridad de la información. Los resultados y gráficos obtenidos de la evaluación no se incluirán en la presente tesis con la finalidad de preservar la confidencialidad de los datos.

Auditoría del SGSI

La Universidad cumple con un nivel bajo, el cumplimiento de este requisito depende de la implementación y funcionamiento del Sistema de Gestión de Seguridad de la Información (SGSI), principalmente del requisito 4.1 “Establecimiento y Gestión del SGSI”. Una vez que se implemente el SGSI y comience a operar se podrá realizar auditoria a intervalos planificados que permitan mejorar el sistema de gestión identificando las conformidades y no conformidades respecto a la norma.

Revisión de la Dirección

Al igual que el requisito anterior, la Universidad cumple con un nivel bajo, al no existir un SGSI formalmente implantado, no cuenta con registros que permitan evidenciar las revisiones de la gestión de seguridad de la información por parte de las autoridades de la institución. Los resultados y gráficos obtenidos de la evaluación no se incluirán en la presente tesis con la finalidad de preservar la confidencialidad de los datos.

Mejora del SGSI

La Universidad cumple con un nivel bajo, el cumplimiento de este requisito depende de la implementación y funcionamiento del SGSI, una vez que se implemente el SGSI y comience a operar se podrá mejorar y aplicar acciones correctivas, preventivas y mejora continua. Los resultados y gráficos obtenidos de la evaluación no se incluirán en la presente tesis con la finalidad de preservar la confidencialidad de los datos.

Bajo lo expuesto, la Universidad cumple con un nivel bajo, existe una brecha de seguridad alta respecto a los requisitos de la norma ISO/IEC 27001:2005, es necesario implementar las acciones descritas en el plan de tratamiento de riesgos para mitigar los riesgos de seguridad e iniciar con la implantación del SGSI. Los resultados y gráficos obtenidos de la evaluación no se incluirán en la presente tesis con la finalidad de preservar la confidencialidad de los datos.

Controles del Anexo A

La determinación de la brecha de seguridad respecto al Anexo A de la norma ISO/IEC 27001:2005 se determina a través de la verificación del cumplimiento de los 133 controles incluidos en los dominios de control A5-A15.

En primera instancia se determina los controles que son aplicables a la realidad de la Universidad, en el análisis realizado al proceso de Admisión de la UTE se considera que 131 controles, los controles excluidos son: A.10.9.1 “Comercio electrónico” y A.10.9.2 “Transacciones en línea” “Transacciones en línea” pertenecientes al objetivo de control A.10.9 “Servicios de comercio electrónico”.

Los resultados obtenidos son los siguientes:

Política de seguridad de la información: La Universidad cumple con un nivel bajo, actualmente no existe una política para dirigir y dar soporte a la seguridad de la información. Los resultados y gráficos obtenidos de la evaluación no se incluirán en la presente tesis con la finalidad de preservar la confidencialidad de los datos.

Organización de la seguridad de la Información: La Universidad cumple con un nivel medio bajo, existe compromiso de las autoridades con la seguridad informática pero se aún no se ha formalizado la gestión de seguridad de la información, ni los sistemas accesados, comunicados y procesados por terceras partes. No existe una unidad de seguridad de la información que se responsabilice por la gestión de la seguridad. Los resultados y gráficos obtenidos de la evaluación no se incluirán en la presente tesis con la finalidad de preservar la confidencialidad de los datos.

Gestión de Activos: La Universidad cumple con el nivel bajo, se mantiene un inventario de activos físicos pero no de los activos de información, los propietarios del riesgo se define parcialmente; no existen las directrices de clasificación de la información. Los resultados y gráficos obtenidos de la evaluación no se incluirán en la presente tesis con la finalidad de preservar la confidencialidad de los datos.

Seguridad de recursos humanos: La Universidad cumple con un nivel medio, se realiza un proceso de selección antes del empleo, se definen las responsabilidades de seguridad de forma parcial, sin embargo, no

existe procedimiento formal de retiro de derechos de acceso y devolución de activos de información cuando el personal termina su contratación laboral. Falta una formación en toma de conciencia acerca de las políticas y procedimientos de seguridad de la información. Los resultados y gráficos obtenidos de la evaluación no se incluirán en la presente tesis con la finalidad de preservar la confidencialidad de los datos.

Seguridad física y ambiental: La Universidad alcanza un nivel medio alto, existen controles de acceso físico implementados pero no se han diseñado e implementado protecciones contra amenazas externas como inundación, sismo, explosión, disturbios y otras formas de desastre natural. Los resultados y gráficos obtenidos de la evaluación no se incluirán en la presente tesis con la finalidad de preservar la confidencialidad de los datos.

Gestión de comunicaciones y operaciones: La Universidad cumple con un nivel medio alto, no existen procedimientos formales para ciertas actividades operativas, ausencia de segregación de funciones en puestos críticos, la gestión de cambios para los recursos del sistema y procesamiento de la información es informal, no se da seguimiento a los servicios de terceras partes, existen recursos de producción que se utilizan en ambientes de desarrollo y pruebas de los sistemas informáticos. Los resultados y gráficos obtenidos de la evaluación no se incluirán en la presente tesis con la finalidad de preservar la confidencialidad de los datos.

