UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

MAYO 2018 – OCTUBRE 2018

PROYECTO DE INVESTIGACIÓN

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERA EN SISTEMAS

TEMA:

"Uso de los Modelos de Control Informático y su incidencia en la Seguridad de la Información en el Sistema de Control de Calificaciones de la Universidad Técnica de Babahoyo".

EGRESADA:

Daysi Magdalena Morante Mosquera

TUTOR:

Ing. Harry Saltos Viteri

Año 2018

Dedicatoria

El presente trabajo de investigación está dedicado a Dios, quien ha estado conmigo en todo momento, a mi abuelita Idalide, a quien con su amor, esfuerzo y apoyo, le debo todo lo que soy hoy en día; a mis hermanos Brayan y Elmer a quienes amo y siempre han creído en mí; a mi tía Julia y a su esposo Eduardo por todo su afecto y apoyo incondicional como si fuera su propia hija; y a toda mi familia que de una u otra manera siempre han estado ahí para extender su mano de ayuda.

Agradecimiento

Primeramente agradezco a Dios y a mi familia por ser una parte fundamental de mis estudios durante todos estos años de esfuerzo y dedicación.

A mi tutor de tesis, el Ing. Harry Saltos Viteri, por ser comprometido y guiarme durante todo el proceso de titulación.

A la Universidad Técnica de Babahoyo por ser mi casa durante todos los años de estudio.

Autorización de la autoría intelectual

Yo, DAYSI MAGDALENA MORANTE MOSQUERA en calidad de autor del presente proyecto investigativo acerca de "Uso de los Modelos de Control Informático y su incidencia en la Seguridad de la Información en el Sistema de Control de Calificaciones de la Universidad Técnica de Babahoyo", por medio de la presente autorizo de manera exclusiva a la UNIVERSIDAD TÉCNICA DE BABAHOYO, hacer uso del contenido de este material con fines educativos.

Los derechos que como autor me corresponden, con excepción de la presente autorización, seguirán vigentes a mi favor, de conformidad con lo establecido en la Ley de Propiedad Intelectual y su Reglamento.

Babahoyo, 06 de febrero de 2019

Informe final del sistema Urkund

URKUND

Urkund Analysis Result

Analysed Document:	Morante_Mosquera_Daysi_Magdalena_Ingenieria_Sistemas_2019.doc (D48288237)
Submitted:	2/25/2019 4:47:00 AM
Submitted By:	mile_dm4@hotmail.com
Significance:	1 %

Sources included in the report:

https://aquinodul.wordpress.com/2015/05/24/cobit/

Instances where selected sources appear:

2

Índice general

ENCUESTA SOBRE EL USO DE LOS MODELOS DE CONTROL INFORMATICO Y SU INCIDENCIA EN LA SEGURIDAD DE LA INFORMACION 75

Índice de gráficos

Índice de Tablas

Introducción.

Este proyecto investigativo está dirigido al estudio de las normas de control informático y su aplicación en el sistema de control de calificaciones de la Universidad técnica de Babahoyo.

Se conoce que la tendencia de las nuevas tecnologías revoluciona cada vez más el mundo; pero a medida que esto sucede se presentan un sin número de ventajas y desventajas, es por ello que se recomienda la actualización frecuente de los sistemas informáticos, los cuales son los factores esenciales para el crecimiento de una institución, organización o un país.

Es relevante destacar que los modelos de control informático son mayormente usados por grandes compañías reconocidas a nivel mundial como GENERAL ELETRIC, APPLE, SAMSUNG ELECTRONICS, IBM, GOOGLE, ORACLE, entre otros; los mismos que constantemente actualizan sus servicios y proporcionan grandes tecnologías.

La adecuada administración de los modelos de control informático otorga seguridad estable en los sistemas de información de las compañías, evitando vulnerabilidades y contratiempos en los sistemas tecnológicos.

CAPÍTULO I.- DEL PROBLEMA

1.1. Idea o tema de Investigación.

Uso de los Modelos de Control Informático y su incidencia en la Seguridad de la Información en el Sistema de Control de Calificaciones de la Universidad Técnica de Babahoyo.

1.2. Marco Contextual.

1.2.1. Contexto Internacional.

En las organizaciones a nivel mundial, lo más importante de sus activos es la información, como es de conocimiento general en tal sentido, pues se han creado parámetros técnicos a modelo de estándares y normas que permiten mayor seguridad, es así que las empresas como Dell, Asus, Hp, tienen modelos de normas de control informático definidos como ITIL y COBIT, los cuales ejecutan acciones determinadas que son aplicables a los procesos de recuperación de los Sistemas de Información.

Desde hace más de 15 años en Europa implementaron normas de calidad, para la gestión de sistemas y tecnologías de la información, para las compañías; mientras que en Latinoamérica empezó la revolución de las normas informáticas hace cinco años.

La aparición de las normas de control informático revolucionaron las tecnologías de la información, que definen los términos y estándares necesarios para brindar protección a

las empresas que adquieran este tipo de normas; que se encargan de describir los procesos a seguir de manera justa y segura.

ISO 9000 es el nombre que se le da a las normas de seguridad, las cuales son las responsables de los procesos y actividades como planes y estrategias claves que se realicen en una determinada compañía que cuenten con tecnologías de la información.

La implementación de normas de control informático es apropiada para empresas que requieran control y calidad en sus servicios; las organizaciones con la tecnología que poseen deberían asegurar la confidencialidad de la información, agregando estándares y buenas prácticas de gestión donde se realizarían aplicaciones, información infraestructura y personas; estas normas de control de control de seguridad se deben regir al modo de operación de las empresas en cuanto a las TIC.

1.2.2. Contexto Nacional.

La norma ISO 17799 que se refiere al conjunto de controles basados en las mejores prácticas de la seguridad de la información, siendo un estándar internacional que cubre todos los aspectos sobre la seguridad de la información.

Hasta el momento, en Ecuador lo más frecuente en delitos informáticos era, por ejemplo, la clonación de tarjetas, las estafas, extorsiones, acceso a correos electrónicos y el buen manejo de los sistemas que procesan gran cantidad de informática.

Desde el año 2009, ecuador empezó a implementar informática Technology Service Management Form (ITSMF), con la finalidad de ofrecer calidad y eficiencia de sus servicios tecnológicos, en diferentes áreas empresariales, incluyendo buenas prácticas en la gestión de sus servicios y procesos de la información.

Las certificaciones de calidad brindan seguridad que satisfacen los requerimientos y las perspectivas de sus clientes, y de esta manera las empresas puedan obtener un sin número de beneficios.

Gran cantidad de compañías que ofrecen seguridad informática proporcionan servicios económicos y asesoría en cuanto a las normas de certificación y buenas prácticas de seguridad; estas compañías se encargan de monitorizar y administrar los sistemas que demandan múltiples soluciones para cada cliente.

1.2.3. Contexto Local.

En la provincia de Los Ríos existen varias empresas, las cuales día a día se esmeran por proteger su información con estándares de control informático.

Las empresa públicas o privadas se ven en la necesidad de implementar políticas de seguridad en sus sistemas informáticos, debido a las amenazas constantes por parte de hackers quienes en todo momento están prestos a violar la integridad de la información; que es el derecho que tiene toda compañía, haciendo referencia a los estándares ISO27001, por lo que se hace frecuente los delitos informáticos que no son más que fraudes generados por accesos no autorizados a los sistemas tecnológicos.

La compañía Quicornac S.A. perteneciente al cantón Vinces, cuenta con el estándar ISO 9001 20000 que certifica que cumple con los requisitos de un sistema de gestión de calidad, pero no cuenta con estándares de seguridad de la información ISO 27001.

1.2.4. Contexto Institucional.

Con la creación de la Universidad Técnica de Babahoyo el 5 de octubre de 1971, vino consigo un sin número de oportunidades académicas para toda la provincia de Los Ríos.

La Universidad Técnica de Babahoyo con el pasar del tiempo ha crecido no solo territorialmente, sino académicamente brindando educación de tercer nivel, arrojando al campo laboral profesionales de calidad.

Con el auge de la tecnología, se inició un alto índice de oportunidades tanto para unidades académicas, compañías o simplemente para uso personal; esta gran tecnología conlleva a delitos informáticos, como extorciones y fraudes.

La Universidad Técnica de Babahoyo, en cuanto a seguridad tiene implementado un Firewall el cual no presta la seguridad necesaria que requiere un tipo de sistema como el Sistema de Control de Calificaciones de la Universidad Técnica de Babahoyo, el cual no es del todo seguro, puesto que es vulnerable a diversos tipos de ataques.

Cuenta con una intranet poco segura, provocando poner en alto riesgo las actividades y procesos informáticos de la institución. Es evidente apreciar la facilidad de acceso para cualquier usuario a la red, poder conectarse al internet y acceder en forma libre e ilimitada a cualquier sitio WEB. Por otro lado, las redes sociales están constantemente disponibles y no existe restricción alguna para ejecutar aplicaciones que puedan conectarse fuera de la red.

El problema de acceso al Sistema de Control de Calificaciones de la Universidad Técnica de Babahoyo; se debe principalmente a la carencia de control, monitoreo y

gestión de la seguridad y los servicios de red, debido a que no está asegurada contra ataques y amenazas constantes que deterioran en un 80% la estructura del sistema (Vega Villacis, 2017).

El departamento de las Tecnologías de la Información, es el encargado de salvaguardar la integridad de sus servidores, los cuales manipulan gran cantidad de información, como los de las páginas web, aulas virtuales e indistintos servicios que proporciona la red. Por lo tanto es de suma importancia gestionar y analizar las causas que se provocan amenazas a los activos (Mejia Viteri, 2016).

1.3. Situación problemática.

¿De qué manera incide la ausencia de seguridad de la información en el Sistema de Calificaciones de la Universidad Técnica de Babahoyo?

El problema actualmente se fundamenta en el Sistema de Control de Calificaciones de la Universidad Técnica de Babahoyo; el cual se caracteriza por presentar anomalías en las calificaciones y la información tanto de docentes como de estudiantes.

Al ingresar al Sistema Académico Integral (SAI), como estudiantes, docentes o personal administrativo, se puede evidenciar con claridad que de una u otra manera existen falencias, que conlleva a la inconformidad de lo que se desea realizar en el mismo.

El inicio del periodo académico es caótico, tanto para estudiantes como el personal administrativo; por lo que los estudiantes se aglomeran en las oficinas de la secretaria porque requieren agilizar sus procesos de matriculación. Puesto que a pesar de que existe un horario establecido por los decanatos de cada facultad para la matriculación en línea de cada nivel académico y la receptación de documentos; al momento de ingresar al sistema

los alumnos sienten gran inconformidad por los problemas que se presentan, como lo es la matriculación en línea a un nivel inferior al que corresponde y la ausencia de una o varias calificaciones; es por ello que se retrasa el proceso de matriculación.

El trabajo para el personal administrativo aumenta debido a que ellos son los encargados de atender y tratar de ayudar a los estudiantes para que puedan gestionar sus procesos académicos. Los docentes no están exentos a la problemática que existe en el sistema y se ven en apuros cuando intentan ingresar notas al sistema; ya sea porque los alumnos no estén debidamente matriculados, o simplemente no consten en el nivel académico correspondiente.

Estos factores influyen de manera inapropiada en el desempeño académico, puesto que la universidad por ser una institución de gran prestigio, perdería credibilidad y aumentaría su vulnerabilidad en el sistema; en esta investigación propondremos normas de seguridad informática para contrarrestar la influencia de las causas sobre el problema.

