VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA.

CENTRO DE POSGRADOS

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS.

V Y VIII PROMOCIÓN

TEMA: "EVALUACIÓN TÉCNICA INFORMÁTICA DE LA ENTREGA, SERVICIO Y SOPORTE DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE SEDE MATRIZ"

AUTORES: BECERRA AUZ FERNANDA JACKELINE.

LEÓN CAISA HENRY ROBERTO.

DIRECTOR: RON EGAS MARIO BERNABÉ.

SANGOLQUÍ

2016

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA TECNOLÓGICA.

CENTRO DE POSGRADOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, "***EVALUACIÓN TÉCNICA INFORMÁTICA DE LA ENTREGA, SERVICIO Y SOPORTE DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE SEDE MATRIZ***" realizado por la señorita ***FERNANDA JACKELINE BECERRA AUZ*** y el señor ***HENRY ROBERTO LEÓN CAISA*** ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo que cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar a la señorita ***FERNANDA JACKELINE BECERRA AUZ*** y al señor ***HENRY ROBERTO LEÓN CAISA*** para que lo sustenten públicamente.

Quito, 14 de mayo de 2015

Ing. Mario Bernabé Ron Egas

DIRECTOR DE TESIS

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA TECNOLÓGICA.

CENTRO DE POSGRADOS

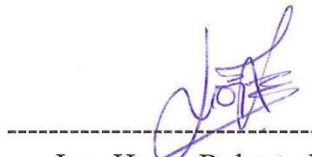
AUTORÍA DE RESPONSABILIDAD

Yo, ***FERNANDA JACKELINE BECERRA AUZ***, con cédula de ciudadanía N° 0401288139 y ***HENRY ROBERTO LEÓN CAISA,*** con cédula de ciudadanía N° 1712399151, declaramos que este trabajo de titulación "***EVALUACIÓN TÉCNICA INFORMÁTICA DE LA ENTREGA, SERVICIO Y SOPORTE DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE SEDE MATRIZ***" ha sido desarrollado considerando los métodos de investigación existentes, así como también se han respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaramos que este trabajo es de nuestra autoría, en virtud de ello nos declaramos responsables del contenido, veracidad y alcance de la investigación mencionada.

Quito, 14 de mayo de 2015

Ing. Fernanda Jackeline Becerra Auz
C.C 0401288139



Ing. Henry Roberto León Caisa
C.C 1712399151

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA TECNOLÓGICA.

CENTRO DE POSGRADOS

AUTORIZACIÓN

Yo, ***FERNANDA JACKELINE BECERRA AUZ*** y ***HENRY ROBERTO LEÓN CAISA***, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar en la Biblioteca Virtual de la institución el presente trabajo de titulación "***EVALUACIÓN TÉCNICA INFORMÁTICA DE LA ENTREGA, SERVICIO Y SOPORTE DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE SEDE MATRIZ***" cuyo contenido, ideas y criterios son de nuestra autoría y responsabilidad.

Quito, 14 de mayo de 2015

Ing. Fernanda Jackeline Becerra Auz
C.C 0401288139

Ing. Henry Roberto León Caisa
C.C 1712399151

DEDICATORIA

Este trabajo está dedicado con mucho cariño a nuestras familias, por ser la fuente de inspiración y motivación para seguirnos desarrollando como excelentes profesionales; por estar junto a nosotros apoyándonos y alentándonos cuando más los necesitamos.

A todas las personas que de una u otra forma fueron parte de esto sueño hecho realidad, y que siempre creyeron en nosotros.

AGRADECIMIENTOS

Agradecemos a Dios por ser el gestor de nuestra existencia y por ser la fuente de optimismo, perseverancia y sabiduría que nos impulsa día a día a seguir por el sendero justo en la búsqueda de nuestros sueños e ideales.

Un agradecimiento y a la vez un reconocimiento especial al Ing. Mario Ron Egas, Director del Proyecto, por su apoyo incondicional, su valioso aporte profesional en toda la elaboración del presente trabajo, su preocupación y desinteresada colaboración.

Así mismo es necesario extender el sentimiento de gratitud a los Maestros del Programa de Maestría en Evaluación y Auditoría de Sistemas tecnológicos por los conocimientos impartidos dentro del aula de clase, ya que en base a ellos nos hemos orientado para el desarrollo del presente trabajo.

Ing. Fernanda Jackeline Becerra Auz.

Ing. Henry Roberto León Caisa.

INDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

En los últimos años el desarrollo tecnológico ha sido eminentemente enorme y a la vez el número de procesos y controles ha aumentado, de modo que el área o la unidad responsable como por ejemplo TICS, de las Instituciones públicas o privadas deben tomar medidas que aseguren la calidad del servicio y la entrega oportuna del mismo a los usuarios. Por ello el objetivo principal del presente proyecto es el de realizar la Evaluación Técnica Informática de la Entrega, Servicio y Soporte de la Universidad de las Fuerzas Armadas ESPE Sede Matriz utilizando la metodología COBIT 5 establecido por ISACA, la cual permitirá identificar el estado actual de la Unidad de Tecnologías de Información y Comunicación (UTIC), evaluar los procesos que actualmente lleva y posteriormente recomendar las posibles mejoras. Cabe destacar que COBIT 5 brinda un marco integral que ayuda a lograr las metas de la organización y entregar valor a través de un gobierno y una administración efectiva; pues se ajusta de forma holística a la organización incluyendo a todos los niveles y áreas de responsabilidad funcionales. De tal manera que servirá como base para que las partes interesadas internas y externas de la Institución acojan a TI como parte esencial de la organización. Esta metodología cuenta con 5 procesos habilitadores, pero el presente trabajo se enfocará en la Entrega, Servicio y Soporte que involucra la Administración de las operaciones, administrar las solicitudes de servicios e incidentes, administrar problemas, la continuidad, los servicios de seguridad y los controles en los procesos de negocio.

PALABRAS CLAVE:
EVALUACIÓN UTIC
ISACA
COBIT 5
ENTREGA, SERVICIO Y SOPORTE (ESS)
MAPEO OBJETIVOS TI Y OBJETIVOS COBIT 5

ABSTRACT

In recent years technological development has been eminently huge and growing number of processes and controls has increased, so that the area or the responsible unit such as ICT, public or private institutions must take measures to ensure the quality service and timely delivery of the same to users. Therefore, the main objective of this project is to make the Technical Evaluation Informatics Delivery, Service and Support University of the armed forces headquarters ESPE matrix using COBIT 5 methodology established by ISACA, which will identify the current state of Unit Information and Communication Technologies (UTIC), evaluate processes currently carried and then recommend possible improvements. Note that COBIT 5 provides a comprehensive framework to help achieve the goals of the organization and deliver value through a government and an effective administration; because it fits holistically including the organization at all levels and areas of functional responsibility. So that will serve as a basis for internal and external stakeholders of the institution making use of IT as an essential part of the organization. This methodology has 5 enabling processes, but this work will focus on the delivery, service and support that involves the administration of the operations, manage service requests and incidents, manage problems, continuity, security services and controls in business processes.