Control de accesos: La Universidad cumple con un nivel medio alto, se evidencia la ausencia de una política de control de accesos, no existe un proceso formal de gestión de contraseñas de usuario y revisión de derechos de accesos de los usuarios en todos los sistemas y redes.

No existe una política de escritorios limpios de papel y dispositivos de almacenamiento removibles, y pantallas limpias. Los resultados y gráficos

obtenidos de la evaluación no se incluirán en la presente tesis con la finalidad de preservar la confidencialidad de los datos.

Adquisición, desarrollo y mantenimiento de sistemas de información: La universidad cumple con un nivel medio bajo, no cuenta con una guía formal de implementación de seguridad a nuevos sistemas, existen datos que son compartidos por los dos sistemas, y no existe un registro el control de vulnerabilidades técnicas sobre los sistemas. Los resultados y gráficos obtenidos de la evaluación no se incluirán en la presente tesis con la finalidad de preservar la confidencialidad de los datos.

Gestión de incidentes de seguridad de la información: La Universidad cumple con un nivel bajo, los eventos de seguridad se reportan de manera informal, no existe un procedimiento formal que canalice todos los eventos y debilidades de seguridad hacia los responsables, no ha establecido un mecanismo para cuantificar y dar seguimiento a los incidentes de seguridad. Los resultados y gráficos obtenidos de la evaluación no se incluirán en la presente tesis con la finalidad de preservar la confidencialidad de los datos.

Gestión de continuidad del negocio: La Universidad cumple con un nivel bajo, no existe un procedimiento para el manejo de la continuidad del negocio, no existe planificación relacionada y no se ha definido una estructura organizacional que se encargue de la planificación de este punto. Los resultados y gráficos obtenidos de la evaluación no se incluirán en la presente tesis con la finalidad de preservar la confidencialidad de los datos.

Cumplimiento: La universidad cumple con un nivel bajo, no existen reglamentos para los controles criptográficos utilizados en la infraestructura de red y aplicaciones. Los resultados y gráficos obtenidos de la evaluación no se incluirán en la presente tesis con la finalidad de preservar la confidencialidad de los datos.

De los 131 controles analizados, un valor bajo cumple con el requerimiento de la norma ISO/IEC 27001:2005 Anexo A, existen controles se encuentran en estado básico, controles deficientes y controles del Anexo A que no se han implementado. Lo que demuestra que la Universidad implícitamente está aplicando la seguridad de la información acorde a lo sugerido en la norma.

El informe se complementa con la presentación de la cantidad de controles del Anexo A agrupados de acuerdo a la pirámide de seguridad de la figura 57, cuyo enfoque está orientado a obtener el valor correspondiente a la seguridad organizativa, lógica, física y legal.

Figura 38: Pirámide de seguridad de la información en función de los controles de la norma ISO/IEC 27001:2005

La debilidad mayor se encuentra en la seguridad organizativa, debido a la falta de procesos, procedimientos y políticas que orienten la gestión, y a la falta de cultura institucional en temas de seguridad de la información. Los resultados y gráficos obtenidos de la evaluación no se incluirán en la presente tesis con la finalidad de preservar la confidencialidad de los datos.

En consecuencia, el cumplimiento de la Universidad es de nivel medio bajo, se evidencia la falta de una política de seguridad, inexistencia de una unidad que se encargue de dirigir el sistema de gestión de seguridad de la información y coordine las actividades en todos los departamentos de la Institución. Los resultados y gráficos obtenidos de la evaluación no se

incluirán en la presente tesis con la finalidad de preservar la confidencialidad de los datos.

Por lo expuesto, se concluye que en la Universidad Tecnológica Equinoccial no existe:

- Lineamientos generales de seguridad de la información que regulen las actividades del proceso de Admisión y las tareas realizadas por los funcionarios involucrados en el proceso.
- Formalización de los procesos y procedimientos de seguridad de la información.
- Involucramiento de las autoridades en temas relacionados a seguridad de la información.
- Departamento que se encargue de la gestión de seguridad de la Información a nivel institucional, las actividades se enfocan únicamente se enfocan a seguridad informática.
- Entrenamiento y concientización suficiente en temas de seguridad a los funcionarios de la Universidad.

En tal razón, las consecuencias están reflejadas en la incertidumbre sobre por el grado de vulnerabilidad del proceso Admisión de estudiantes de pregrado, campus Quito, efectividad de los controles de seguridad implementados actualmente, la protección efectiva de la información y se genere una brecha demasiado alta entre la situación actual respecto a los requisitos de la norma ISO/IEC 27001:2005.

4.2.9.1.2 Informe: Plan de tratamiento de riesgos.

El presente informe es un instrumento primordial para la toma de decisiones estratégicas relacionadas a seguridad de la información, contiene las acciones enfocadas a minimizar el impacto de los riesgos encontrados en el proceso de Admisión de Estudiantes de la Universidad.

Es importante mencionar que el 22.2% (22 de 99) de los activos están expuestos a riesgos de nivel alto y se torna imprescindible la acción inmediata por parte de las autoridades.

La implantación de una acción puede ayudar a minimizar riesgos de nivel medio y bajo, por ejemplo: La acción “5.1.1 Documento de la política de seguridad de la información” puede mitigar paralelamente al riesgo de nivel 3 R080 “Fuga de información” y “mala utilización de la información” que afecta al activo “Exámenes de conocimientos resueltos por los aspirantes a la Facultad de Arquitectura” y al riesgo de nivel 2 R107 “Fuga de información” que afecta al activo “Listado de aspirantes admitidos”.