1.4. Planteamiento del problema.

1.4.1. Problema general.

¿De qué manera los modelos de control informático inciden en la seguridad de la información almacenada en el sistema de control de calificaciones de la Universidad Técnica de Babahoyo?

1.4.2. Subproblemas o derivados.

¿De qué manera incide la ausencia de normas de seguridad informática en el Sistema de Control de Calificaciones de la Universidad Técnica de Babahoyo?

¿Cuáles son los factores que afectan e impiden el ingreso al Sistema de Control de Calificaciones de la Universidad Técnica de Babahoyo?

¿Qué tipo de normas de seguridad se deben emplear para el correcto funcionamiento al Sistema de Control de Calificaciones de la Universidad Técnica de Babahoyo?

1.5. Delimitación de la investigación.

1.5.1. Delimitación Temporal.

Desde mayo a octubre de 2018.

1.5.2. Delimitación Espacial.

Línea de investigación: Redes y Conectividad

Objeto de estudio: Normas de control Informático

Campo de acción: Redes informáticas

Institución: Universidad Técnica de Babahoyo

Ubicación: Av. Universitaria Km $2^{1}/_{2}$ vía a Montalvo

Teléfono: 052570368

Correo electrónico: contacto@utb.edu.ec

País: Ecuador

Provincia: Los Ríos

Cantón: Babahoyo

1.6. Justificación.

La adquisición de normas de control informático, actualmente son el medio de seguridad más eficaz para proteger los sistemas informáticos; desde hace varios años tanto instituciones académicas como compañías emplean este tipo de normas, para asegurar de esta manera la seguridad de la información.

El uso de los modelos de control informático en el Sistema de Control de Calificaciones de la Universidad Técnica de Babahoyo, permitirá el mejor desempeño y actualización del sistema con estándares de calidad e infraestructuras de las Tecnologías de la Información que harán que dicho sistema sea ordenado, organizado, sistemático y con buenas practicas, brindando la seguridad que se necesita para proteger la información evitando riesgos y amenazas que se presenten.

El proceso de matriculación en línea seria menos estresante y mucho más fluido, por lo que no se presentarían anomalías al momento de ingresar al sistema; porque los modelos de control informático se ocuparían de corregir cualquier proceso que se esté ejecutando de manera irregular e informaría de manera automática al departamento de sistemas el cual es el responsable de toda la información que se maneja de la universidad.

La finalidad del presente proyecto investigativo, demostrará que con la adquisición de normas de seguridad informática por lo que trabajara con estándares y marcos de gestión administrativa y organizativa en cada proceso, y de esta manera se podrá brindar seguridad en la información; el Sistema de Control de Calificaciones de la Universidad Técnica de Babahoyo, será mucho más seguro y confiable al momento de subir al sistema las calificaciones, o simplemente visualizar las diferentes notas académicas, y los estudiantes, docentes y personal administrativo serán los más beneficiados por lo que no tendrán dificultades al acceder al sistema y podrán realizar cualquier proceso académico.

1.7. Objetivos de investigación.

1.7.1. Objetivo general.

Evaluar la incidencia de los modelos de control informático en la seguridad de la información en el sistema de control de calificaciones de la Universidad Técnica de Babahoyo.

1.7.2. Objetivos específicos.

Determinar las causas de la inseguridad informática en el Sistema de Control de Calificaciones de la Universidad Técnica de Babahoyo.

Investigar la información teórica referente al tipo de normas aplicadas en la seguridad de la información inherente a los sistemas informáticos

Analizar los factores que afectan a la seguridad del Sistema de Control de Calificaciones de la Universidad Técnica de Babahoyo.

CAPÍTULO II.- MARCO TEORICO O REFERENCIAL.

2.1. Marco teórico.

2.1.1. Marco conceptual.

2.1.1.1. Seguridad de la Información.

La tecnología y los sistemas de información avanzan continuamente en todo el planeta; la seguridad informática es una disciplina o ciencia que se creó para brindar seguridad en los procesos tecnológicos, como respaldar la integridad de la información de sus activos; sin embargo no es inmune a cualquier tipo de ataques. Los sistemas creados para brindar seguridad en la información deben custodiar y certificar la integridad de sus activos, detectando con anterioridad las amenazas que puedan ser contraproducentes para la estabilidad del sistema y su información.

Los sistemas informáticos están expuestos a frecuentes vulnerabilidades, por esta razón se cree inasequible que la seguridad de la información sea del todo completa; pero la seguridad informática se encarga de procesar, almacenar y proteger la integridad de sus activos (Estrategica, 2014).

Según el autor (Baca Urbina, 2016) para salvaguardar la integridad de la información y garantizar la seguridad de los sistemas, en primera instancia se debe proteger la información de robos y manipulación no autorizada por parte de personas ajenas al sistema; previniendo así que el sistema sea vulnerable y propenso a ataque y amenazas por parte de entes extraños al sistema.

Según (Chicano Tejada, 2014), el análisis de los procesos de la seguridad informática, es la auditoria informática; que permite recabar la información necesaria para la seguridad del hardware, previniéndolo de peligros; mientras que la seguridad del software es la responsable de corroborar procesos y actualizaciones que forman parte de un sistema.

Mediante Acuerdo Ministerial Nos. 804 y 837 de 29 de julio y 19 de agosto de 2011, respectivamente, la Secretaría Nacional de la Administración Pública creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación conformada por delegados del Ministerio de Telecomunicaciones y de la Sociedad de la Información, la Secretaría Nacional de Inteligencia y la Secretaría Nacional de la Administración Pública y dentro de sus atribuciones tiene la de establecer lineamientos de seguridad informática, protección de infraestructura computacional y todo lo relacionado con ésta, incluyendo la información contenida para las entidades de la Administración Pública Central e Institucional (EGSI, 2013).

2.1.1.2. Control Informático para la seguridad de la información.

Las normas de control informático proporcionan valides en la función de sus procesos, recomendando mecanismos que provean y salvaguarden la seguridad de la información. Toda institución pública o privada debe ser administrada con un adecuado control de la información; de esta manera se recomienda realizar un control interno exhaustivo de las organizaciones para suplir las expectativas de custodia y salvaguarda de los activos, manteniendo la veracidad y confiabilidad de procedimientos y técnicas que ayuden en las actividades, funciones y procesos reglamentados en el sistema (Muñoz Razo, 2002).

Las autoridades que permiten la difusión de certificados son personas especializadas en la materia. La autoridad certificante, quien se encarga de la emisión de certificados, suele ser un ente privado o público especializado en el tema. Dado los requerimientos técnicos y legales que son cuantiosos y estrictos, por ello es necesario que el organismo este en un alto nivel de seguridad. Los certificados corporativos o personales proporcionan diferentes servicios; los corporativos en la red externa y los personales en la red interna (Nakasone, 2012).

Las bases para el desarrollo de software se toman en consideración de los modelos informáticos se consideran actualmente, que permiten dictaminar los problemas mediante la abstracción. Model Driven Development (MDD) se encarga de monitorear la productividad y calidad de los procesos aplicados en modelos con indistinto nivel de abstracción (Coral Calero, Moraga, & Piattini, 2010).

Existen bibliotecas e infraestructuras informáticas creadas para brindar un mayor servicio en cuanto a la seguridad de redes y seguridad de la información, entre las cuales tenemos:

2.1.1.2.1. Los estándares de administración del riesgo.

Los riesgos informáticos son más frecuentes, por ello es recomendable el estudio de sus procesos, como los ataques, amenazas y las vulnerabilidades constantes, que puedan determinar las normas de control y así evitar cualquier tipo de vulnerabilidades. Los controles que sean adquiridos deben salvaguardar la integridad de la información del sistema en riesgo.

Por lo que es importante referenciar los siguientes:

ITIL.

ITIL (Information Technology Infrastructure Library), sus siglas en español significan: Biblioteca de Infraestructuras de Tecnologías de Información; permite la administración de servicios de buenas prácticas de las tecnologías de la información. ITIL es un derivado del estándar ISO 27001 y buenas prácticas que proponen servicios como, operación, diseño, estrategia, calidad del servicio y transiciones.

Según (Baud, 2017) ITIL presenta tres puntos imprescindibles:

Selecciona los servicios en base a la necesidad del cliente.

Eleva la calidad de los servicios requeridos.

Verifica el valor de los servicios proporcionados.

Los servicios informáticos trabajan en un area relacionada con las buenas prácticas, permitiendo rendimientos de calidad que permitan asumir riesgos y poder afrontarlos.

COBIT.

COBIT (Control Objetives for Information and Related Technology), sus siglas en español significan: Objetivos de Control para las Tecnologías de la Información y Relacionados; es una herramienta o marco de gestión informático que proporciona buenas practicas relacionado a la administración de las normas de control informático, en base a las tecnologías de la información (Fonseca Luna, Sistemas de Control Interno para organizaciones, 2011).

2.1.2. Marco referencial sobre la problemática de investigación.

2.1.2.1. Antecedentes investigativos.

Los antecedentes del presente proyecto se pudieron realizar en base a investigaciones y proyectos ya realizados en la UTB y en otras universidades del país y el mundo, con la finalidad de encontrar similitudes para la continuidad de los mismos o el reforzamiento del presente trabajo en cuanto a los procedimientos, técnicas y experiencias válidas.

Los sistemas de control están enfocados a seguir planes, métodos, estrategias y procedimientos para salvaguardar la seguridad de la información, los estándares a adoptar deben regirse a las normas y leyes vigentes de cada país, para obtener cambios positivos en cuanto a la seguridad de la información.

Previa y posteriormente a la evaluación de los procesos de ITIL V3 en indistinta empresa o institución, es necesario respaldar la seguridad del sistema antes ser evaluado y determinar las pautas que se deben aplicar para los diferentes propósitos (Soto Acosta & Valdivieso Jácome, 2014).

En la Universidad de las Fuerzas Armadas, Soto Acosta & Valdivieso Jácome, desarrollaron la tesis de maestría con el tema, “Diseño e implementación de un modelo de gestión de Service Desk basado en ITIL V3 para PDVSA Ecuador” en el año 2014.

Entre los objetivos para el desarrollo de este estudio investigativo se definen los siguientes:

Garantizar la seguridad de la información sobre los servicios de la las TI.

Delimitar el alcance de los servicios brindados y proponer acuerdos específicos con alto nivel de calidad para la gestión de las TI.

Inventariar y auditar la seguridad de la información de una manera práctica y sencilla, que permita la administración de activos del sistema.

El estudio de la presente maestría radica en que no existen metodologías de planificación, seguimiento y gestión de los servicios de TI que permitan evidenciar el impacto en las estrategias organizacionales de PDVSA.

La metodología que se utilizó, fue la investigación aplicada, que se caracterizó por ser sistemática, ordenada, metódica racional y critica; mediante metodologías de trabajo que utilicen procedimientos e instrumentos.

La gestión de los servicios de TI presenta 4 áreas de negocio:

Los usuarios finales y la alta dirección; se encargan de evaluar y monitorear la calidad del servicio recibido.

Los proveedores externos y los departamentos de las TI; entregan los servicios y cumplen las responsabilidades adquiridas para estar pendiente ante cualquier incidente que se presente en la plataforma tecnológica de indistinta organización.

Implementar ITIL implica constancia, tiempo y esfuerzo; utilizando metodologías en sus procesos.

Para que ITIL trabaje de una mejor manera, es necesario implementar un marco de referencia, como lo es COBIT que permite evaluar el estado inicial de un proceso.

El proceso PAM permitió evaluar el nivel de capacidad de los procesos de ITIL, que se plantearan antes y después de su implementación; obteniendo así un alto nivel dentro de la Gestión de Service Desk en PDVSA Ecuador.