KEYWORDS:
EVALUATION UTIC
ISACA
COBIT 5
DELIVER, SERVICE AND SUPPORT (DSS)
MAPPING IT OBJECTIVES AND COBIT 5 OBJECTIVES

CAPÍTULO I

1 Introducción

1.1 Antecedentes

Desde hace algunos años, la Universidad de las Fuerzas Armadas ESPE, ha venido ejecutando varios proyectos en el área informática, con el objeto de apoyar a las diferentes actividades que desarrolla la Universidad.

Se han implementado algunos servicios informáticos y otros se encuentran en desarrollo, para lo que se han adquirido equipos, instalado redes y contratado servicios adicionales.

La Universidad de las Fuerzas Armadas ESPE, como una Institución Educativa de Prestigio que brinda servicios académicos de alta calidad, cuenta con una Unidad de Tecnología de Información y Comunicación (UTIC) que centraliza la administración y gestión de las actividades de TI, es decir se encarga del análisis, desarrollo e implantación de los sistemas requeridos en la ESPE y se preocupa por el adecuado funcionamiento de las aplicaciones existentes, redes y comunicaciones.

La ESPE se encuentra en un proceso de cambio institucional, en el que se ha adoptado un nuevo modelo educativo, a la par de una estructura organizacional diferente, con procesos acondicionados a esta nueva estructura.

Por lo expuesto se ha elaborado y aprobado formalmente el Proyecto para realizar la Evaluación Técnica Informática de la Universidad de las Fuerzas Armadas, con la finalidad de asegurar que los objetivos de Gobierno de TI, se hayan cumplido en la Institución. Para este proyecto se utilizará como marco de referencia COBIT V5 y las normas relacionadas que sean necesarias.

1.2 Planteamiento del Problema

La Universidad de las Fuerzas Armadas ESPE en vista del constante desarrollo, evolución, avance tecnológico y tomando como referencia que el objetivo principal de

esta Institución Educativa es mantenerse entre las mejores universidades del País, ha visto la necesidad de estar a la vanguardia en cuanto a la parte tecnológica se refiere, por ello ha adquirido equipo informático, el cual ha sido implementado en su debido tiempo. Sin embargo, se requiere controlar y verificar su funcionamiento óptimo. Por lo tanto a través de este proyecto se determinará el estado actual de los mismos.

1.3 Formulación del problema

- ¿La Universidad de las Fuerzas Armadas ESPE, a través de la Evaluación Técnica Informática podrá mejorar los procesos de Entrega, Servicio y Soporte a sus múltiples dependencias?
- ¿El aplicar COBIT como marco de referencia, permite certificar que el análisis llevado a cabo es correcto?
- ¿La metodología utilizada en el presente estudio, puede ser enfocada a otras áreas?

1.4 Justificación del Problema

En la actualidad en las empresas, instituciones públicas o privadas al momento de adquirir o contratar un bien o servicio, debe tomar en cuenta algo muy importante "La Entrega, Soporte y Servicio", el cual debe estar enmarcado bajo parámetros de buenas prácticas o modelos de referencia, como COBIT 5 (Control Objectives for Information and Related Technology), mismo que puede servir como referencia o guía para la Gestión de TI. (ISACA, 2014, p. 1).

1.5 Objetivo General

Realizar una Evaluación Técnica Informática de la Entrega, Servicio y Soporte de la Universidad de las Fuerzas Armadas ESPE Sede Matriz, aplicando como marco de referencia COBIT 5.

1.6 Objetivos Específicos

- Elaborar la Planificación detallada del proyecto.
- Elaborar el Plan de investigación de campo en base al análisis y alineación de los Objetivos Estratégicos de la ESPE y COBIT 5.

- Elaborar y aplicar los instrumentos de investigación de campo.
- Realizar el análisis de la información.
- Redactar los informes.
- Presentar los informes y acoger los puntos de vista.

CAPÍTULO II

2 Marco teórico y estado del arte.

2.1 Antecedentes

2.1.1 COBIT

COBIT (**Control Objectives for Information and Related Technology**) que significa Objetivos de Control para la Información y Tecnologías Relacionadas, es un marco de mejores prácticas aceptado internacionalmente para el control de la información y publicado por ISACA (*Information Systems Audit and Control Association*) y el IT GI (IT Governance Institute), que contiene un conjunto de recursos para la gestión de TI, incluyendo medidas de desempeño, directivas de aseguramiento, factores críticos, modelos de madurez, etc.

A lo largo del tiempo COBIT presentó muchas versiones, siendo publicada la primera versión en 1996, la segunda edición en 1998, la tercera en 2000, la cuarta edición en diciembre de 2005; en el 2007 lanzó la versión 4.1 y posteriormente en abril del 2012 aparece la última edición llamada COBIT 5, proporcionando una visión empresarial del Gobierno de TI que tiene a la tecnología y a la información como protagonistas en la creación de valor para las empresas. (ISACA, COBIT 5 Introducción - Presentación de Power Point - Isaca, 2012)

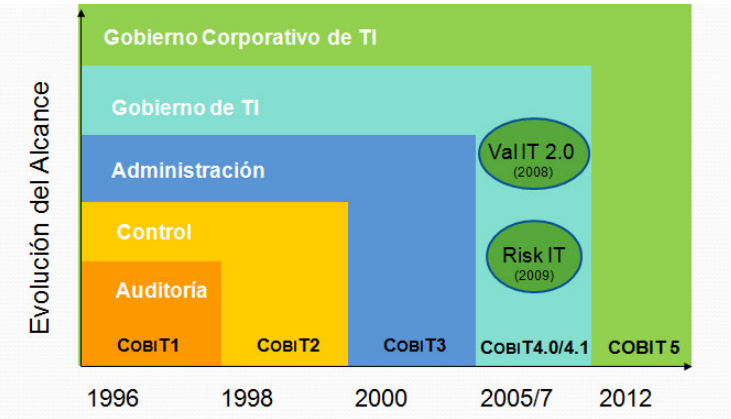


Figura 1. Versiones de COBIT

Fuente: (ISACA, 2012)

2.1.1.1 COBIT 5.

COBIT 5 es el único marco de negocio para el gobierno y la gestión de las TI corporativas. Es el producto de un grupo de trabajo global y equipo de desarrollo de ISACA, una asociación sin fines de lucro, independiente de profesionales de casi 100.000 de gobierno, seguridad, riesgo y de garantía en 160 países.