Las acciones descritas en el plan de tratamiento de riesgos están basadas en las mejores prácticas de la norma ISO/IEC 27001:2005 y tendrán un responsable se para llevar a cabo su ejecución.

En el plan de tratamiento se recomienda a responsables de ejecutar una acción según las mejores prácticas de la norma ISO/IEC 27001:2005 y NTE INEN-ISO/IEC 27005:2012, a pesar de que no exista en la estructura organizacional de la Universidad. Por ejemplo, “Desarrollar la planificación anual de las actividades de seguridad de la información para toda la Universidad” se asigna al Área de Seguridad de la Información (no existe actualmente).

Es importante mencionar que la presente tesis no abarca el análisis de factibilidad de cada acción propuesta, los costos de implementación y tiempo de ejecución.

Cuadro 45: Acciones relacionadas a "Política de seguridad de la información"

Política de seguridad de la información

Control	Acciones	Responsable
Documento de la política de seguridad de la información	Desarrollar, aprobar una política de seguridad de la información a nivel institucional	Rectorado, Comité de Seguridad de la Información
	Publicar la política de seguridad de la información	Relaciones Públicas
	Comunicar la política de seguridad de la información a usuarios internos y las relaciones con terceras partes.	Todos los departamentos
Revisión de la política de seguridad de la información	Verificar mensualmente el cumplimiento de política de seguridad de la información	Área de Seguridad de la información
	Revisar que la política esté actualizada de acuerdo a los cambios organizacionales.	Rectorado

Cuadro 46: Acciones relacionadas a "Organización interna"

Organización interna

Control	Acciones	Responsable
Compromiso de la dirección para la seguridad de la información	Asignar recursos para el desarrollo de las actividades relacionadas a la seguridad de la información	Rectorado
	Comunicar el apoyo de las autoridades en temas relacionados a seguridad de la información.	Rectorado
	Participar activamente en reuniones de Comité de seguridad de la información	Rectorado
	Aprobar las actividades de seguridad de la información en actividades de la universidad, por ejemplo publicaciones en medios de comunicación, capacitaciones.	Rectorado
Coordinación de la seguridad de la información	Establecer un Comité de seguridad de la información conformado por representantes de autoridades de diferentes áreas de la Universidad	Rectorado
	Definir los roles y responsabilidades del Comité de Seguridad de la Información.	Rectorado

Asignación de responsabilidades sobre seguridad de la información	Crear un área específica para tratar temas de Seguridad de la Información, que reporte directamente a Rectorado	Rectorado
	Definir los roles y responsabilidades del área de Seguridad de la Información	Rectorado
	Designar al oficial de seguridad de la información	Área de Seguridad de la información
	Desarrollar la planificación anual de las actividades de seguridad de la información en función de los objetivos institucionales.	Área de Seguridad de la información
	Definir, aprobar y difundir las normas y procedimientos de seguridad de la información para toda la Universidad	Área de Seguridad de la información
	Establecer y comunicar las directrices generales de seguridad de la información a los usuarios internos y externos que tengan relación con la Universidad.	Área de Seguridad de la información
Proceso de autorización para los recursos de procesamiento de la información	Definir, aprobar y comunicar el proceso de autorización de nuevos servicios de procesamiento de información.	Área de Seguridad de la Información
	Implementar el proceso de autorización de nuevos servicios de procesamiento de información.	Área de Seguridad de la Información
Acuerdos de confidencialidad	Identificar los requisitos de seguridad de la información que deben constar en los acuerdos de confidencialidad o no divulgación, tanto para usuarios internos como para las partes externas.	Área de Seguridad de la Información
	Elaborar los acuerdos de confidencialidad.	Departamento Legal
	Incluir los acuerdos de confidencialidad en los contratos laborales de la Universidad	Recursos Humanos
	Hacer firmar los acuerdos de confidencialidad a las personas que están laborando actualmente.	Recursos Humanos
	Definir un proceso para aplicar los acuerdos de confidencialidad a las partes externas.	Departamento Legal
	Revisar por lo menos una vez al año los requisitos de los acuerdos de confidencialidad para garantizar que estén acorde a las necesidades de la organización	Área de Seguridad de la Información
Contacto con las autoridades	El oficial de seguridad de la información debe tener contacto con grupos de interés y el CSIRT nacional e internacional	Área de Seguridad de la Información
Revisión independiente de la seguridad de la información	Revisar al menos una vez al año los controles, procesos y procedimientos para la seguridad de la información	Área de Seguridad de la Información
	Realizar auditorías semestrales de la gestión de seguridad de la información.	Auditoría (Interna o Externa)

A continuación se presentan las recomendaciones sobre la ejecución del plan de tratamiento de riesgos:

- La principal acción que la Universidad debe realizar es crear el área de seguridad de la información que reporte directamente a Rectorado y coordine todas las actividades relacionadas al sistema de gestión de seguridad.
- Crear una política de seguridad y directrices generales para el buen uso de los activos importantes para la Universidad.
- Realizar un análisis de costo/beneficio de las acciones del plan de tratamiento de riesgos para determinar la priorización en la ejecución de las acciones acorde a las necesidades de la universidad.
- Implantar de manera inmediata las acciones sugeridas en este plan de tratamiento de riesgo para minimizar el impacto negativo sobre la institución, y a corto plazo dar tratamiento a los riesgos de nivel medio y bajo.
- Orientar todas las acciones del plan de tratamiento del riesgo a los requerimientos de seguridad de la información definidos por las autoridades de la Universidad.
- Implantar una metodología de gestión de riesgos formal que permita evaluar los riesgos y reajustar el plan de tratamiento de riesgos acorde a los cambios en la Universidad.
- Establecer los indicadores y métricas para medir la efectividad de los controles implementados, reajustar las acciones para mitigar los riesgos y mejorar la calidad de la gestión de seguridad de la información.
- Capacitar y concientizar al personal sobre la seguridad de la información para minimizar la probabilidad de materialización de una amenaza.

Con las acciones recomendadas en el plan de tratamiento de riesgos, la Universidad podrá iniciar el camino para implantar un sistema de gestión

de seguridad de la información en el campus matriz Quito y posteriormente replicarlo en las Sedes, que ayude a minimizar los riesgos en la elaboración de exámenes, evaluación a los aspirantes, análisis de datos y ponderaciones requeridas para la toma de decisiones por parte de las autoridades.

4.2.9.1.3 Seguridad de la información percibida por los aspirantes en el Proceso de Admisión.

Para conocer la percepción de los aspirantes sobre la seguridad de la información en la recepción de exámenes del proceso de Admisión de Estudiantes de Pregrado UTE se realizó una encuesta a los aspirantes al finalizar el examen de admisión del periodo septiembre 2013 – febrero 2014. El instrumento utilizado se detalla en el anexo B.

La aplicación de la encuesta fue realizada por los autores de la presente tesis con el apoyo del personal del departamento de Orientación Académica UTE y los profesores tutores de aulas.

Cálculo de la muestra representativa

El cálculo de la muestra representativa se realizó mediante la fórmula f1 detallada a continuación:

f1) $$n = \frac{N\sigma^2 Z^2}{(N-1)e^2+\sigma^2 Z^2}$$

Dónde:

n = el tamaño de la muestra.

N = tamaño de la población.

$\sigma =$ Desviación estándar de la población que, generalmente cuando no se tiene su valor, suele utilizarse un valor constante de 0,5.

Z = Valor obtenido mediante niveles de confianza. Es un valor constante que, si no se tiene su valor, se lo toma en relación al 95% de confianza equivale a 1,96 (como más usual) o en relación al 99% de confianza equivale 2,58, valor que queda a criterio del investigador.

e = Límite aceptable de error muestral que, generalmente cuando no se tiene su valor, suele utilizarse un valor que varía entre el 1% (0,01) y 9% (0,09), valor que queda a criterio del encuestador.

$$n = \frac{6080 * 0{,}5^2 * 1{,}96^2}{(6080 - 1) * 0{,}05^2 + 0{,}5^2 * 1{,}96^2}$$

$$n = 362$$

Con lo que se receptaron resultados de 362 encuestas durante los procesos de recepción de exámenes a los aspirantes para el periodo septiembre 2013 – febrero 2014.

Resultados de la encuesta

La encuesta de 5 preguntas efectuada a 362 aspirantes y los resultados de la tabulación de datos se detallan a continuación:

PREGUNTA 1: ¿Se verificó tu identidad dentro del aula?

Los resultados de la pregunta 1 evidencian que los funcionarios de la Universidad si realizan la verificación de identidad previa al inicio del examen, el 98.62% (357) respondió que sí y el 1,38% (53) de los aspirantes respondieron que no se había verificado su identidad dentro del aula, como se indica en la figura 39.

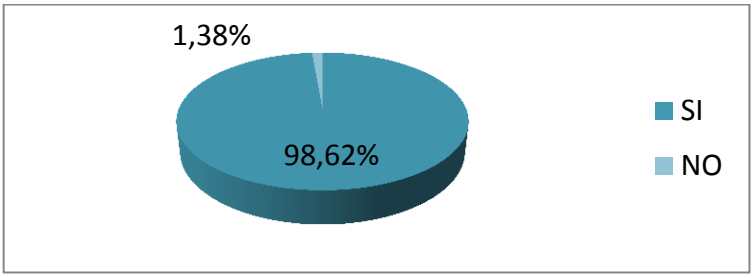


Figura 39: Resultados a la pregunta1: ¿Se verificó tu identidad dentro del aula?

PREGUNTA 2: ¿Usted rindió el examen de admisión en el aula y horario asignado durante la inscripción?

En la figura 40 se presentan los resultados de la pregunta 2, el 2,49% (9) de los aspirantes no rindieron el examen de admisión en el aula y horario asignado durante la inscripción, mientras que el 97,51% (353) indicaron que el examen fue rendido en el aula y horario asignado durante la inscripción.

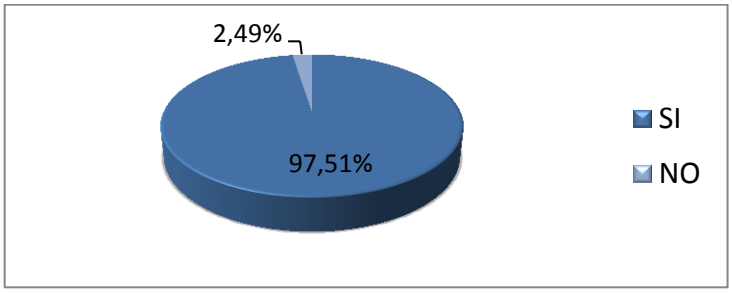


Figura 40: Resultados a la pregunta2: ¿Usted rindió el examen de admisión en el aula y horario asignado durante la inscripción?