COBIT 4.1, además de garantizar un eficiente gobierno de de las TI en cualquier organización, proporciona recursos importantes que permiten evaluar otros marcos de referencia como ITIL; dicha evaluación debe ser precisa y confiable, que garantice una visión clara de la situación actual.

Antes de la implementación de herramientas de gestión de las TI basadas en ITIL es necesario que las aplicaciones se acoplen a lo que necesite la organización, como soporte, capacidad, base de datos, recurrencia de usuarios para suplir con los requerimientos de cualquier tipo de organización.

La seguridad de la información influye directamente en el crecimiento de los proyectos de TI, las empresas u organizaciones se encargan de gestionar proyectos (Galán Chuquimarca & Brussil Velásquez, Guia Metodologica para Proyectos de TI basados en el marco de trabajo PMBOK desde la perspectiva de la gestion de servicio de ITIL, y su seguimiento a traves de las métricas de COBIT para empresas de Tecnologías de la Información, 2015).

En la Pontificia Universidad Católica del Ecuador, Galán Chuquimarca & Brussil Velásquez, desarrollaron la tesis de maestría con el tema, “Guía Metodológica para Proyectos de TI basados en el marco de trabajo PMBOK desde la perspectiva de la gestión de servicio e ITIL, y su seguimiento a través de las métricas de COBIT para empresas de Tecnologías de la Información” en el año 2015.

El objetivo principal que utilizaron para la realización de este estudio fue “establecer un modelo formal que apoye el éxito del desarrollo de proyectos en particular de TI”; que corresponden a la ejecución del proyecto.

Proponen varios objetivos para la gerencia de proyectos:

Los cambios en los requerimientos varían durante el ciclo de vida del proyecto.

Determinar mediante un presupuesto establecido el costo del proyecto

Garantizar el cumplimiento de los requerimientos.

Garantizar la satisfacción del cliente al término del proyecto.

Es imprescindible crear un amiente de trabajo organizado para que los proyectos tengan éxito en su ejecución.

ITIL se hizo importante y famoso cuando en 2003 la empresa Procter &Gamble en Estados Unidos, ahorro 5 millones de dólares con la implantación de ITIL.

ITIL se desarrolló al momento de que la mayoría de las organizaciones dependían cada vez más de la informática; es por ello que con mucha frecuencia, servicios informáticos que cumplan con las expectativas del cliente.

El objetivo de ITIL es ofrecer un marco que facilite los procesos de los servicios de TI.

ITIL maneja las siguientes funciones:

- El centro de servicios que se encarga de los procesos relacionados a los usuarios de las TI.

- La gestión de operaciones de TI, es responsable del servicio manteniéndolo.
- La gestión técnica, se encarga de incluir los aspectos técnicos involucrados en la gestión de las TI.
- La gestión de aplicaciones, es responsable de la gestión de del ciclo de vida de las TI.

ITIL se alinea a la gestión de proyectos, incluyendo procesos, como:

- Gestión de cambio.
- Servicio de activos y gestión de configuración.
- Gestión de conocimiento.
- Gestión de versiones e implementación.

COBIT, es un estándar que ofrece buenas prácticas, para la gestión y control de las TI; permitiendo en las organizaciones optimización de sus recursos a partir de las TI, disminuyendo así los niveles de riesgos.

Determinaron que las empresas poseen activos valiosos como la información y las tecnologías COBIT con sus buenas prácticas, es el encargado de asegurar la habilitación e procesos mediante recursos y s riesgos de TI.

COBIT 5 es un marco que se caracteriza por orientarse a procesos en controles y procesos de gobernanza y gestión de las TI; enfocados en el control y no en la ejecución.

Para que las TI tengan éxito, se debería implantar un sistema de control interno o un marco de trabajo COBIT, que aporta requerimientos de negocios, organizando actividades de TI.

COBIT presenta algunos principios:

- Satisface las necesidades de las partes interesadas, manteniendo un equilibrio entre realizar y optimizar el uso de recursos.
- Cubrir la empresa de extremo a extremo, se refiere a la información y a la tecnología como activos de la empresa.
- Aplicar un marco de referencia único integrado, se alinea a altos niveles de con marcos y estándares de trabajo en la gestión de las TI en una empresa u organización.
- Hacer posible un enfoque holístico, es efectivo en un gobierno y gestión de las TI.
- Separar el gobierno de la gestión, permite diferentes actividades con estructuras organizativas, que sirven para distintos propósitos.

Analizando las metodologías utilizadas lograron cumplir con los objetivos de la tesis de la maestría, aplicado a una compañía de TI.

Los estándares para la gestión de TI, permiten beneficios en cuanto a la estrategia de la empresa. Las cátedras impartidas en dicha maestría ayudaron a cubrir los requerimientos para nuevas habilidades a futuro; la universidad mediante esta maestría brinda las herramientas eficientes para la gerencia de TI.

Se aconseja tener autoridad, a los usuarios que apliquen en sus empresas esta guía metodológica para realizar la gestión de proyectos donde se podrá evidenciar lo que se desea obtener. Si se desea trabajar con el desarrollo del software se recomienda aplicar un análisis.

El capital más valiosos de las empresas son las tecnologías de la información; la mayoría de las veces el éxito de la empresa depende de los beneficios que aportan las

normas de control informático. COBIT con sus buenas prácticas en el gobierno TI es el encargado de asegurar, la alineación de Negocios, permitiendo la habilitación de Procesos de negocios, mediante la optimización de recursos y el Manejo de riesgos de Tecnologías de la Información (Galán Chuquimarca & Brussil Velásquez, 2015).

2.1.2.2. Categorías de análisis.

Normas de control interno de instituciones públicas

El departamento de las Tecnologías de la Información reglamentara adquisición, proceso y desarrollo de un software con métodos y procedimientos; en los cuales se pueden considerar:

La implantación del software se aplicara en base a proyectos con planes de contingencia debidamente certificados y respetando las leyes establecidas por el Estado (ESTADO, 2014).

La aplicación, mantenimiento y adopción de las leyes y estándares internacionales para la interfaz de usuario, validación de requerimientos, desempeño de los sistemas, mantenimiento y adopción de las leyes y estándares (ESTADO, 2014).

Favorecer, identificar y especificar los requerimientos institucionales que son aprobados por las entidades estatales; incluyendo requerimientos de entrada y salida, definiendo interfaces y procesos; plan de pruebas, y seguridad de control aplicables en auditoria (ESTADO, 2014).

Aceptación y especificación de criterios que abastecerán los requerimientos económicos y tecnológicos, análisis de riesgos en cuanto a costos y beneficios,

desarrollando estrategias para la aplicación de software, ante percances que puedan presentarse (ESTADO, 2014).

El software aplicativo en la adquisición, mantenimiento y procesos de desarrollo, se consideran: documentación de calidad, diseño físico y lógico, estándares de aplicación que están preparados para reaccionar ante cualquier error o ataque que se presente durante el proceso, siendo oportuno, auditable, control de ingreso (ESTADO, 2014).

La adquisición de software trabajara en el proceso de dispositivos que aseguren las sugerencias que satisfagan los requerimientos de la institución. El convenio estará detallado lo suficientemente con aspectos relacionados, como las licencias y servicios, que definen los procedimientos, para la adquisición de materiales generalizado, puntualizando el mantenimiento y soporte garantizador por el proveedor (ESTADO, 2014).

Las contrataciones efectuadas por usuarios ajenos a al desarrollo del software, debe evidenciar que los derechos de autor aplicados a la ley de propiedad, que pertenezcan a la institución y el contratista entregue los códigos fuentes (ESTADO, 2014).

El software llevado a cabo debe incluir procedimientos de configuración, pruebas y aceptación, considerando los aspectos validados. Contra la seguridad de la información y la organización, términos, aplicaciones existentes y los sistemas de bases de daos, la documentación requerida, manual de usuario, prueba del sistema (ESTADO, 2014).

Los derechos de autor del software pertenecerán de manera definitiva a la institución competente. Se obtendrá licencias para el software adquirido (ESTADO, 2014).

Las actas de aceptación de los usuarios de deben formalizar, los sistemas aprobados en pruebas y producción en su implantación (ESTADO, 2014).

La configuración, instalación y la elaboración de manuales técnicos, serán publicados de forma estable (ESTADO, 2014).

Estas técnicas o métodos en gran parte benefician a los sistemas informaticos de la Universidad Técnica de Babahoyo, puesto que se aplican en base a lo establecido.

La seguridad de la información.

Los departamentos de las TI, debe estar preparado para mantener a salvo la seguridad de la información y aplicar los siguientes mecanismos:

- La ubicación y acceso al departamento es áreas específicas como bibliotecas, servidores y desarrollo (ESTADO, 2014).
- Definir los procedimientos de respaldo en cronogramas establecidos (ESTADO, 2014).
- La actualización de la tecnología enviará la información con estándares respaldando la información recuperada (ESTADO, 2014).
- La garantía de gestión la información será almacenada en un lugar distinto a la empresa (ESTADO, 2014).
- La gestión e implantación del hardware y software vigilara la seguridad de la información, con hechos y pruebas periódicas en base a la vulnerabilidad de la seguridad (ESTADO, 2014).
- Establecida instalación física que abarque, técnicas y dispositivos, particularmente para controlar vulnerabilidades, y sosteniendo un control de humedad y temperatura entre otros (ESTADO, 2014).

- Los lugares de procesamiento opcionales se deben considerar (ESTADO, 2014).
- El personal de turno definirá los métodos de seguridad en las noches (ESTADO, 2014).

El plan de contingencias perteneciente al departamento de las TI, son aprobados para tomar acciones emergentes sobre el proceso de la información en programas o equipo.

- Se consideran los siguientes aspectos:
- Los riesgos se la seguridad de la información, definen planes de respuesta y contingencias específicas (ESTADO, 2014).
- La ejecución de técnicas de control para las TI, reflejando la solicitud de la empresa (ESTADO, 2014).
- Las operaciones en marcha de centros de cómputo en un Data Center gubernamental, mientras se mantenga la posibilidad de comunicaciones y respaldo de la información (ESTADO, 2014).
- La recuperación de desastres incluirá, prevención antes, durante y después de desastres (ESTADO, 2014).
- Realizar contingencias en caso de presentarse emergencias (ESTADO, 2014).
- Se describirá procedimientos en caso de emergencias que salvaguarden la veracidad en los sistemas de información (ESTADO, 2014).
- La aprobación de un plan de contingencia, se ejecutara con instrucciones y métodos, configurando los equipos de cómputo (ESTADO, 2014).

La gestión de las TI definirá procedimientos adecuados que salvaguarden la seguridad de la información de los servicios tecnológicos. Se consideran varios aspectos:

- La revisión frecuente determinara el trabajo de los recursos (ESTADO, 2014).
- Conferir la identidad de los usuarios relacionando los servicios tecnológicos con los sistemas (ESTADO, 2014).
- Normalizar la identidad y legalizar la gestión de los usuarios. (ESTADO, 2014).
- Verificación periódica del usuario en línea y los procedimientos realizados en los sistemas de información (ESTADO, 2014).
- Adoptar medidas de advertencia y enmiendas para salvaguardar la integridad de la información (ESTADO, 2014).
- Manipulación de operaciones y servicios para los procesos de requerimientos de las TI (ESTADO, 2014).
- Servicios de requerimientos y prioridades, que permitan la observación del cumplimiento de acuerdos ministeriales (ESTADO, 2014).
- Gestión de peticiones en cuanto a los servicios de información mediante procesos (ESTADO, 2014).
- La conservación de almacenamiento estará definido para el software y hardware, procurando la utilización de aplicaciones para la solución de problemas (ESTADO, 2014).
- Gestión y respaldo de librerías (ESTADO, 2014).
- Adoptar mecanismos que se acoplen a los procesos de protección de la información encriptada (ESTADO, 2014).