COBIT 5 incorpora las ideas más recientes en las técnicas de gobierno y gestión de la empresa, y proporciona principios globalmente aceptados, prácticas, herramientas analíticas y modelos para ayudar a aumentar la confianza y el valor de los sistemas de información. (Otalora Chisco, 2014)

COBIT 5 construye y expande en COBIT 4.1 mediante la integración de otros marcos importantes, normas y recursos, incluyendo Val de ISACA TI y Risk IT, Tecnología de la Información Biblioteca de Infraestructura (ITIL®) y las normas relacionadas de la Organización Internacional de Normalización (ISO).

Los principios en los que COBIT 5 se fundamenta son:

Figura 2. Principios de COBIT 5

Fuente: (ISACA COBIT 5, 2012)

1. Satisfacer las necesidades de los interesados: implica el aspecto fundamental que es el de crear valor, con lo cual el gobierno es responsable de decidir los diferentes intereses a través de estrategias, para ello COBIT 5 establece las metas en cascada.
2. Cubrir la organización de forma integral: se enlaza el denominado gobierno TI y el gobierno corporativo para cubrir las funciones de la organización, alineados con los procesos.
3. Aplicar un solo maco integrado: que quiere decir que COBIT 5 se integra sin ningún problema con otros marcos de trabajo como COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 38500, ITIL, etc.
4. Habilitar un enfoque holístico: son 7 elementos que trabajan para el correcto funcionamiento de TI corporativo junto al Gobierno y Administración de manera sencilla, proporcionando una estructura.

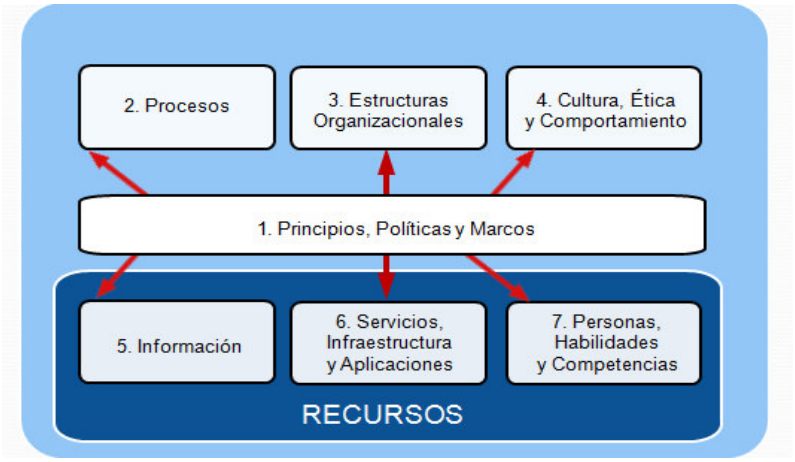


Figura 3. Principios, Políticas y Marcos

Fuente: (ISACA COBIT 5, 2012)

5. Separar el Gobierno de la Gestión: En COBIT 5 se observa una clara demarcación entre lo que es Gobierno y Gestión de acuerdo a una evolución de versiones anteriores y las prácticas que actualmente se aplican, de tal manera que el Gobierno está bajo el ciclo EDM (Evaluar, Dirigir y Supervisar) que permite asegurar que los objetivos de la empresa sean logrados y la responsabilidad es de la Junta Directiva; mientras que la administración o gestión se establece bajo el ciclo PBRM (Planear, Construir, Ejecutar, Supervisar), actividades que mantienen alineamiento con el gobierno y con otros marcos de referencia con la responsabilidad de la alta administración y a la cabeza está el CEO. (ISACA, COBIT 5 Introduction Spanish, 2012)

2.2 Análisis de las diferencias entre COBIT 4.1 y COBIT 5

En primera instancia se mencionan los cambios a nivel general que COBIT 5 presenta a diferencia de COBIT 4.1:

- Nuevos principios de Gobierno de TI.

- Mayor foco en Habilitadores.
- Nuevo modelo de referencia de procesos.
- Procesos nuevos y modificados.
- Prácticas y actividades.
- Objetivos y Métricas más desarrolladas.
- Entradas y Salidas a nivel de práctica.
- Cuadros RACI más desarrollados.
- Modelos de madurez de capacidad de procesos y evaluaciones.

Cabe indicar que COBIT 5 integra tanto a COBIT 4.1 como tal, Val IT 2.0 y Risk IT para conformar un modelo de referencia de procesos y con esta evolución se destacan 37 procesos de gobierno y de gestión que a su vez tienen diferentes actividades, por tanto dichas prácticas son similares a los objetivos que ofrece COBIT 4.1. En tanto que en su cuarta edición, COBIT tiene 34 procesos que cubren 210 objetivos de control (específicos o detallados) clasificados en cuatro dominios:

1. Planificación y Organización (*Plan and Organize))*
2. Adquisición e Implantación (*Acquire and Implement*)
3. Entrega y Soporte (*Deliver and Support*)
4. Supervisión y Evaluación (*Monitor and Evaluate*)

Las actividades de COBIT 5 se relacionan en cuanto a lo que COBIT 4.1, Val IT y Risk IT ofrecen respecto a prácticas de control y administración.

En lo relacionado a las metas del negocio y las metas de TI, COBIT 5 analiza más detenidamente dichos aspectos clasificándolos en primarios y secundarios a diferencia de COBIT 4.1, tomando en cuenta que la cantidad de metas de negocio se mantienen con un número de 17 pero con cambios en los contenidos en base a lo que enuncia el Balanced Scord Card. Pero en el caso de las metas de TI, COBIT 5 se queda con 17 metas de un total de 28 tomando perspectivas de acuerdo a índices de aprendizaje, financiero, cliente e interna.

Es evidente el cambio, cuando se elimina la figura del "pentágono" que identificaba a COBIT 4.1 al mencionar el Gobierno de TI, pues en la nueva versión reemplaza por el ciclo denominado EDM. Así mismo el "cubo" donde se representaban los 7 criterios

de la información tales como: efectividad, eficiencia, integridad, confiabilidad, disponibilidad, confidencialidad y cumplimiento donde para COBIT 5 se establecen términos como: utilidad, usabilidad, libre de error, credibilidad, accesibilidad, seguridad y conformidad.

La nueva perspectiva de evaluación de la capacidad del proceso o el llamado "Modelo de Madurez" en COBIT 5 estará apoyado por la ISO/IEC 15504 que engloba lo concerniente a la determinación de la capacidad de mejora del proceso de software, tanto en sistemas de información como en productos de software; dicho estándar es más riguroso para pasar de nivel, pues se debe cumplir lo que está dispuesto en cada proceso. Es así que se desplaza el antiguo modelo de COBIT 4.1 ya que no es posible obtener en sus evaluaciones resultados similares.