PREGUNTA 3: ¿Se presentó algún problema con la computadora utilizada para rendir el examen de admisión?

- Apagó la computadora
- Congeló la pantalla
- Reinició la computadora
- Dañó el teclado, mouse, monitor

- Otro:
- NO existieron problemas

En los resultados se obtuvieron que al 0,28% (1) de los aspirantes se les apagó la computadora durante el examen, el 0,28% (1) tuvo problemas con los periféricos de entrada o salida y el 99,44% (360 encuestados) indicaron que no existieron problemas durante la rendición del examen de admisión, como se indica en la figura 41.

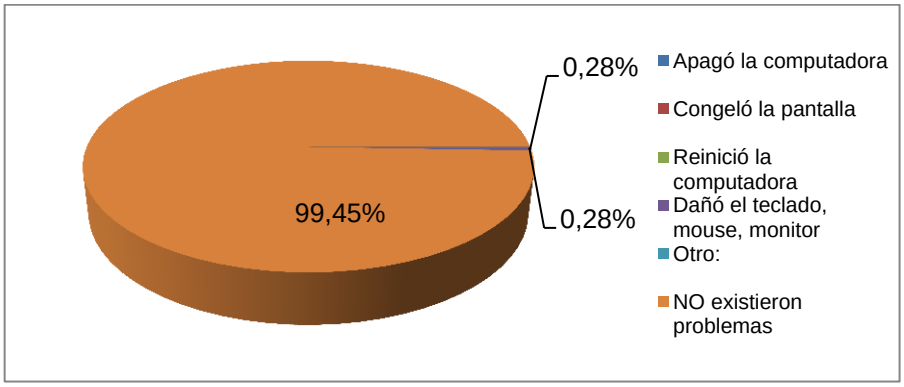


Figura 41: Resultado porcentual de la cantidad de problemas presentados en los equipos de cómputo

PREGUNTA 4: ¿Existieron problemas relacionados con el despliegue de las preguntas, gráficos y contenidos?

El 3,87% (14 encuestados) de los aspirantes indicaron existieron problemas relacionados con el despliegue de las preguntas, gráficos y contenidos, mientras que el 96,13% (348 encuestados) informaron que no tuvieron ninguna clase de problemas con el examen de admisión, como se indica en la figura 42.

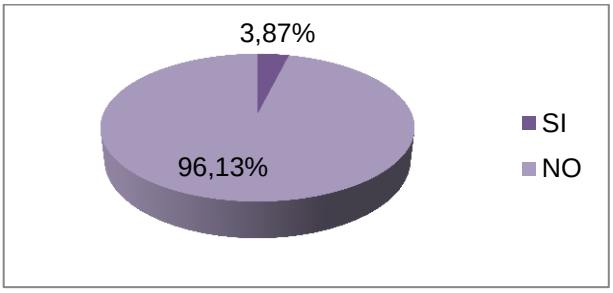


Figura 42: Resultados a la pregunta: ¿Existieron problemas relacionados con el despliegue de las preguntas, gráficos y contenidos?

PREGUNTA 5: ¿Consideras que tu examen será calificado de manera confiable, ya que es calificado a través de un sistema informático?

El 95,86% (347 encuestados) de los aspirantes indicaron confían en el sistema informático que realiza la calificación de los exámenes, mientras que el 4,14% (15 encuestados) indicaron desconfianza, como se indica en la figura 43.

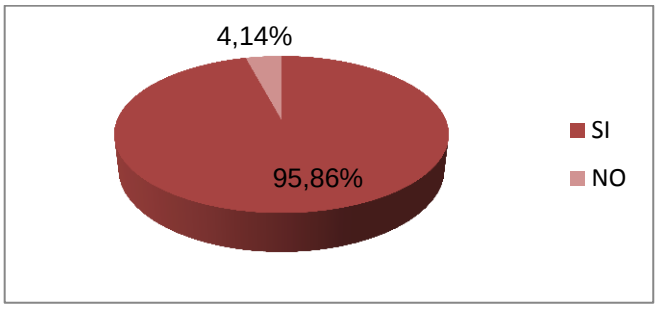


Figura No. 43: Resultados a la pregunta: ¿Consideras que tu examen será calificado de manera confiable, ya que es calificado a través de un sistema informático?

Conclusión derivada de la encuesta

De los resultados de la encuesta realizada a la muestra de aspirantes que rindieron el/los examen/es de ingreso para el periodo Septiembre 2013 - Febrero 2014 en la UTE se puede concluir que los aspirantes de la

Universidad tienen un alto grado de confianza en el proceso de recepción de exámenes y en los sistemas informáticos que soportan el proceso de Admisión de aspirantes en la UTE, sin embargo, a pesar de que existe una cantidad baja de aspirantes que no están conformes con el sistema, la Universidad debe emprender acciones necesarias para mantener y/o mejorar la confianza obtenida hasta el momento.