Los estándares que permiten gestionar la seguridad de las tecnologías de la información; se encargan de proporcionar los procesos y funciones, con estándares definidos como ITIL y COBIT.

COBI, es adoptado por las tecnologías de la información, creando los requerimientos necesarios para la implementación de herramientas.

ITIL, pertenece al estándar ISO 27001, donde se disponen mecanismos para la protección de la integridad de la información.

Estos dos estándares definen las vulnerabilidades a las que están expuestos los sistemas de información; proveen de actividades, en el desarrollo de la seguridad de la información.

2.1.3. Postura teórica.

La Universidad Técnica de Babahoyo fue el ambiente donde se analizó el uso de los modelos de control informático en el Sistema de Control de Calificaciones.

Siendo una unidad educativa de prestigio a nivel nacional y con gran cantidad de estudiantes; no es posible que en pleno siglo XXI, y con lo avanzada que esta la tecnología; solo cuente con un Firewall como protección de sus redes.

Por esta razón se sugiere la implementación de normas de control informático que permitirán la seguridad y confidencialidad de la información. Uno de los entes más vulnerables es el sistema de control de calificaciones el cual presenta diversas irregularidades al momento de ingresar al sistema ya que está expuesto a diferentes ataques.

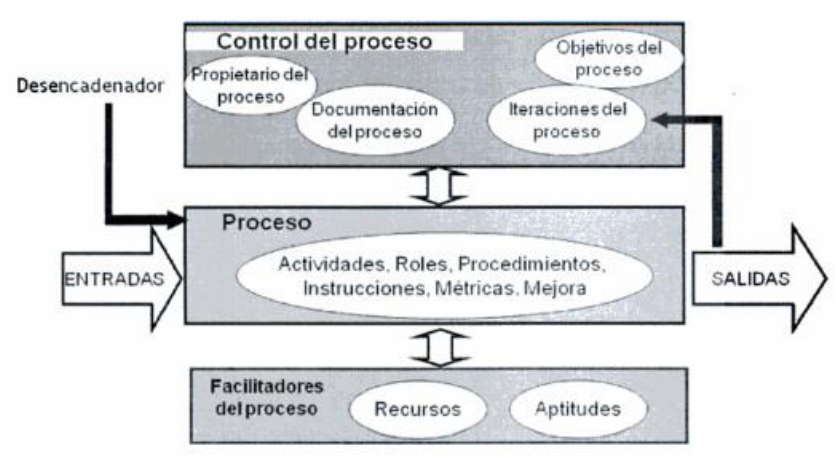
Según (Fonseca Luna, Sistema de Control Interno para Organizaciones, 2013), su teoría es buena porque desde su punto de vista, el control interno no es del todo seguro, debido a que la toma de decisiones es fundamental para el correcto desempeño del sistema. La utilización frecuente de las tecnologías de la información, en las organizaciones e instituciones permite restringir el acceso no autorizado de usuarios ajenos al sistema, donde se puede manipular y alterar la información emitida.

Todas las unidades académicas deben adoptar normas de control informático, que faciliten la seguridad y veracidad de la información, puesto que son estándares de calidad esenciales para las restricciones y buenas prácticas de seguridad informática.

ITIL.

ITIL se fundamenta en el trabajo de los usuarios, experiencias y buenas prácticas, permitiendo la gestión de servicios sobre las Tecnologías de la Información, incluyendo procesos de entrada y salida los cuales deben estar documentados y controlados para ser implementado, como ya se lo ha hecho en más 50 países (BAUD, 2015).

Figura 1



BAUD (2015). Ilustración de la Preparación para la certificación ITIL Foundation V3 ITIL V3-2011. Recuperado de https://books.google.com.ec/books?id=vOEGFtNoUjcC&pg=PA308&dq=itil+2014&hl=es-419&sa=X&ved=0ahUKEwjgvrWerc_gAhVrm-AKHeiDBgIQ6AEILjAB#v=onepage&q

Los procesos de gestión de seguridad se encargan del diseño de leyes de seguridad de los servicios de las TI, utiliza las normas ISO/IEC 27001 permitiendo la implementar los sistemas de gestión de sistemas de información, que se presenta en la fase de diseño del servicio (Diaz Orueta, Alzórriz Armendáriz, Sancristóbal Ruiz, & Castro Gil, 2014)

Los procesos de gestión de acceso se encargan de hacer cumplir las leyes de seguridad diseñadas en cada servicio, como privacidad, integridad autenticación y control de acceso; esto se presenta en la fase de operación del servicio (Diaz Orueta, Alzórriz Armendáriz, Sancristóbal Ruiz, & Castro Gil, 2014).

ITIL se encarga específicamente de los procesos relacionados al ciclo de vida de las Tecnologías de la Información, estos servicios de deben planificar, diseñarse, implementarse, operarse y mantenerse y estar sujetas a la mejora continua de sus fases (Diaz Orueta, Alzórriz Armendáriz, Sancristóbal Ruiz, & Castro Gil, 2014).

Figura 2

Díaz G; Alzórriz I; Sancristóbal E; Castro M. 2014. Figura6.6. El ciclo de vida de un servicio TI en ITIL. Ilustracion de Procesos y herramientas para la seguridad de redes. Recuperado de https://books.google.com.ec/books?id=dG4lAwAAQBAJ&pg=PT197&dq=itil+2014&hl=es-419&sa=X&ved=0ahUKEwi1nqG9zs_gAhUII6wKHZsuD

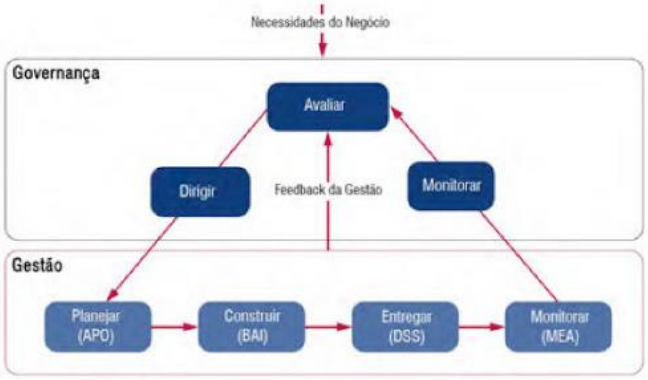
COBIT.

COBIT aprueba auditorias y evaluaciones de los sistemas informáticos de una organización, para estimar los beneficios y el desempeño en lo que respecta a la seguridad informática, permitiendo a los usuarios comprender y encargarse de los peligros informáticos (BAUD, 2015).

COBIT es un modelo de gobernanza de gestión de las TI; está estructurado de forma gerencial y lógica, atendiendo las necesidades de gobernanza corporativas basadas en las Tecnologías de la Información; su metodología evalúa los intereses de sus objetivos,

habilitando principios, políticas, modelos, procesos, estructuras, cultura, ética, servicios, infraestructura aplicadas a los procesos (Cantabria, 2015).

Figura 3



Cantabria, E. 2015. FIGURA 1 - VISÃO DO FRAMEWORK COBIT 5.0. Recuperado de https://books.google.com.ec/books?id=rsafCgAAQBAJ&pg=PA37&dq=COBIT+2015&hl=es-419&sa=X&ved=0ahUKEwjUrvWC3s_gAhVoTd8KHchUAu4Q6AEIOTAC#v=onepage&q=COBIT%202015&f=false

Según el sitio web (WordPress.com, 2015), el principal objetivo de COBIT es proveer de guías de alto nivel para estipular controles internos, el cual con lleva:

- Afianzar el buen gobierno, protegiendo los intereses de los Clientes, accionistas, empleados, etc (WordPress.com, 2015).
- Certificar el cumplimiento normativo del sector al que pertenezca la organización (WordPress.com, 2015).
- Favorecer la eficiencia de los procesos y actividades de la organización (WordPress.com, 2015).
- Salvaguardar la integridad, disponibilidad y confidencialidad de la información (WordPress.com, 2015).

2.2. Hipótesis.

2.2.1. Hipótesis general.

La utilización de los modelos de control informático incidirá favorablemente en la seguridad de la información almacenada en el sistema de control de calificaciones de la Universidad Técnica de Babahoyo.

2.2.2. Subhipótesis o derivadas.

- La carencia de normas de seguridad informática incidirá negativamente en el Sistema de Control de Calificaciones de la Universidad Técnica de Babahoyo.
- Si analizáramos los factores que afectan e impiden el ingreso al Sistema de Control de Calificaciones de la Universidad Técnica de Babahoyo podríamos salvaguardar la integridad de la información.
- Las normas de seguridad se deberían emplear para el correcto funcionamiento al Sistema de Control de Calificaciones de la Universidad Técnica de Babahoyo.

2.2.3. Variables.

2.2.3.1. Variable dependiente.

Seguridad de la Información.

2.2.3.2. Variable independiente.

Modelos de Control Informático.

CAPÍTULO III.- RESULTADOS DE LA INVESTIGACIÓN.

3.1. Resultados obtenidos de la investigación.

3.1.1. Pruebas estadísticas aplicadas.

La siguiente formula es para realizar encuestas y obtener la muestra.

$$\mathrm{n} = \frac{\mathrm{Z}^2 * p * q}{\mathrm{e}^2}$$

Donde:

n= muestra

N= población

e= margen de error

Z= nivel de confianza

p= probabilidad a favor

q= probabilidad en contra

Para obtener la población y muestra del proyecto investigativo se tomó en consideración 384 individuos entre ellos estudiantes, docentes y personal administrativo

de la Facultad de Administración Finanzas e Informática de la Universidad Técnica de Babahoyo.

$$\mathrm{n} = \frac{\mathrm{Z}^2 * p * q * N}{\mathrm{e}^2\ (N-1) + \mathrm{Z}^2 * p * q}$$

$$\mathbf{n} = \frac{\mathbf{1.96^2 * 0.5 * 0.5 * 384}}{\mathbf{0.06^2(384-1) + 1.96^2 * 0.5 * 0.5}}$$

$$\mathrm{n} = \frac{368.7936}{2.3392}$$

$$\mathrm{n} = 157{,}65$$

3.1.2. Análisis e interpretación de datos.

Resultados de la encuesta realizada a los estudiantes, docentes y personal administrativo de la Facultad de Administración, Finanzas e Informática de la Universidad Técnica de Babahoyo.

1. **Conoce si la UTB utiliza seguridad informática en sus sistemas?**

Alternativa	Frecuencia	Porcentaje
Si	240	63%
No	144	37%
Total	384	100%

Tabla 1, Elaborado por: (Daysi Morante, 2018).