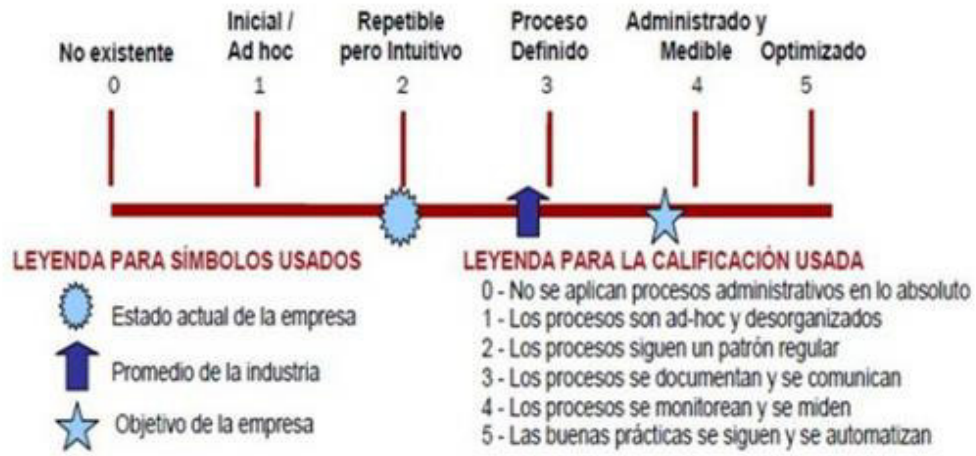


Figura 4. Modelo de Madurez COBIT 4.1

Fuente: (ISACA COBIT 5, 2012)

Figura 5. Modelo de Madurez COBIT 5

Fuente: (ISACA COBIT 5, 2012)

2.3 Administración de riesgos

La Administración del Riesgo Empresarial (Enterprise Risk Management-ERM) es el proceso por el cual la dirección de una empresa u organización administra el amplio espectro de los riesgos a los cuales está expuesto ya sean de mercado u operacionales.

En el área de Tecnologías de información (TI) este tema se relaciona con la evaluación de riesgos y vulnerabilidades, tomando en cuenta los activos de TI físicos y lógicos, además se puede incluir una revisión de las instalaciones y la seguridad de los mismos. Siendo uno de los retos analizar numerosos datos (de acuerdo al rango de riesgos definido), con lo cual se podrá contar con más información dinámica y compleja, pero al mismo tiempo seguir manteniendo los costos de implementación, los riesgos bajo control y las técnicas de mitigación apropiadas.

Actualmente las empresas enfrentan un aumento en la exposición a riesgos en relación a la demanda del continuo funcionamiento de los sistemas de información, puesto que la tecnología informática claramente sostiene cada proceso comercial de la empresa.

Los riesgos informáticos típicos incluyen pérdida de productividad o negocios debido al tiempo de inactividad, responsabilidad por brechas de seguridad que exponen

la información de los clientes, multas por violaciones de normas y la imposibilidad de defenderse de demandas debido a la conservación inadecuada de registros. (KIT, 2015)

2.3.1 Soluciones

Por ello, es preciso combinar un conjunto de las mejores prácticas que se desprenden de numerosas organizaciones, grandes y complejas, para enfrentar los riesgos informáticos de sus entornos mediante la priorización y planificación de opciones de mitigación, calcular los impactos de los riesgos informáticos, diseñar soluciones, alinear los riesgos informáticos y los costos con la empresa para optimizar las inversiones y construir una capacidad unificada para administrar los riesgos informáticos de manera continua. (KIT, 2015)

2.3.2 Problemas que se identifican

- Identificar eventos o amenazas que podrían tener impacto en la continuidad de las operaciones empresariales, en la imagen o en la reputación de la marca, y la probabilidad de que ocurran.
- Realizar un análisis detallado de amenazas o establecer planes de avance para mitigar riesgos.
- Determinar cómo las nuevas iniciativas empresariales o la nueva tecnología tendrán impacto en la empresa.
- Establecer planes de avance para mitigar riesgos.
- Identificar las exposiciones con respecto al cumplimiento reglamentario. (KIT, 2015)

2.4 Auditoría Informática

La auditoría informática es aquel proceso que tiene por objeto realizar un examen crítico, objetivo, sistemático y selectivo que evalúa la eficacia y eficiencia de los recursos informáticos, si a su vez éstos mantienen la integridad de los datos, salvaguardan los activos de la empresa, cumplen las leyes y regulaciones establecidas;

identificando además qué información es crítica y por ende si está alineada con los objetivos y las metas del negocio, en base a la recolección de evidencias y su respectivo análisis.

La auditoría informática mejora el desempeño de la empresa en cuanto a: fiabilidad, seguridad, eficacia, rentabilidad y privacidad; además surge una combinación de áreas dentro del gobierno corporativo. Por ello la creación de lineamientos estándar es cada vez más importante para el ejercicio de la auditoría informática, estableciendo herramientas de mejores prácticas como COBIT, COSO e ITIL. (Academia de Administración, 2011)

2.4.1 Auditoría Interna

Este tipo de auditoría se la realiza con personal, recursos de la empresa y por expresa decisión de la misma, teniendo como ventaja la realización de revisiones periódicas que puede ser parte del plan anual y a su vez brindar las recomendaciones pertinentes para la mejora en el trabajo.

2.4.2 Auditoría Externa

Es aquella auditoría en la cual la empresa contrata a personas que no pertenezcan a la misma, para evaluar los mecanismos de control que están implantados, e identificar si son adecuados y cumplen con los requerimientos necesarios.

2.4.3 Pruebas y herramientas para efectuar una auditoría informática.

En la realización de una auditoría informática el auditor puede realizar las siguientes pruebas:

Pruebas sustantivas: Verifican el grado de confiabilidad del Sistema de Información (SI) del organismo. Se suelen obtener mediante observación, cálculos, muestreos,

entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican así mismo la exactitud, integridad y validez de la información.

Pruebas de cumplimiento: Verifican el grado de cumplimiento de lo revelado mediante el análisis de la muestra. Proporciona evidencias de que los controles claves existen y que son aplicables efectiva y uniformemente. (ANF, 2013).

Las principales herramientas de las que dispone un auditor informático son: observación, realización de cuestionarios, entrevistas a auditados y no auditados, muestreo estadístico, flujogramas, listas de chequeo, mapas conceptuales, etc. (ANF, 2013)

2.5 Marco conceptual

2.5.1 Auditoría

La palabra auditoría significa integridad (que no falta nada), comportamiento de una actividad según ciertos lineamientos, que implica la forma en que se llevan las cosas. Por ello una auditoría puede llevarse a cabo para verificar o examinar que todo esté correcto y presente.