Respecto a la logística de la recepción de exámenes, se determina que el personal de la Universidad en coordinación el Vicerrectorado Académico ha ejecutado eficientemente los procedimientos durante el proceso, sin embargo, es necesario implantar un proceso de gestión de incidentes que permita minimizar el tiempo de respuesta a los problemas suscitados durante la recepción de los exámenes.

5 CAPÍTULO IV

5.1 Conclusiones

- La metodología propuesta se diferencia de la norma ISO/IEC 27005 porque define el proceso a través de un conjunto de pasos específicos para realizar la evaluación de seguridad de la información y conseguir mejores resultados.
- La selección de la metodología de gestión de riesgos que se aplicará a una organización, depende de su situación actual y los requerimientos de seguridad definidos por los directivos de alto nivel.
- Las directrices de la gestión de riesgos basada en ISO/IEC 27005 brindan un soporte continuo a los requisitos del sistema de gestión de seguridad de la información basado en ISO/IEC 27001, permiten plantear recomendaciones oportunas y reducir el riesgo a un nivel aceptable.
- La gestión de la seguridad de la información y la gestión de riesgos son sistemas dinámicos que se adaptan fácilmente a los cambios organizacionales a fin de mantener o mejorar la efectividad de los controles implementados y el nivel de seguridad en toda la organización.
- Las organizaciones deben alinear las directrices de seguridad de la información y la gestión de riesgos a los requerimientos definidos por la alta dirección para asegurar el cumplimiento de los objetivos del negocio.
- La participación de la alta dirección en el proceso de gestión de riesgos y en el sistema de gestión de seguridad es de vital importancia para establecer un compromiso en toda la organización, definir los lineamientos de seguridad, implementar el sistema y priorizar las acciones del plan de tratamiento que reducirán la ocurrencia de los riesgos.

5.2 Recomendaciones

- La metodología cualitativa debe ser utilizada en la etapa de evaluación de riesgos cuando se realiza por primera vez una evaluación de seguridad de la información y las organizaciones pretendan no invertir demasiados esfuerzos en actividades irrelevantes.
- Utilizar la metodología cuantitativa en la etapa de evaluación de riesgos cuando la gestión de la organización se encuentre en un nivel de madurez alto o se requiera profundizar el análisis sobre un activo o proceso específico.
- Incluir el análisis de brecha en las evaluaciones de seguridad de la información basadas en la ISO/IEC 27001 previo al análisis de riesgos para revelar los riesgos más críticos y direccionar adecuadamente los esfuerzos para mitigarlos.
- La alta dirección debe aceptar los riesgos residuales antes de iniciar la implementación del plan de tratamiento para evitar que las acciones propuestas se omita o se pospongan.

CAPÍTULO 6

6 Bibliografía

Asamblea Constiuyente. (2008). *CONSTITUCIÓN DEL ECUADOR .*

ANUIES. (2013). Resultados de la encuesta de seguridad de la información 2011 en las instituciones de educación superior. Retrieved August 6, 2013, from http://publicaciones.anuies.mx/libros/166/resultados-de-la-encuesta-de-seguridad-de-la-informacion-2011-en-las

AutoevaluaciónUTE.pdf. (n.d.). Retrieved from http://www.ute.edu.ec/Autoevaluaci%C3%B3n.pdf

Baray, H. L. (2006). *Introducción a la metodología de la investigación.* Chiguagua, Mexico.

Bel Ibérica Soluciones de Seguridad Global. (01 de 07 de 2011). La universidad y la seguridad . *El Portal de los Profesionales de la Seguridad.* Recuperado el 30 de 07 de 2013, de http://www.belt.es/noticiasmdb/home2_noticias.asp?id=12305

BELT. (n.d.). La universidad y la seguridad. Retrieved August 6, 2013, from http://www.belt.es/noticiasmdb/home2_noticias.asp?id=12305

Bertolín, J. A. (2008). *Seguridad de la información: redes, informática y sistemas de información*. Editorial Paraninfo.

Blanca Rubiela Duque Ochoa - Metodologías de Gestión de Riesgos. (n.d.). Retrieved from http://auditoriauc20102mivi.wikispaces.com/file/view/Metodolog%C3%ACas+deGesti%C3%B2n+de+Riesgos.pdf

Brunner, J. J. (1990). *Educación Superior en América Latina: Cambios y Desafíos.* Santiago de Chile: Fondo de Cultura Económica.

BSIGROUP. (n.d.). ¿Los riesgos de seguridad de la información amenazan a su negocio? Nueva norma mejorada ISO / IEC 27005 que refuerza la protección. Retrieved August 8, 2013, from http://www.bsigroup.es/es/certificacion-y-auditoria/Sistemas-de-

gestion/Novedades/Noticias-2011/LD-News-Source-/Los-riesgos-de-seguridad-de-la-informacion-amenazan-a-su-negocio-Nueva-norma-mejorada-ISO-IEC-27005-que-refuerza-la-proteccion/

CEAACES. (2013). *Modelo Evaluación.* Recuperado el 23 de 07 de 2013, de CEAACES: http://www.ceaaces.gob.ec

CINDA. (2012). *Aseguramiento de la Calidad en Iberoamérica - Educación Superior Informe 2012.* Santiago de Chile: RIL Editores.