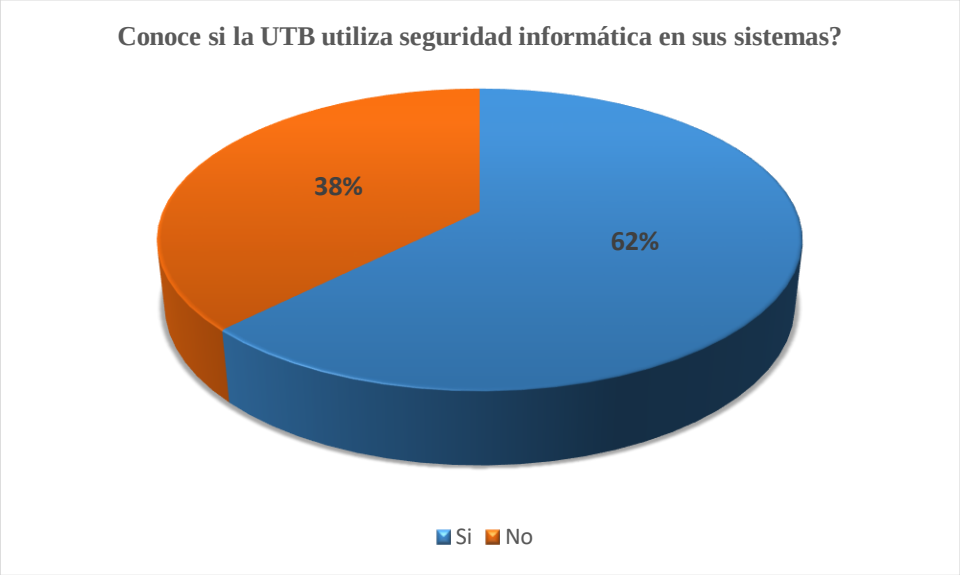


Ilustración 1, Elaborado por: (Daysi Morante, 2018).

Análisis e interpretación. El 62% de la población encuestada contestaron que si tienen conocimiento de que la Facultad de Administración Finanzas e Informática de la Universidad Técnica de Babahoyo utilice seguridad informática en sus sistemas; mientras que el 38% de la población encuestada no cuenta con dicha información.

2. **Tiene conocimiento acerca de lo que es un modelo de control informático?**

Alternativa	Frecuencia	Porcentaje
Si	149	39%
No	235	61%
Total	384	100%

Tabla 2, Elaborado por: (Daysi Morante, 2018).

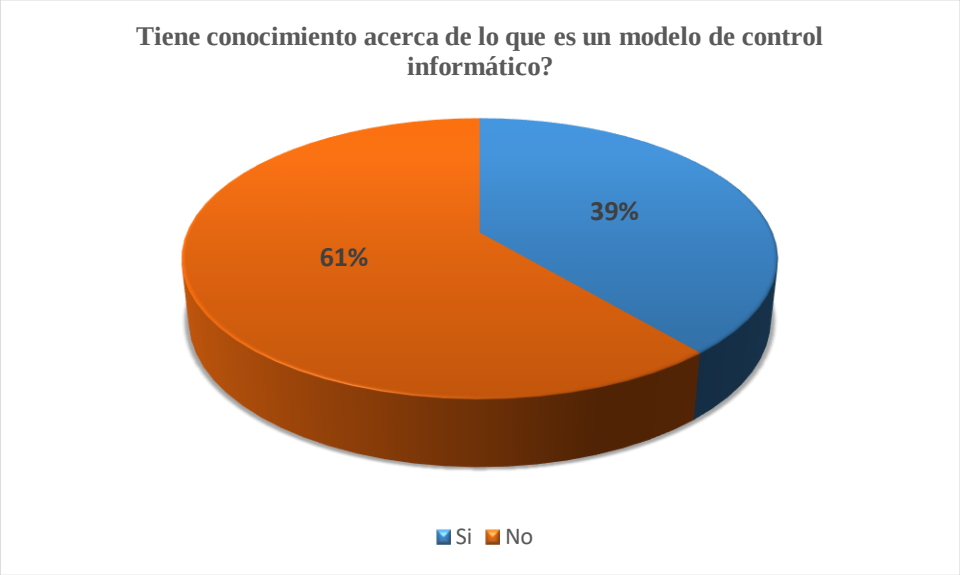


Ilustración 2, Elaborado por: (Daysi Morante, 2018).

Análisis e interpretación. El 61% de la población encuestada no tiene conocimiento acerca de lo que es un modelo de control informático; mientras que el 39% de los encuestados si tienen dicho conocimiento.

3. Está conforme con el servicio del SAI en el periodo de matrículas online?

Alternativa	Frecuencia	Porcentaje
Si	164	43%
No	220	57%
Total	384	100%

Tabla 3, Elaborado por: (Daysi Morante, 2018).

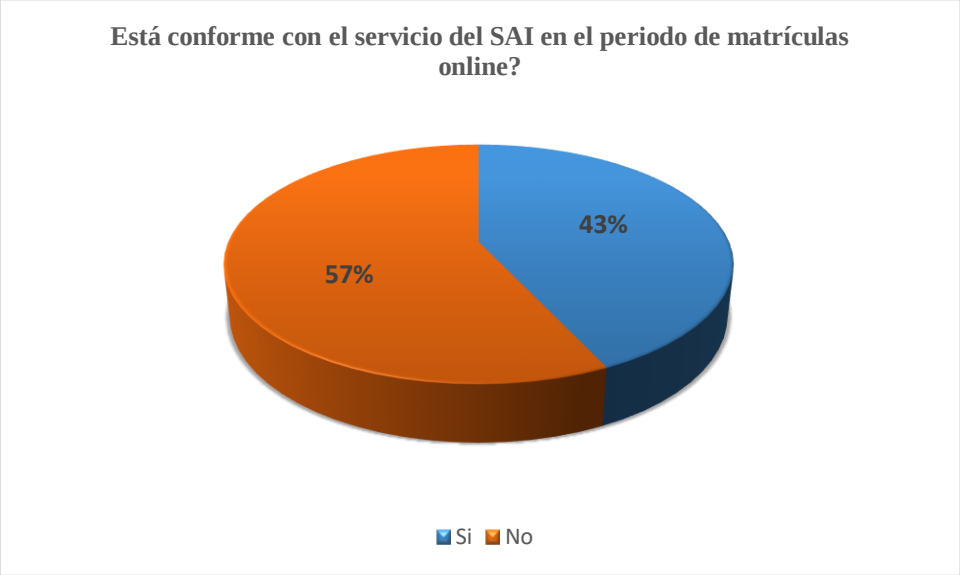


Ilustración 3, Elaborado por: (Daysi Morante, 2018).

Análisis e interpretación. El 57% de la población encuestada opinaron que no están conformes con el servicio que ofrece el sistema de control de calificaciones de la Universidad Técnica de Babahoyo en el periodo de matriculación en línea; mientras que el 43% de los encuestados si están de acuerdo con servicio prestado.

4. Sabe lo que es un FIREWALL?

Alternativa	Frecuencia	Porcentaje
Si	172	45%
No	212	55%
Total	384	100%

Tabla 4, Elaborado por: (Daysi Morante, 2018).

Ilustración 4, Elaborado por: (Daysi Morante, 2018).

Análisis e interpretación. El 55% de la población encuestada concluyo que no tienen conocimiento acerca de lo que es un FIREWALL; mientras que el 45% de los encuestados si saben lo que es un FIREWALL.

5. **Al momento de ingresar al SAI se le han presentado inconvenientes?**

Alternativa	Frecuencia	Porcentaje
Si	180	47%
No	204	53%
Total	384	100%

Tabla 5, Elaborado por: (Daysi Morante, 2018).

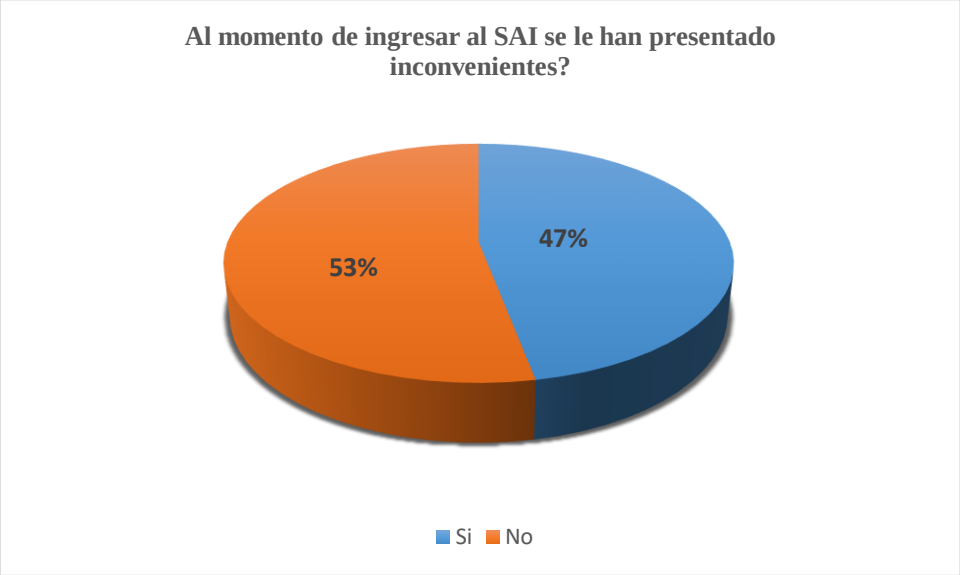


Ilustración 5, Elaborado por: (Daysi Morante, 2018).

Análisis e interpretación. El 53% de la población encuestada opino que si han tenido inconvenientes al momento de ingresar al sistema de control de calificaciones de la Universidad Técnica de Babahoyo; mientras que al 47% de los encuestados no se le han presentado inconvenientes.

6. Tiene conocimiento acerca de lo que es un estándar de seguridad?

Alternativa	Frecuencia	Porcentaje
Si	136	35%
No	248	65%
Total	384	100%

Tabla 6, Elaborado por: (Daysi Morante, 2018).

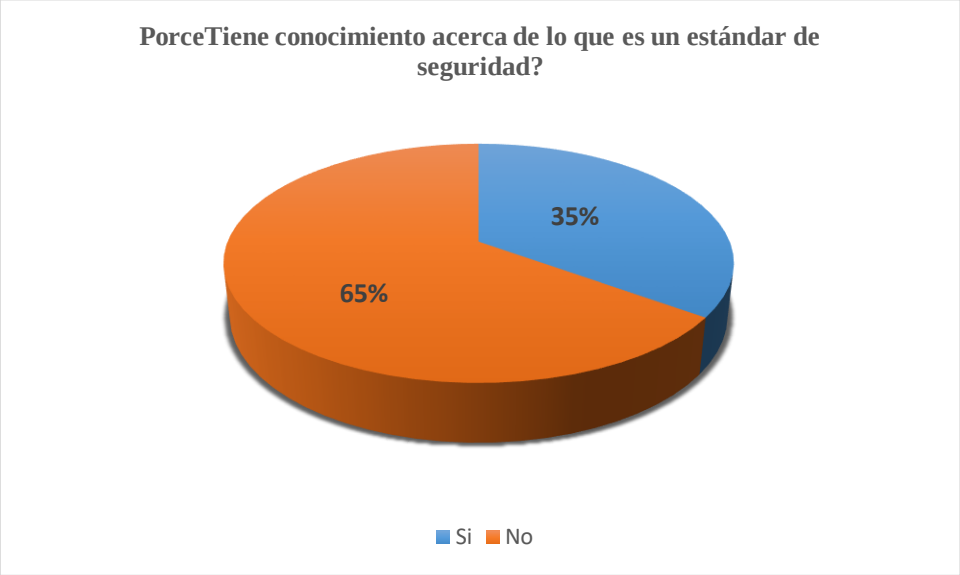


Ilustración 6, Elaborado por: (Daysi Morante, 2018).

Análisis e interpretación. El 65% de la población encuestada contesto que si tienen conocimientos acerca de lo que es un estándar de seguridad; mientras que el 35% de los encuestados no cuentan con dicho conocimiento.

7. **Considera que el inicio de sesión del sistema de control de calificaciones es seguro?**

Alternativa	Frecuencia	Porcentaje
Si	266	69%
No	118	31%
Total	384	100%

Tabla 7, Elaborado por: (Daysi Morante, 2018).