Con relación a lo anteriormente mencionado, auditar es la acción que realiza el profesional experto en el análisis de evidencias que mostrará resultados a los interesados e informará si las actividades se las realizó de acuerdo a las disposiciones. (Arter, 2004)

2.5.2 ISACA

Es el acrónimo de ***Information Systems Audit and Control Association*** (Asociación de Auditoría y Control de Sistemas de Información), una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades auditoría y control en sistemas de información. (Universidad de Sevilla, 2015)

2.5.3 Riesgo

El término riesgo posee algunos significados tales como: Es el efecto de la incertidumbre en la consecución de los objetivos, combinación de la probabilidad de un evento y su consecuencia. La posibilidad que algo suceda y que tenga impacto en el logro de los objetivos. (ISO 31000:2009, 2011)

2.5.4 ISO

La Organización Internacional para la Estandarización (ISO) es una federación de alcance mundial no gubernamental que tiene como función buscar la estandarización de normas de productos y seguridad para las empresas a nivel internacional, las cuales están en permanente revisión. El término ISO, se inspiró en el término griego isos, que significa "igual"; esto se debe a que las normas pretenden establecer comparaciones entre compañías en igualdad de condiciones.
Todos los trabajos realizados por la ISO resultan en acuerdos internacionales los cuales son publicados como Estándares Internacionales. (Summers, 2006)

2.6 Estado del arte

A nivel mundial COBIT es un modelo que ha permitido a muchas empresas obtener criterios para evaluar la gestión y control de los sistemas de información y tecnología, con lo que se promueve el control de los negocios y la seguridad de TI.

Según la revista ***SearchDataCenter en Español*** la realidad geográfica de Latinoamérica muestra dos grupos: las empresas reguladas donde el estándar es COBIT y las no reguladas quienes adoptan estándares cuando están buscando mejores prácticas o porque simplemente tratan de imitar a otras empresas.

En el Ecuador la idea de implementar COBIT como un marco general flexible que se adapte a los recursos de la empresa y orientado a los objetivos de la misma es cada vez más oportuno e interesante debido a que es una herramienta que se enfoca a controles específicos y además es una recomendación de expertos internacionales como ISACA (Asociación de Auditoría y Control de Sistemas de Información).

2.7 Metodologías y Técnicas de Investigación

2.7.1 Métodos Teóricos

2.7.1.1 Método Analítico

Este método en el desarrollo de la investigación permite realizar un procedimiento de descomposición de un todo general, para el caso "Entrega, Soporte y Servicio", de tal forma que se extrae los elementos o partes que lo componen para efectuar un estudio de forma particular, evidenciando un análisis más profundo y concreto en cada una de ellas, como base para la evaluación.

2.7.1.2 Método Deductivo

Este método permite realizar un análisis específico en cuanto a la metodología aplicada a la presente evaluación técnica en base a "COBIT 5"; donde se identifica uno a uno los parámetros e indicadores establecidos en la misma, frente a los servicios que corresponden al área de Entrega, Soporte y Servicio de la Universidad de las Fuerzas Armadas ESPE.

2.7.1.3 Método Sintético

A través de este procedimiento se logra relacionar todos los elementos necesarios para la evaluación técnica informática y unificarlos para posteriormente obtener como resultado el Informe final de este trabajo.

2.8 Instrumentos de Investigación.

Las técnicas de investigación son los medios o herramientas que utiliza el investigador en la recopilación de los datos, las cuales se seleccionan conforme a las necesidades de la investigación, en función de la muestra elegida y se aplican tanto para hacer acopio de los antecedentes como para la observación del fenómeno, la experimentación de los elementos de la encuesta, etc.; entre las que destacan la

recopilación documental, cuestionarios, entrevistas, encuestas, observación y experimentación. (Razo, 1998).

2.8.1 Recopilación Documental

La recopilación documental es un instrumento o técnica de investigación general cuya finalidad es obtener datos e información a partir de fuentes documentales con el fin de ser utilizados dentro de los límites de una investigación en concreto. (Torrealba, 2009)

2.8.2 Cuestionarios

Es la recopilación de datos que se realiza de forma escrita por medio de preguntas abiertas, cerradas, dicotómicas, por rangos, de opción múltiple, etc. En este caso el encuestado contesta según su criterio y con sus respuestas se obtienen resultados representativos. (Razo, 1998)

2.8.3 Entrevistas

La entrevista es una técnica de recopilación de información mediante una conversación profesional, con la que además de adquirirse información acerca de lo que se investiga, tiene importancia desde el punto de vista educativo; los resultados a lograr en la misión dependen en gran medida del nivel de comunicación entre el investigador y los participantes en la misma.

Según el fin que se persigue con la entrevista, ésta puede estar o no estructurada mediante un cuestionario previamente elaborado. Cuando la entrevista es aplicada en las etapas previas de la investigación donde se quiere conocer el objeto de investigación desde un punto de vista externo, sin que se requiera aún la

profundización en la esencia del fenómeno, las preguntas a formular por el entrevistador, se deja a su criterio y experiencia. (Ferrer, 2010).

2.8.4 Encuesta

Es el procedimiento mediante el cual los sujetos brindan directamente información al investigador. Son técnicas llamadas de reporte personal, ya que son las personas las que aportan la información. La investigación por encuesta proviene del contexto de la investigación cuantitativa aunque también puede recopilar información cualitativa; la intención es describir, analizar y establecer las relaciones entre variables en poblaciones o grupos particulares, generalmente de cierta extensión. La investigación por encuesta es propicia cuando se quiere obtener un conocimiento de colectivos o clases de sujetos, instituciones o fenómenos. (Yuni, 2006)

2.8.5 Observación

Es una técnica que recoge información con el uso sistemático de nuestros sentidos orientados a la captación de la realidad que queremos estudiar, el principal sentido implicado es la vista para estudiar los objetos o fenómenos de la naturaleza, además está sujeta a una serie de principios y reglas necesarias para poder llegar a su realización. (Peinado, 2015)

2.8.6 Experimentación

Es el estudio de un fenómeno sometido a condiciones especiales conforme a las necesidades del investigador pero que también puede ser susceptible de modificaciones en sus variables. (Razo, 1998).

2.9 Base Legal

2.9.1 Código Orgánico Integral Penal

2.9.1.1 Delitos contra la seguridad de los activos de los sistemas de información y comunicación.

Artículo 229.- Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.

Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

Artículo 230.- Interceptación ilegal de datos.- Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.
2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.
3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Artículo 232.- Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

Artículo 233.- Delitos contra la información pública reservada legalmente.- La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años.

La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años.

Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.

Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga

dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

2.9.2 Leyes

2.9.2.1 Ley Del Sistema Nacional De Registros De Datos Públicos

Art. 4.- Responsabilidad de la información.- Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este provee toda la información.

Las personas afectadas por información falsa o imprecisa, difundida o certificada por registradoras o registradores, tendrán derecho a las indemnizaciones correspondientes, previo el ejercicio de la respectiva acción legal.

La Dirección Nacional de Registro de Datos Públicos establecerá los casos en los que deba rendirse caución.