CSI Computer Security Institute. (2011). Computer Crime and Security Survey. (R. Richardson, Ed.) Recuperado el 07 de 25 de 2013, de https://cours.etsmtl.ca/log619/documents/divers/CSIsurvey2010.pdf

De Freitas, V. (2009). Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. *Enlace*, *6*(1), 43–55.

de Pablos Heredero et al. (2006). *Dirección y gestión de los sistemas de información en la empresa*. ESIC Editorial.

Disposición 1330 del BOE núm. 25 de 2010 - BOE-A-2010-1330.pdf. (n.d.). Retrieved from http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *04*(02), 92–100. doi:10.4236/jis.2013.42011

Elisabete Piresa, F. M. (2012). Integration of Information and Communication Technology in Schools. Online Safety. *Procedia Technology 5 - SciVerse ScienceDirect*, 59-66.

Fernandez Collado, C., Hernandez Sampieri, R., & Baptista Lucio, P. (2006). *Metodología de investigación* (4ta Edición ed.). Mac Graw-Hill.

Flores Barrios, L., Soto del Ángel, M., Camacho Díaz, O., & Barrera Reyes, M. (2011). En el análisis de impacto de los sistemas de gestión de seguridad de la información bajo la norma ISO/IEC 27001 en las empresas de la cuidad Tuxpan, Mexico. *Revista de la Alta Tecnología y Sociedad,* *5*(ISSN 1940-2171), 7. Obtenido de

http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=c3a887bf-8bac-4ea3-b4a6-12d86db8fcf5%40sessionmgr112&vid=2&hid=118

Flores Barrios, L., Soto del Ángel, M., Camacho Díaz, O., & Barrera Reyes, M. (2011). En el análisis de impacto de los sistemas de gestión de seguridad de la información bajo la norma ISO/IEC 27001 en las empresas de la cuidad Tuxpan, Mexico. *Revista de la Alta Tecnología y Sociedad, 5*(ISSN 1940-2171), 7. Obtenido de http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=c3a887bf-8bac-4ea3-b4a6-12d86db8fcf5%40sessionmgr112&vid=2&hid=118

Gazzola, L., & Didriksson, A. (2008). *Tendencias de la Educación Superior en América Latina y el Caribe.* Caracas: IESALC-UNESCO.

Gimer Torres, I., Michelena Fernández, E., & Hernández Rabell, L. (2010). MODELO PARA MEJORAR LA GESTIÓN DE PROCESOS EDUCATIVOS UNIVERSITARIOS. *Revista Científica de la Cuaje*, 1-7. Obtenido de http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=8175c924-103d-49d9-b337-eebd68d451b1%40sessionmgr10&vid=2&hid=26

Global, B. I. (01 de 07 de 2011). La universidad y la seguridad. *El Portal de los Profesionales de la Seguridad.* Recuperado el 30 de 07 de 2013, de http://www.belt.es/noticiasmdb/home2_noticias.asp?id=12305

Huber, M. (2011, July). The risk university: Risk identification at higher education institutions in England. Monograph. Retrieved August 6, 2013, from http://www.lse.ac.uk/CARR

Insights, AlgoSec Survey. (2012). *Algosec Inc.* Recuperado el 30 de 07 de 2012, de Algosec Inc.: http://www.algosec.com/resources/files/Specials/Survey%20files/120404_Survey%20Report.pdf

Instituto Ecuatoriano de Normalización. (28 de 06 de 2013). *Instituto Ecuatoriano de Normalización*. Recuperado el 16 de 07 de 2013, de Normas oficializadas desde Enero2013: http://www.inen.gob.ec

Instituto Tecnológico de Veracruz. (n.d.-a). Amenazas Informáticas. Retrieved August 4, 2013, from http://www.prograweb.com.mx/Seguridad/010201amenazas.html

Instituto Tecnológico de Veracruz. (n.d.-b). Riesgos Informáticos. Retrieved August 5, 2013, from http://www.prograweb.com.mx/Seguridad/010203riesgos.html

Instituto Tecnológico de Veracruz. (n.d.-c). Vunerabilidad informática. Retrieved August 4, 2013, from http://www.prograweb.com.mx/Seguridad/010202vulnerabilidad.html

ISO 27000. (n.d.). ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información. Retrieved August 5, 2013, from http://www.iso27000.es/sgsi.html Sección 2a - 2f

International Register of ISMS Certificates. (2013). *International Register of ISMS Accredited Certificates*. Recuperado el 26 de 05 de 2013, de International Register of ISMS Accredited Certificates: http://www.iso27001certificates.com/

International Register of ISMS Certificates. (s.f.). *International Register of ISMS Accredited Certificates*. Recuperado el 26 de 05 de 2013, de International Register of ISMS Accredited Certificates: http://www.iso27001certificates.com/

ISO. (2011). *ISO survey.* Recuperado el 16 de 07 de 2013, de ISO: http://www.iso.org/iso/iso-survey

mapa.jpg (JPEG Image, 1600 × 743 pixels) - Scaled (45%). (n.d.). Retrieved January 15, 2014, from http://3.bp.blogspot.com/-qgioRVI-jxo/UCwmk9x2UyI/AAAAAAAAABI/A_Z7p7JFCBw/s1600/mapa.jpg