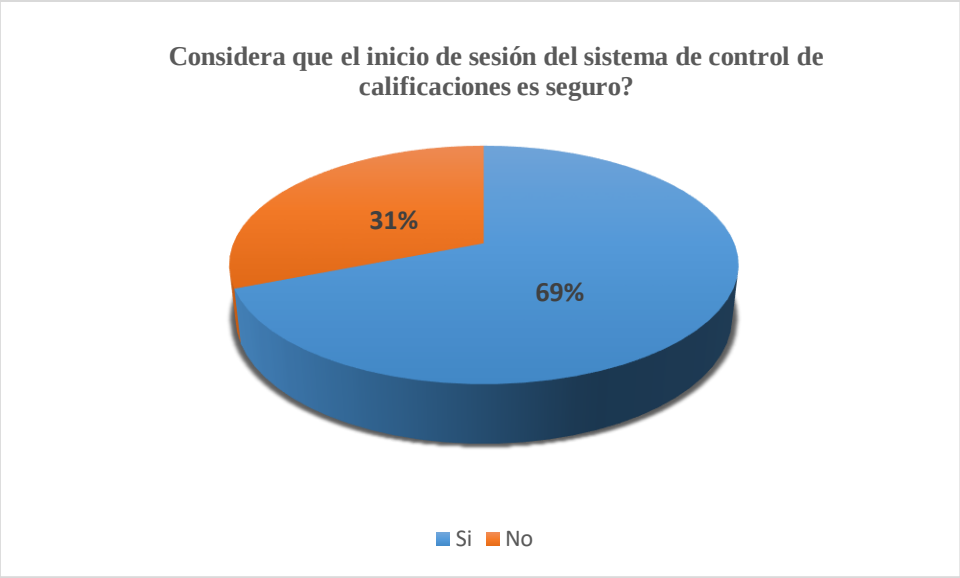


Ilustración 7, Elaborado por: (Daysi Morante, 2018).

Análisis e interpretación. El 69% de los encuestados si consideran seguro el inicio de sesión en el sistema de control de calificaciones de la Universidad Técnica de Babahoyo; mientras que el 31% de los encuestados consideran que no es seguro el inicio de sesión.

8. **Tiene conocimiento de los beneficios que proporcionan los estándares de seguridad informática?**

Alternativa	Frecuencia	Porcentaje
Si	64	17%
No	320	83%
Total	384	100%

Tabla 8, Elaborado por: (Daysi Morante, 2018).

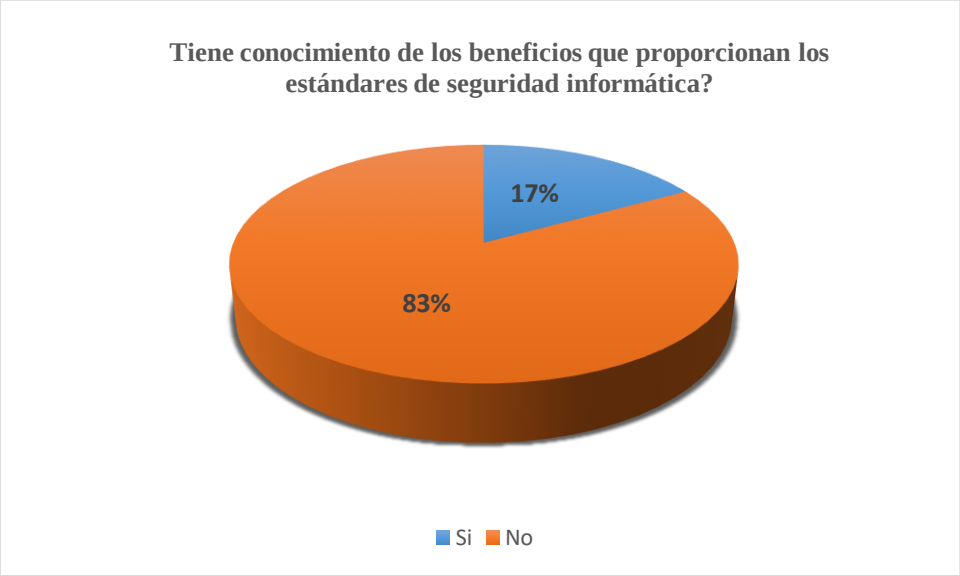


Ilustración 8, Elaborado por: (Daysi Morante, 2018).

Análisis e interpretación. El 83% de la población encuestada no tienen conocimientos acerca de los beneficios que pueden proporcionar los estándares de seguridad informática; mientras que el 17% de los encuestados si cuentan con dichos conocimientos.

9. **Cree que las autoridades de la Universidad Técnica de Babahoyo deberían reforzar** la seguridad informática de sus sistemas?

Alternativa	Frecuencia	Porcentaje
Si	336	87%
No	48	13%
Total	384	100%

Tabla 9, Elaborado por: (Daysi Morante, 2018).

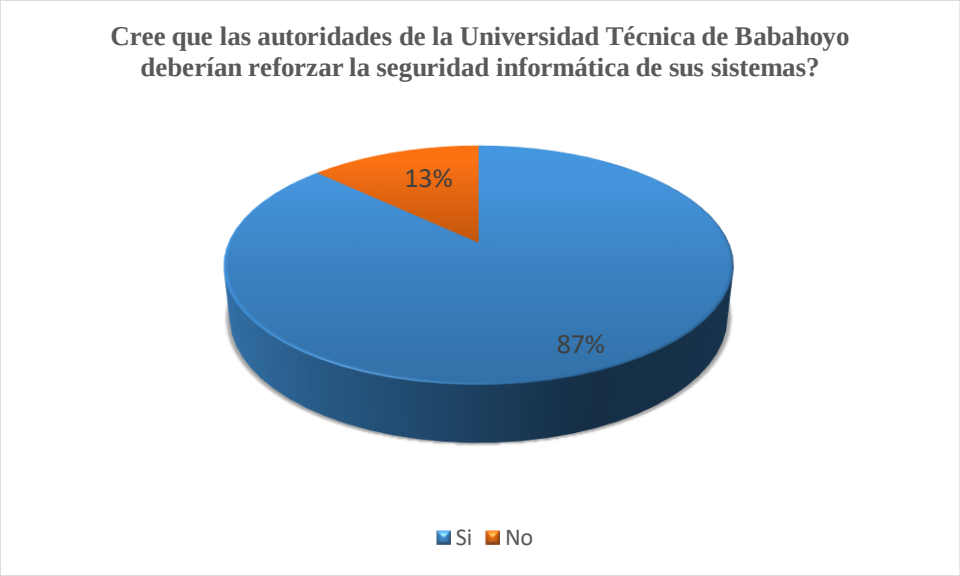


Ilustración 9, Elaborado por: (Daysi Morante, 2018).

Análisis e interpretación. El 87% de a población encuestada está de acuerdo que las autoridades de la Universidad Técnica de Babahoyo deberían reforzar la seguridad informática de sus sistemas; mientras que el 13% de los encuestados no están de acuerdo con dicha petición.

3.2. Conclusiones específicas y generales

3.2.1. Específicas.

Lamentablemente la mayoría de los alumnos encuestados de la Universidad Técnica de Babahoyo, no tienen conocimiento acera de lo que son los modelos de control informático y de lo que es un FIREWALL, por esta razón no saben los grandes beneficios que proporcionan los estándares de seguridad informática.

Por otra parte es considerable su inconformidad con el servicio que ofrece el sistema de control de calificaciones en los procesos de matriculación en línea, por los diferentes

inconvenientes que se presentan al momento de ingresar al sistema; además piensan que las máximas autoridades de la institución deben reforzar la seguridad de sus sistemas para proteger la información de los mismos.

3.2.2. General.

El uso de los modelos de control informático anima a toda la comunidad universitaria a investigar y aprender lo que es y cómo funcionan estos estándares, permitiendo de esta manera contar con una tecnología de alta calidad que permita la seguridad de la información.

3.3. Recomendaciones específicas y generales

3.3.1. Específicas.

Analizando los resultados obtenidos de la encuesta realizada se sugiere:

Al director del departamento de sistemas de Universidad Técnica de Babahoyo, que con base a sus conocimientos, incentive y dé a conocer a las máximas autoridades los grandes beneficios que se pueden adquirir al automatizar sus sistemas informáticos con estándares de seguridad, para salvaguardar la seguridad de la información.

Se recomienda crear una comisión de estudiantes y docentes de la escuela de sistemas de la Facultad de Administración, Finanzas e Informática, para que den a conocer en la misma facultad y en las demás facultades de la alma mater sobre lo que son los modelos de control informático y lo que es a seguridad de la información en cuanto al

sistema al que ellos tienen acceso, es por esta razón que no pueden estar ajenos a este tipo de información que es muy importante en sus carreras académicas.

3.3.2. General.

Se recomienda al rector de la Universidad Técnica de Babahoyo, como máxima autoridad la adquisición de normas de control informático, como ITIL y COBIT, que permitan la administración de servicios de buenas prácticas de las tecnologías de la información, para el mejor desempeño del sistema; y mediante estos estándares salvaguardar la seguridad de la información.

CAPÍTULO IV.- PROPUESTA DE APLICACIÓN.

4.1. Propuesta de aplicación de resultados.

4.1.1. Alternativa obtenida.

Estandarización de un modelo de control con componentes de ITIL y COBIT, para garantizar el buen funcionamiento del sistema de control de calificaciones de la Universidad Técnica de Babahoyo.

4.1.2. Alcance de la alternativa.

Nombre de la institución: Universidad Técnica de Babahoyo

Dirección de ubicación: Av. Universitaria Km 2 1/2 Av. Montalvo

Provincia: Los Ríos

Cantón: Babahoyo

Parroquia: Clemente Baquerizo

Sostenimiento y recursos: Fiscal

Región: Costa

La forma de acceso: Terrestre

4.1.3. Aspectos básicos de la alternativa.

4.1.3.1. Antecedentes.

Latinoamérica impulsa el uso de los modelos de control informático en la seguridad de la información y el control de activos; si bien es cierto existen herramientas y aplicaciones de seguridad informática, desarrollados por el sector académico y privado, los cuales permiten proteger los sistemas y equipos contra ataques maliciosos. A diferencia de las normas de control informático como ITIL y COBIT que proporcionan las mejores prácticas de ejecución, implementación, diseño y aplicación en la gestión de las TI.

Ecuador ocupa el sexto el lugar entre los países latinoamericanos, logrando un nivel intermedio sobre las medidas de seguridad informáticas implementadas; entre los acuerdos ministeriales establecidos, encontramos funciones como la elaboración de análisis y protocolos sobre la idoneidad técnica y profesional a cargo de las herramientas informáticas y tecnologías de la información.

4.1.3.2. Justificación

La intención de este proyecto investigativo, es alcanzar la atención de autoridades, personal administrativo, docentes y estudiantes de la Universidad Técnica de Babahoyo, sobre los usos y beneficios que proporcionan los modelos de control informático en la seguridad de la información, debido a que son estándares de alta calidad.

ITIL es un marco de trabajo con buenas practicas, que garantiza la seguridad de la información sobre los servicios de la Tecnologías de la Información permitiendo auditorias de manera práctica permitiendo la administración de los activos de la

institución, que incluyen varios procesos como la gestión de cambio, configuración, conocimiento e implementación.

COBIT al igual que ITIL es un estándar de buenas prácticas para la gestión y control de las Tecnologías de la Información, que permite la optimización de recursos disminuyendo riesgos cubriendo la empresa de extremo a extremo.