Art. 23.- Sistema Informático.- El sistema informático tiene como objetivo la tecnificación y modernización de los registros, empleando tecnologías de información, bases de datos y lenguajes informáticos estandarizados, protocolos de intercambio de datos seguros, que permitan un manejo de la información adecuado que reciba, capture, archive, codifique, proteja, intercambie, reproduzca, verifique, certifique o procese de manera tecnológica la información de los datos registrados.

El sistema informático utilizado para el funcionamiento e interconexión de los registros y entidades, es de propiedad estatal y del mismo se podrán conceder licencias de uso limitadas a las entidades públicas y privadas que correspondan, con las limitaciones previstas en la Ley y el Reglamento.

Art. 26.- Seguridad.- Toda base informática de datos debe contar con su respectivo archivo de respaldo, cumplir con los estándares técnicos y plan de contingencia que impidan la caída del sistema, robo de datos, modificación o cualquier otra circunstancia que pueda afectar la información pública. (Ley del Sistema Nacional de Registro de Datos públicos, 2010)

2.9.3 Reglamentos

2.9.3.1 Reglamento General De Bienes Del Sector Público

Art. 95.- Plan de Mantenimiento Todas las entidades públicas deberán, deberán tener un Plan Anual de Mantenimiento de Equipos Informáticos , el mismo que debe contar con cronogramas, y financiamiento y estar aprobado por las máximas autoridades.

Art. 96.- Mantenimiento El mantenimiento de equipos informáticos estará a cargo de la Unidad responsable de esta actividad en cada institución. En las entidades que no dispongan de esta unidad, se deberán contratar los servicios externos para el efecto, de acuerdo a los procedimientos internos de cada entidad y en atención a las normas vigentes sobre la materia.

Art. 97.- Control Corresponde a la unidad responsable de cada entidad independientemente del inventario que mantenga la Unidad de Activos Fijos, mantener un listado actualizado de los equipos que conforman el parque informático de la institución. El registro deberá contener los datos básicos de cada equipo, como son: Código de activo fijo, número de serie, marca, ubicación del bien, características principales, fecha de compra, período de garantía, proveedor del equipo y estado del equipo, de manera que permita conocer sus características . Con la finalidad de mantener actualizada la información, las unidades administrativas, darán a conocer a la unidad responsable las novedades de movilización efectuadas.

Adicionalmente, la unidad responsable deberá mantener un historial de los trabajos efectuados.

La unidad responsable de cada entidad deberá mantener también un registro actualizado del licenciamiento del software adquirido, el mismo que comprenderá el código de activo fijo, identificación del producto, descripción del contenido, número

de versión, número de serie, nombre del proveedor, fecha de adquisición y otros datos que sean necesarios.

Art 98.- Reparación de talleres particulares Cuando los equipos de la entidad u organismo deban ser reparados en talleres particulares, previamente a su salida se debe, se debe contar con la autorización y conocimiento de las correspondientes unidades administrativas y del Guardalmacén de la entidad, y con los documentos de respaldo de la persona que ha entregado el equipo y del taller que lo recibió.

Art 99.- Clases de mantenimiento El término mantenimiento se entenderá como:

Mantenimiento correctivo, que es el conjunto de procedimientos utilizados para reparar una máquina o equipos ya deteriorados. Mediante el mantenimiento correctivo no solo ser repara maquinaria ya deteriorada sino que se realizan ajustes de equipos cuyos procesos evidentemente tienen fallas.

Mantenimiento preventivo, que es la inspección periódica de máquinas y equipos, para evaluar su estado de funcionamiento, identificar fallas, prevenir y poner en condiciones el equipo, para su óptimo funcionamiento, limpieza, lubricación y ajuste. Es también en este tipo de mantenimiento, en el que se remplazan piezas, para las cuales el fabricante del equipo, ha identificado que tiene un número específico de horas de servicio.

Mantenimiento predictivo, que consiste en el monitorio continuo de máquinas y equipos con el propósito de detectar y evaluar, cualquier pequeña variación en su funcionamiento, antes de que se produzca una falla. (Reglamento General de Bienes del Sector Público, 2006)

2.9.3.2 Reglamento General De La Ley Orgánica Del Sistema Nacional De Contratación Pública

Art.121.- Administrador del contrato En todo contrato, la entidad contratante designará de manera expresa, un administrador del mismo, quien velará por el aval y oportuno cumplimiento de todas y cada una de las obligaciones derivadas del contrato. Adoptará las acciones que sean necesarias para evitar retrasos injustificados e impondrá las multas y sanciones a que hubiere lugar.

Si el contrato es de ejecución de obras, prevé y requiere de los servicios de fiscalización, el administrador del contrato velará porque está actúe de acuerdo a las especificaciones constantes en los pliegos o en el propio contrato.

Art 124.- Contenido de las actas Las actas de recepción provisional, parcial, total y definitivas serán suscritas por el contratistas y los integrantes de la Comisión designada por la máxima autoridad de la entidad contratante o su delegado conformada por el administrador del contrato y un técnico que no haya intervenido en el proceso de ejecución del contrato.

Las actas contendrán los antecedentes, condiciones generales de la ejecución, condiciones operativas, liquidación económica, liquidación de plazos, constancia de la recepción, cumplimiento de las obligaciones contractuales, reajustes de precios pagados, o pendientes de pago, o cualquier otra circunstancia que se estime necesaria.

En las recepciones provisionales parciales, se hará constar como antecedente, los datos relacionados con la recepción precedente. La última recepción provisional incluirá la información sumaria de todas las anteriores.

(Reglamento general a la ley orgánica del sistema nacional de contratación pública, 2009)

2.9.4 Normas De Control Interno Para Las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que Dispongan De Recursos Públicos.

2.9.4.1 Normas de Control Interno "Tecnología de la información"

410-01 Organización informática.- Las entidades y organismos del sector público deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control, así como el involucramiento de la alta dirección, por lo que las actividades y procesos de tecnología de información de la organización deben estar bajo la responsabilidad de una unidad que se encargue de regular y estandarizar los temas tecnológicos a nivel institucional.

410-02 Segregación de funciones.- Las funciones y responsabilidades del personal de tecnología de información y de los usuarios de los sistemas de información serán claramente definidas y formalmente comunicadas para permitir que los roles y responsabilidades asignados se ejerzan con suficiente autoridad y respaldo.

410–03 Plan informático estratégico de tecnología.- La unidad de tecnología de la información elaborará e implementará un plan informático estratégico para administrar y dirigir todos los recursos tecnológicos, el mismo que estará alineado con el plan estratégico institucional y éste con el Plan Nacional de Desarrollo y las políticas públicas de gobierno.

410-04 Políticas y procedimientos.- La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria.