Melo, A. H. (2008). El derecho informático y la gestión de seguridad de la información. Una perspectiva con base en la norma ISO27001. *Revista de derecho, 29*, 336-366. Recuperado el 30 de 07 de 2013, de http://web.ebscohost.com/ehost/detail?sid=a59e203e-0dbc-4961-8e73-dbf6c42ce4a0%40sessionmgr11&vid=1&hid=26&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#db=a9h&AN=34969402

MINISTERIO DE COMUNICACIONES COLOMBIA - Diagnóstico de la situación Actual Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea. (n.d.). Retrieved from http://programa.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/DiagnosticodelaSituacionActual.pdf

Ministerio de Hacienda y Administraciones Públicas. (n.d.). Magerit versión 3. Retrieved August 8, 2013, from https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/

Modelo_Educativo_new.pdf. (n.d.). Retrieved from http://www.ute.edu.ec/Modelo_Educativo_new.pdf

Mora, M. E. (2006). *Metodología de la Investigación - Desarrollo de la inteligencia* (5ta ed.). Mexico.

NTP ISO IEC 17799 - isoiec17799.pdf. (n.d.). Retrieved from http://www.bvindecopi.gob.pe/normas/isoiec17799.pdf

PARANINFO. (2011). *SEGURIDAD INFORMATICA ED.11 Paraninfo*. Editorial Paraninfo.

Pires, E., & Moreira, F. (2012). The Integration of Information and Communication Technology in Schools. Online Safety. *Procedia Technology*, *5*, 59–66. doi:10.1016/j.protcy.2012.09.007

PM157A_D04_WhitePaper_BestPractices_HigherEd_112811.indd - PMA_Education_BestPractices_WhitePaper.pdf. (n.d.). Retrieved from http://pmacompanies.com/pdf/MarketingMaterial/PMA_Education_BestPractices_WhitePaper.pdf

Rama, G. (1987). *Desarrollo y Educación en América Latina y el Caribe.* Buenos Aires: Kapelusz.

Sayef Sami Hassen, M. S. Z. (2013). Managing University IT Risks in Structured and Organized Environment. *Journal of Applied Sciences, Engineering and Technology*, 2270–2276.

SEMPLADES . (2008). *Seminario Internacional de Admisión y Nivelación a la Universidad en América Latina - Diagnóstico y Perspectivas .* Quito: Hojas y Signos.

Silvio, J. (2000). *La Virtualización de la Universidad: Como transformar la Educación Superior con la tecnoclogía?* Caracas.

Sistema Nacional de Nivelación y Admisión - SNNA. (12 de 03 de 2013). *Reglamento del SNNA.* Obtenido de Sistema Nacional de Nivelación y Admisión: http://www.snna.gob.ec/descargas/Reglamento.pdf

Stallings, W. (2003). *Fundamentos de seguridad en redes: aplicaciones y estándares*. Pearson Educación.

Stouffer, K., Falco, J., & Scarfone, K. (2013). *Guide to Industrial Control Systems (ICS) Security : Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC)* (No. NIST SP 800-82r1). National Institute of Standards and Technology. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf

Symantec. (04 de 2013). *Publicaciones de Security Response.* Obtenido de Security Response: http://www.symantec.com/es/mx/security_response/publications/threatreport.jsp

Taylor, S., & Bogdan, R. (1988). *Introducción a los métodos cualitativos de investigación.*

Tanenbaum, A. S. (2003). *Redes de computadoras*. Pearson Educación.

UNAM. (10 de 12 de 2012). Riesgo tecnológico y su impacto para las organizaciones parte II Gobierno de TI y riesgos. (A. R. Castro, Ed.) *Seguridad Cultura de Prevención para TI, 11 y 15*. Recuperado el 25 de 07 de 2013, de http://revista.seguridad.unam.mx

Unidad de Excelencia Académica y Desarrollo Curricular | UTE. (n.d.). Retrieved January 22, 2014, from

http://www.ute.edu.ec/DefaultUEA.aspx?idPortal=11&idSeccion=973&idCategoria=1095

Universidad Tecnológica Equinoccial. (18 de 05 de 2009). *Sistema de Difusión de Documentación Legal de la Universidad Tecnológica Equinoccial - LEX UTE.* Recuperado el 15 de 07 de 2013, de LEX - UTE: http://app.ute.edu.ec/lexute/AdminDoc/Carpetas.aspx

Villegas, M., Meza, M., & Leon , P. (01 de 2011). Las metricas, elemento fundamental en la construccion de modelos de madurez de la seguridad informatica. *Revista Telematique*. Recuperado el 24 de 07 de 2013, de http://www.publicaciones.urbe.edu/index.php/telematique/article/viewArticle/975/html

Viloria, O., & Blanco, W. (2009). Modelo Sistémico de la Seguridad de la Información en las Universidades. *Revista Venezolana de Análisis de Coyuntura, XV*(ISSN 1315-3617), 219-240. Recuperado el 31 de 07 de 2013, de http://www.redalyc.org/articulo.oa?id=36411719011

Viloria, O., Villegas, M., & Blanco, W. (06 de 2009). La Seguridad de la Información bajo una Perspectiva de la Madurez Organizacional. *Seventh LACCEI Latin American and Caribbean Conference for Engineering and Technology (LACCEI'2009)* (págs. 1-8). San Cristóbal, Venezuela: LACCEI. Recuperado el 31 de 07 de 2013, de http://www.laccei.org/LACCEI2009-Venezuela/p162.pdf