4.2.2. Objetivos.

4.2.2.1. General.

Estandarizar modelos de control informático con partes de ITIL y COBIT en el sistema de control de calificaciones de la Universidad Técnica de Babahoyo.

4.2.2.2. Específicos.

Analizar los tipos de modelos de control que existen para salvaguardar la seguridad de la información.

Definir el tipo de modelos de control informático que se deben emplear para el mejor funcionamiento del sistema de control de calificaciones de la Universidad Técnica de Babahoyo.

Gestionar la adquisición de normas de control informático con partes de ITIL y COBIT en el sistema de control de calificaciones de la Universidad Técnica de Babahoyo.

4.3.3. Estructura general de la propuesta.

4.3.3.1. Título.

Estandarización de un modelo de control con componentes de ITIL y COBIT, para garantizar el buen funcionamiento del sistema de control de calificaciones de la Universidad Técnica de Babahoyo.

4.3.3.2. Componentes.

4.3.3.2.1. Revisión y selección de estándares.

Todas las organizaciones a nivel mundial, como parte de sus políticas necesitan adquirir buenas prácticas para el mejor desempeño de sus sistemas, que permitan salvaguardar la seguridad de la información.

Las normas o estándares de control son actas donde está estipulado directrices y mandatos, para llevar a cabo su ejecución, las mismas que certifican su nivel de calidad y son elaboradas por expertos de la ISO.

El objetivo de los sistemas de gestión es determinar los objetivos propuestos; los estándares de control son creados y certificados por la ISO (International Standar Organization), especialmente para establecer reglamentos.

Entre los recursos de TI tenemos:

Aplicación.- es importante en los procesos de información de los usuarios automatizados.

Información.- incorpora las referencias de entrada y salida de los procedimientos de negocios.

Infraestructura.- incluye hardware, software, base de datos y usuarios.

Personas.- incorpora planes, logros, soporte y monitoreo en la evolución de los sistemas de información.

ISO 20000.

Es un estándar internacional elaborado para la administración de servicios delas TI, aplicados al area informática establecidos a las buenas prácticas de ITIL

ISO 27000.

La ISO 27000 es una norma que permite salvaguardar la seguridad de los activos de los sistemas de información, de esta norma se deriva otras normas referentes a la seguridad de la información.

ISO 27001.

Esta encargada de la administración de la seguridad, para organizar las contingencias para la implementación de sistemas de información.

ISO 27002.

Proporciona las mejores prácticas para los sistemas de información con la finalidad de establecer los objetivos de control.

ISO 27003.

Esta norma apoya a la activación de los sistemas de gestión d seguridad informática.

ISO 27004.

Esta norma detalla los reglamentos específicos para adquirir objetivos.

ISO 27005.
Esta norma permite la detección de amenazas.

ISO 27006.
Otorga las certificaciones de las organizaciones acreditadas.

ISO 27007.
Esta norma permite la audición de los objetivos de control junto con sus asignaciones.

ISO 38500.
Fija normas internacionales para las gerencias corporativas de las TIC.

ITIL.
ITIL es una biblioteca que contiene cinco libros basados en las mejores prácticas en un entorno de trabajo que define los términos sobre la administración de servicios de las organizaciones para la mejora constante de sus servicios.

ITIL comprende procesos los mismos que están conformados por normas que permiten adaptarse a las buenas prácticas de la gestión de servicios de las tecnologías de la información como la producción, preparación, aprobación y valoración.

Según el autor (Medina Cárdenas, Areniz Arévalo, & Rico Bautista, 2016), ITIL comprende estrategias de servicio como diseño, desarrollo y estrategias para la administración de servicios de TI.

El diseño de servicio es el encargado del modelo y desarrollo de los procedimientos de sus servicios, en los cuales podemos encontrar:

Figura 4

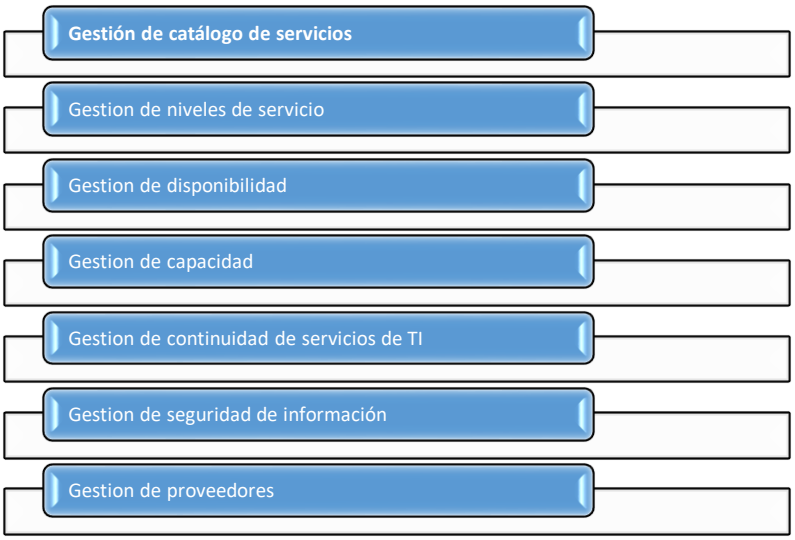


Ilustración 10, Elaborado por: (Daysi Morante, 2018).

La transición de servicios se encarga de gestionar y coordinar, los procedimientos, los sistemas y funciones para corroborar e implementar los servicios de operación. Entre sus procesos tenemos:

Figura 5

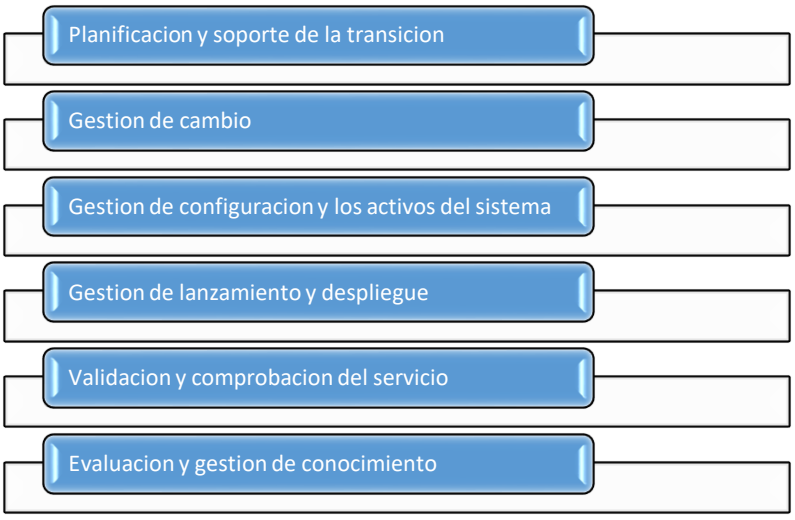


Ilustración 11, Elaborado por: (Daysi Morante, 2018

La operación de servicio es el encargado de coordinar las actividades y procedimientos indispensables para la administración de servicios aplicado a los usuarios y clientes de la organización, en el rango establecido. Entre sus procesos tenemos:

Figura 6

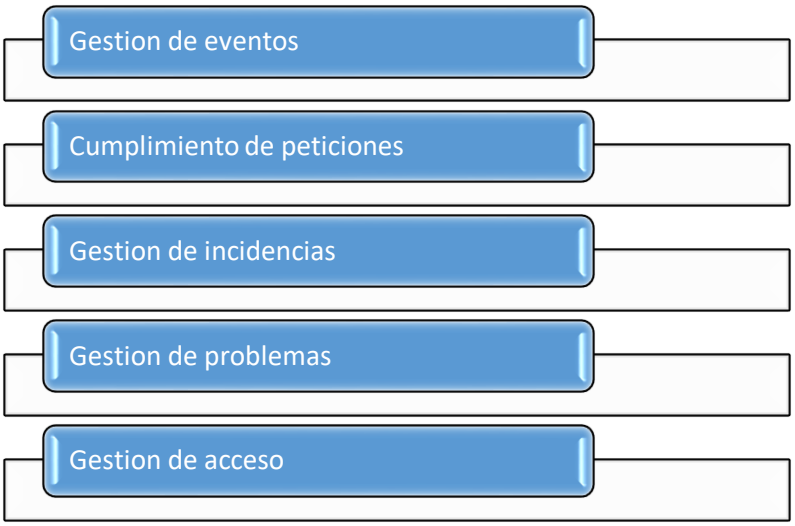


Ilustración 11, Elaborado por: (Daysi Morante, 2018).

La mejora continua es el encargado de mejorar los servicios de manera permanente que permita garantizar que dichos servicios correspondan a la mejora continua de los servicios y procesos del ciclo de vida.

Estrategias y Planeación.

Está encabezada por administradores del departamento quienes son los responsables de calcular y monitorear los elementos atribuidos a la dependencia, seguimiento y control de las estratégias de trabajo, gestión de riesgos, observancia de deberes y compromisos adquiridos, revisando reglamentos avalados por el equipo de calidad y buenas practicas ara el adecuado funcionamiento de los servicios.

Tecnologías y Sistemas de Información.

Esta dirigida por los administradores del departamento de Sistemas, quienes son los encargados de estimar, controlar y llevar a cabo los análisis de activación de procesos informáticos como la conectividad, internet los sistemas de información, etc.

Certificaciones de ITIL.

Se permite la certificación de ITIL para sujetos de diferentes rangos, los mismos que permiten descifrar la metodología e incrementar sus capacidades, hasta el año 2006 se habían emitido 500.000 certificaciones.

La informática evoluciona constantemente en cuanto a sus servicios desde la perspectiva de ITIL V3, manteniendo un equilibrio entre el servicio y el cliente; el cual permite mejorar y monitorear el coste de dichos servicios proporcionados.

Existen tres niveles de certificación ITIL para expertos en tecnologías de la información:

1. Fundation Certificate (Certificado Básico): autentifica los conocimientos básicos sobre ITIL, en la administración de servicios de TI.

2. Practitioner's Certificate (Certificado de Responsabilidad): está dirigido aquellos sujetos que tienen responsabilidades de procesos de proyectos de administración de las TI.

3. Manager's Certificate (Certificado de Director): declara que el sujeto que obtenga dicho certificado dispone de gran inteligencia en diferentes áreas de administración de los departamentos de las TI.

COBIT

Las normas COBIT son emitidas por ITGI (Instituto de Gobierno de las Tecnologías de la Información), que fue fundada por ISACA (Asociación de Información, Auditoría de Sistemas y Control.) la cual permite a las organizaciones de TI afianzar la entrega de productos y la reducción de riesgos, proporcionando las mejores prácticas de administración y rendimiento de las TI.

COBIT es un marco de referencia que permite la organización de la gestión de gobiernos de TI, con objetivos de control que proporcionan buenas prácticas, detallando los procedimientos, políticas y compromisos diseñados para brindar seguridad en la gestión de las TI.

COBIT está compuesto por procesos, actividades y 4 dominios que se juntan con el propósito de planificar, crear, realizar y controlar las tareas correspondientes a las TI.

Los dominios de COBIT comprenden:

- Planeamiento y organización
- Adquisición e implementación
- Entrega y soporte
- Monitoreo

Alineación Estratégica.

Salvaguarda el vínculo que existe entre la organización y las TI, manteniendo su calidad.

Mediante la entrega de valor se pueden obtener los valores garantizados; la administración de recursos de las TI, permite la gestión de aplicación, estructura y personas; mientras que la gestiona de administración de riesgos, propone discernir los riesgos a los que están expuestos las TI, mediante el cumplimiento, transparencia y responsabilidades; mediante la técnica de medición de desempeño se pueden obtener las estrategias de implementación y administración de recursos.