410-05 Modelo de información organizacional.- La unidad de tecnología de información definirá el modelo de información de la organización a fin de que se facilite la creación, uso y compartición de la misma; y se garantice su disponibilidad, integridad, exactitud y seguridad sobre la base de la definición e implantación de los procesos y procedimientos correspondientes.

410-06 Administración de proyectos tecnológicos.- La unidad de tecnología de información definirá mecanismos que faciliten la administración de todos los proyectos informáticos que ejecuten las diferentes áreas que conformen dicha unidad.

410-07 Desarrollo y adquisición de software aplicativo.- La unidad de tecnología de información regulará los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos.

410-08 Adquisiciones de infraestructura tecnológica.- La unidad de tecnología de información definirá, justificará, implantará y actualizará la infraestructura tecnológica de la organización.

2.9.4.2 Normas de Control Interno “Mantenimiento y control de IT”

410-09 Mantenimiento y control de la infraestructura tecnológica.- La unidad de tecnología de información de cada organización definirá y regulará los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de las entidades.

410-10 Seguridad de tecnología de información.- La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

410-11 Plan de contingencias.- Corresponde a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado.

410-12 Administración de soporte de tecnología de información.- La unidad de tecnología de información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen.

410-13 Monitoreo y evaluación de los procesos y servicios.- Es necesario establecer un marco de trabajo de monitoreo y definir el alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad.

410-14 Sitio web, servicios de internet e intranet.- Es responsabilidad de la unidad de tecnología de información elaborar las normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio WEB de la entidad, a base de las disposiciones legales y normativas y los requerimientos de los usuarios externos e internos.

410-15 Capacitación informática.- Para la creación de un comité informático institucional, se considerarán los siguientes aspectos: El tamaño y complejidad de la entidad y su interrelación con entidades adscritas. La definición clara de los objetivos que persigue la creación de un comité de informática, como un órgano de decisión, consultivo y de gestión que tiene como propósito fundamental definir, conducir y evaluar las políticas internas para el crecimiento ordenado y progresivo de la tecnología de la información y la calidad de los servicios informáticos, así como apoyar en esta materia a las unidades administrativas que conforman la entidad. La conformación y funciones del comité, su reglamentación, la creación de grupos de

trabajo, la definición de las atribuciones y responsabilidades de los miembros del comité, entre otros aspectos.

410-17 Firmas electrónicas.- Las entidades, organismos y dependencias del sector público, así como las personas jurídicas que actúen en virtud de una potestad estatal, ajustarán sus procedimientos y operaciones e incorporarán los medios técnicos necesarios, para permitir el uso de la firma electrónica de conformidad con la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y su Reglamento. (Normas de aplicación obligatoria para las entidades del sector público ecuatoriano expedidas por la Contraloría General del Estado, 2009).

CAPÍTULO III

3 Desarrollo de la Evaluación Técnica Informática

3.1 Introducción

Previo a la evaluación propuesta se realiza un análisis general de la información contenida en el Plan Estratégico de Desarrollo Institucional de la ESPE, así como también de la organización interna de la Unidad de Tecnologías de Información y Comunicación (UTIC), para definir e identificar los procesos a evaluar y los medios utilizados para la verificación de su cumplimiento.

3.2 Plan Estratégico Institucional

3.2.1 Perspectivas o Dimensiones Estratégicas

- De Talento Humano, Financiera e Infraestructura.
- De Procesos.
- De Estudiantes y Usuarios.
- De Impacto en la Ciudadanía.

3.2.2 Objetivos Estratégicos

1. Incrementar el reconocimiento de la Universidad de las Fuerzas Armadas – ESPE como una institución referente en educación superior.
2. Incrementar la calidad de los profesionales y postgraduados.
3. Incrementar la producción científica - tecnológica y su calidad.
4. Incrementar el impacto social de los programas de vinculación.
5. Incrementar la eficiencia y eficacia del sistema formativo de grado y postgrado.
6. Incrementar la capacidad del sistema de investigación integrándolo con el modelo formativo.

7. Incrementar la capacidad y calidad del sistema de vinculación integrándolo con el sistema de investigación y con el modelo formativo.
8. Incrementar las capacidades de sustentación institucional. (Talento Humano-Finanzas- Recursos Físicos y Tecnológicos). (Plan Estratégico de Desarrollo Institucional PEDI 2014).

3.3 Estructura Interna actual de procesos en la UTIC.

Actualmente la Unidad de Tecnologías de Información y Comunicación (UTIC) cuenta con la siguiente estructura en la organización de procesos:

- Dirección de UTIC
- Evaluación Interna y Acción
- Planificación de Gestión de TICs.
- Aplicaciones y Desarrollo de Servicios TICs.
- Infraestructura de TICs.
- Provisión de Servicios de TICs.