El primer dominio de COBIT es de planeamiento y organización, el cual comprende procedimientos de alto rendimiento, presentando 10 objetivos:

PO1.- detalla el plan estratégico de las TI.

PO2.- detalla la estructura de la información.

PO3.- puntualizar guía tecnológica.

PO4.- determinar los pasos de organización y relación de las TI.

PO5.- gestionar el financiamiento de las TI.

PO6.- anunciar la ambición y decretos de la gerencia.

PO7.- gestionar los recursos humanos de las TI.

PO8.- gestión de calidad.

PO9.- calcular la gestión de riesgos de TI.

PO10.- gestionar proyectos.

El segundo dominio está vinculado a estrategias de TI, permitiendo la identificación, desarrollo de las soluciones implementadas, contando con 7 objetivos de control:

AI1: reconocer las soluciones automatizadas.

AI2: lograr y mantener el software aplicativo.

AI3: lograr y mantener la estructura tecnológica.

AI4: proporcionar la ejecución y utilización.

AI5: lograr recursos de las TI.

AI6: gestionar cambios

AI7: establecer y autentificar resoluciones y cambios.

El tercer dominio esta designado a entrega y soporte en la administración y seguridad del servicio brindado a los usuarios; este dominio presenta 13 objetivos de control:

DS1.- define y gestiona el rango de calidad del servicio.

DS2.- gestionar funciones de terceras personas.

DS3.- administrar la ejecución y calidad del servicio.

DS4.- certificar la constancia del servicio.

DS5.- garantizar la seguridad del sistema.

DS6.- verificar y otorgar costos.

DS7.- instruir y capacitar a los usuarios.

DS8.- gestionar una reunión de funciones y eventualidades.

DS9.- gestionar la configuración del sistema.

DS10.- gestionar los problemas.

DS11.- gestionar datos.

DS12.- gestionar el ambiente laboral.

DS13.- gestionar acciones.

El cuarto dominio comprende monitoreo y evaluación, presenta 4 objetivos de control:

ME1.- controlar y estimar el desempeño de las TI.

ME2.- controlar y calcular el control interno.

ME3.- certificar el acatamiento de reglamentaciones.

ME4.- proveer de gobiernos de las TI.

COBIT es reconocido como un marco de referencia que se apoya en los controles de gestión de riesgos

4.3.3.2.2. Creación de políticas “Manual Guía”.

Existen guías metodológicas diseñadas para el buen funcionamiento de los estándares de control, los cuales son los encargados de brindar seguridad a los sistemas de información de las instituciones u organizaciones; los mismos que son proporcionados por las empresas proveedoras; dichos manuales pueden presentarse de forma física o digital las cuales permitirán una adecuada administración de los usuarios y claves del sistema.

La modificación de cuentas en el sistema, de estudiantes, docentes y personal administrativo, se podrá administrar de manera personal, siendo dicha modificación monitoreada por el departamento de sistemas de la Universidad Técnica de Babahoyo para corroborar que el usuario que este ingresando al sistema sea el correcto.

Se establecerá políticas y procedimientos para el correcto uso y funcionamiento del sistema de control de calificaciones de la Universidad Técnica de Babahoyo.

El almacenamiento de datos en la nube, es tendencia hoy en día, por ello se debe utilizar servidores externos para poder acceder a los datos desde cualquier lugar que el usuario desee acceder.

4.3.3.2.3. Gestión de aprobación de políticas para su aplicación.

La gestión para la aprobación de las políticas y su aplicación en el Sistema de Control de Calificaciones de la UTB, se organizó de la siguiente manera:

El departamento de sistemas de la Universidad Técnica de Babahoyo se reúne y socializa con las máximas autoridades del alma mater sobre los grandes beneficios que aporta

el obtener estándares de seguridad con componentes de ITIL y COBIT con las mejores prácticas para la seguridad de la información.

La máxima autoridad, representada por el rector que aprueba la creación de políticas y aplicación de las normas de seguridad para salvaguardar la información emitida en los sistemas.

El rector propone y dispone socializar el tema sobre las normas de control informático con el personal administrativo, docentes y estudiantes del alma mater, para dar a conocer el tipo de estándares de seguridad que se desean aplicar en el sistema de control de calificaciones de la UTB, para mantener a salvo la seguridad de la información y mejorar su desempeño.

4.4. Resultados esperados de la alternativa.

Adoptar estándares de seguridad con partes de ITIL y COBIT incidirá positivamente en el sistema de control de calificaciones de la Universidad Técnica de Babahoyo, salvaguardando la seguridad de la información de dicho sistema, al mismo tiempo desarrollando las capacidades intelectuales tanto de alumnos, docente y personal administrativo que estarán inmersos en dichas modificaciones del sistema.

Una vez aplicados los estándares de seguridad en el sistema de control de calificaciones de la Universidad Técnica de Babahoyo, se podrá acceder a dicho sistema de manera rápida y sencilla, sin ningún tipo de molestias que puedan provocar de contratiempos.

Con la obtención de las normas de control informático la Universidad Técnica de Babahoyo, se nivelara con instituciones académicas de alto prestigio en cuanto a la seguridad y salvaguarda de sus sistemas de información, dando a conocer de esta manera

de que todas las instituciones públicas o privadas tienen el derecho de actualizar constantemente sus sistemas.

Los beneficios proporcionados por los estándares de seguridad permiten fomentar el estudio de tecnologías avanzadas y poderlas aplicar a nuevos sistemas, evitando posibles riesgos durante su ejecución.

Bibliografía.

Referencias

Baca Urbina, G. (2016). *Introduccion a la Seguridad Informatica.* México: Grupo Editorial Patria.

BAUD, J.-L. (2015). Preparacion para la certificacion ITIL Foundation V3 ITIL V3-2011. En J.-L. BAUD, *Preparacion para la certificacion ITIL Foundation V3 ITIL V3-2011.* Barcelona, España: Ediciones ENI. Obtenido de https://books.google.com.ec/books?id=vOEGFtNoUjcC&pg=PA308&dq=itil+2014&hl=es-419&sa=X&ved=0ahUKEwjgvrWerc_gAhVrm-AKHeiDBgIQ6AEILjAB#v=onepage&q=itil%202014&f=true

Baud, J.-L. (2017). *ITIL V3 PREPARACIóN A LA CERTIFICACIÓN ITIL FOUNDATION, Volumen 3.* Barcelona: Eni Ediciones.

Cantabria, E. U. (2015). Gobernanza empresarial de tecnologias de la informacion. En E. U. Cantabria, *Gobernanza empresarial de tecnologias de la informacion.* España: Editorial Universidad Cantabria.

Chicano Tejada, E. (2014). *Auditoria de seguridad informatica.* Málaga: ic editorial.

Coral Calero, Moraga, M., & Piattini, M. (2010). *Calidad del producto y proceso software.* Madrid: RA-MA Editorial.

Diaz Orueta, G., Alzórriz Armendáriz, I., Sancristóbal Ruiz, E., & Castro Gil, M. (2014). Procesos y herramientas para la seguridad de redes. En G. Diaz Orueta, I. Alzórriz

Armendáriz, E. Sancristóbal Ruiz, & M. A. Castro Gil, *Procesos y herramientas para la seguridad de redes.* Madrid: Edicion digital.

EGSI. (2013). *Esquema Gubernamental de Seguridad de la Informacion.* Quito.

ESTADO, C. G. (16 de diciembre de 2014). *NORMAS DE CONTROL INTERNO DE LA CONTRALORIA*. Obtenido de https://www.oas.org/juridico/pdfs/mesicic5_ecu_ane_cge_12_nor_con_int_400_cge.pdf

Estrategica, S. C. (2014). *Seguridad de la Información.* Guatemala.

Fonseca Luna, O. (2011). *Sistemas de Control Interno para organizaciones.* Lima: Publicidad & Matiz.

Fonseca Luna, O. (2013). *Sistema de Control Interno para Organizaciones.* Lima Peru: Publicidad & Matiz.

Galán Chuquimarca, L., & Brussil Velásquez, C. (2015). Guia Metodologica para Proyectos de TI basados en el marco de trabajo PMBOK desde la perspectiva de la gestion de servicio de ITIL, y su seguimiento a traves de las métricas de COBIT para empresas de Tecnologías de la Información. *Maestria en Gerencia de Tecnologías de la Información.* Pontificia Universidad Catolica del Ecuador, Quito.

Medina Cárdenas, Y., Areniz Arévalo, Y., & Rico Bautista, D. (2016). *MODELO ESTRATEGICO PARA LA GESTION: PLAN TACTICO DE LA CALIDAD (ITIL & ISO 20000).* MEDELLIN: FONDO EDITORIAL ITM.

Mejia Viteri, G. V. (2016). Análisis y Evaluación del Riesgo de la Información. *UNIANDES EPISTEME: Revista de Ciencia, Tecnología e Innovación*.

Muñoz Razo, C. (2002). *Auditoria en Sistemas Computacionales.* Mexico: Pearson Educacion.

Nakasone, G. (2012). *Confidencialidad del correo electrónico, Diseño de un esquema de seguridad basado en DNSSEC.* Buenos Aires.

Preparacion para la certificacion ITIL Foundation V3. (s.f.).

Soto Acosta, V. E., & Valdivieso Jácome, F. S. (2014). Diseño e implementacion de un modelo de gestion de Srevice Desk basado en ITIL V3 para PDVSA Ecuador. *Maestria en Evaluacion y Auditoria de Sistemas Tecnologicos III Promocion.* Universidad de las Fuerzas Armadas, Quito.

Vega Villacis, R. M. (2017). *VULNERABILIDADES Y AMENAZAS A LOS SERVICIOS WEB DE LA INTRANET DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO.* Babahoyo.

WordPress.com. (24 de mayo de 2015). *ITI III ESTRATEGIAS DE GESTION DE SERVICIOS DE TI*. Obtenido de ITI III ESTRATEGIAS DE GESTION DE SERVICIOS DE TI: https://aquinodul.wordpress.com/2015/05/24/cobit/

Anexos

ENCUESTA SOBRE EL USO DE LOS MODELOS DE CONTROL INFORMATICO Y SU INCIDENCIA EN LA SEGURIDAD DE LA INFORMACION

Objetivo: Definir las incidencias en el uso de los modelos de control informático.

Dirigido a: varios grupos de estudiantes de la Universidad Técnica de Babahoyo.

Por favor lea con atención las preguntas y responda de acuerdo a su criterio sincero con un visto en la respuesta que considere valida.

Encuestador – Daysi Morante Mosquera

1. Conoce si la UTB utiliza seguridad informática en sus sistemas?

Si ( ) No ( )

2. Tiene conocimiento acerca de lo que es un modelo de control informático?

Si ( ) No ( )

3. Está conforme con el servicio del SAI en el periodo de matrículas online?

Si ( ) No ( )

4. Sabe lo que es un FIREWALL?

Si ( ) No ( )

5. Al momento de ingresar al SAI se le han presentado inconvenientes?

Si ( ) No ( )

6. Tiene conocimiento acerca de lo que es un estándar de seguridad?

Si ( ) No ( )

7. Considera que el inicio de sesión del SAI es seguro?

Si ( ) No ( )

8. Tiene conocimiento de los beneficios que proporcionan los estándares de seguridad informática?

Si ( ) No ( )

9. Cree que las autoridades de la UTB deberían reforzar la seguridad informática de sus sistemas?

Si ( ) No ( )