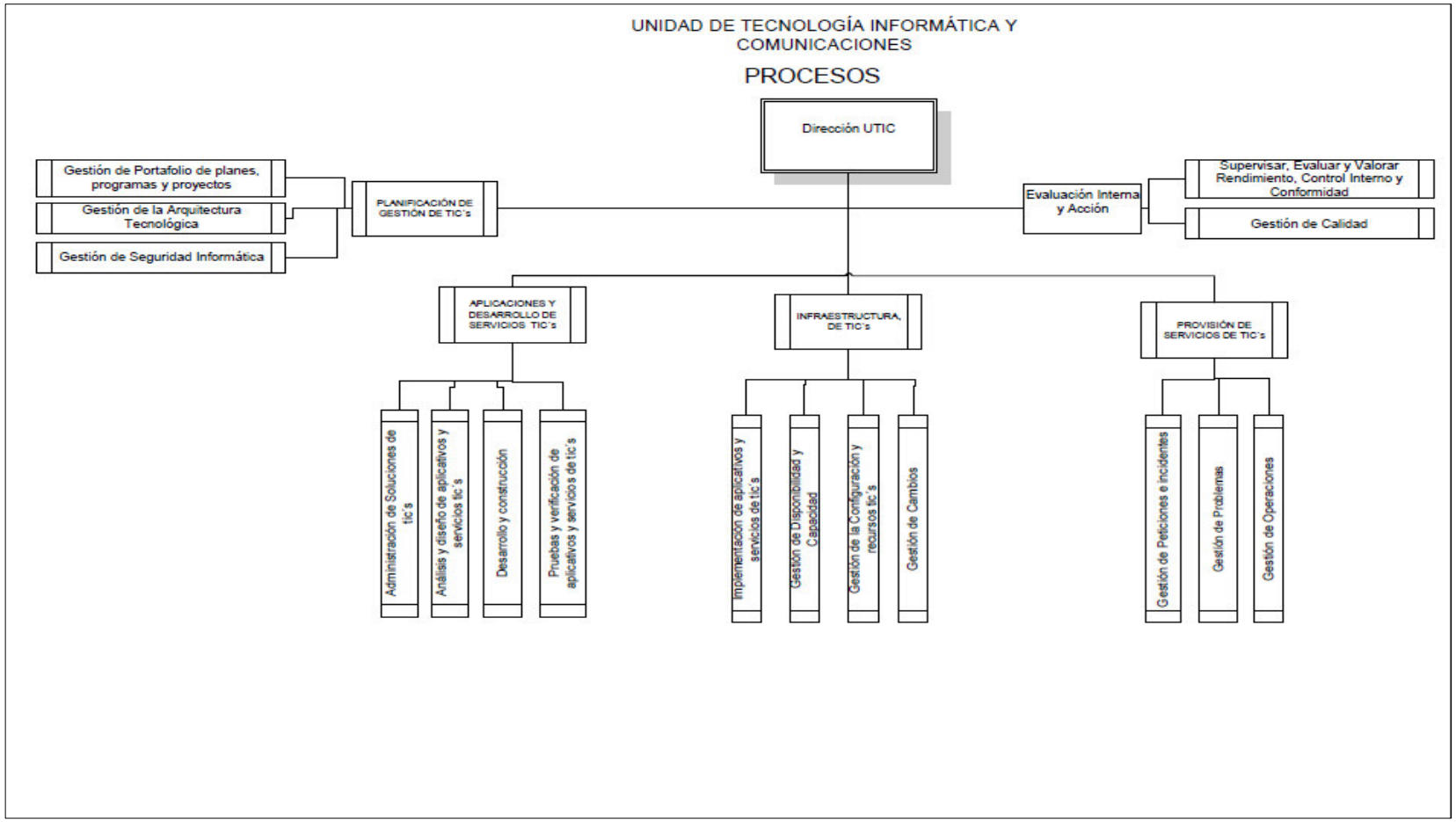


Figura 6. Estructura de Procesos UTIC-ESPE

Fuente: (UTIC, 2015)

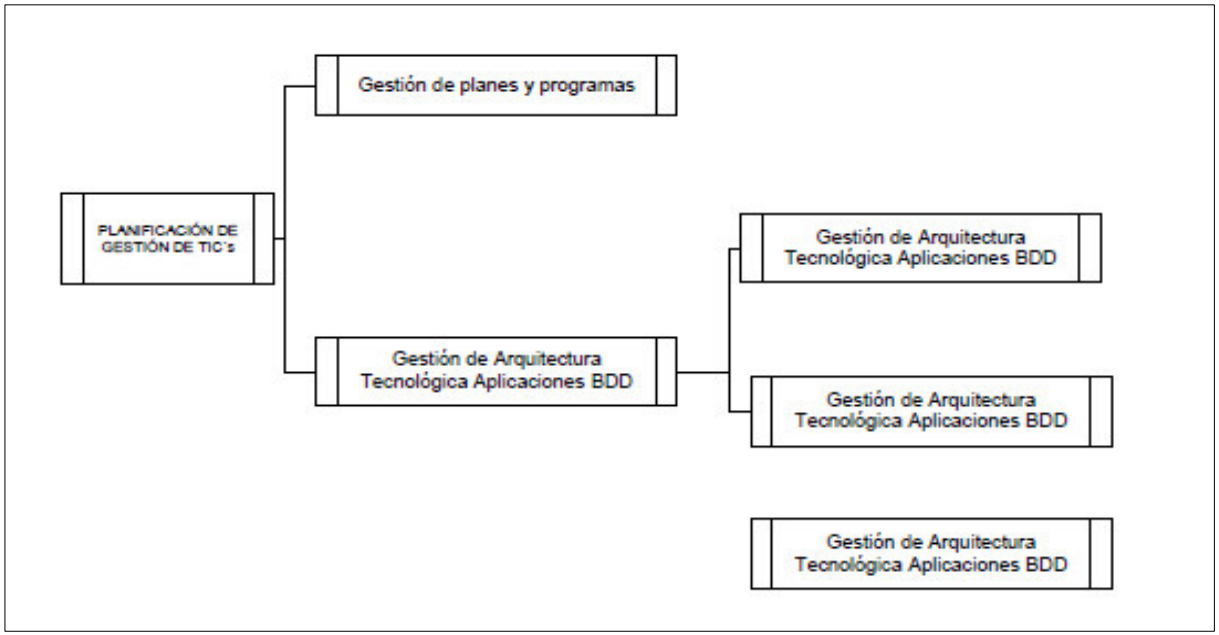


Figura 7. Estructura de Procesos UTIC-ESPE-2

Fuente: (UTIC, 2015)

3.4 Mapeos detallados entre COBIT 5, Objetivos TI y Procesos de Entrega, Servicio y Soporte.

3.4.1 Mapeo de Objetivos Corporativos COBIT 5 Vs Objetivos Estratégicos ESPE.

La Tabla 1 contiene:

- En las columnas, los 17 Objetivos genéricos de la empresa definidos en COBIT 5, agrupados por dimensión del Cuadro de Mando Integral (CMI).
- En las filas, los 8 Objetivos Estratégicos de la ESPE establecidos en el Plan Estratégico de Desarrollo Integral 2014-2017.
- En la parte superior se muestran los resultados totales de la suma por columnas.
- Esta matriz muestra el mapeo realizado por el grupo de Evaluación de Entrega, Soporte y Servicio del Proyecto general desarrollado para la ESPE.
- Un mapeo de cómo cada Objetivo Corporativo de COBIT 5 es soportado por el objetivo Estratégico de la ESPE. Este mapeo utiliza la siguiente escala: 1, 2, y 3, es decir relación menor, relación media y relación de mayor importancia respectivamente para los objetivos de la compañía.

3.4.2 Consolidado de resultados del mapeo Objetivos Estratégicos ESPE Vs Objetivos Corporativos COBIT 5 (por grupos de trabajo del Proyecto).

La Tabla 2 contiene:

- En las columnas, los nombres de las personas responsables de cada grupo para el desarrollo del proyecto ESPE, con los respectivos resultados por grupo con base al Mapeo de Objetivos Corporativos COBIT 5 Vs Objetivos Estratégicos ESPE.
- En las filas, los 17 objetivos genéricos de la empresa definidos en COBIT 5.

3.4.3 Validación de resultados del mapeo Objetivos Corporativos COBIT 5 Vs Objetivos Estratégicos ESPE (por grupos de trabajo del Proyecto).

La Tabla 3 contiene:

- Una vez obtenidos los resultados por grupos de trabajo para la respectiva validación se procede a sumar el contenido de las filas relacionadas con los Objetivos corporativos de COBIT 5.
- En la columna denominada *Importancia*, se ubica el orden de los resultados según su importancia por ejemplo: el máximo valor es 159 puntos por lo tanto estará en primer lugar, el valor de 148 puntos está en segundo lugar y así sucesivamente.
- En la columna denominada *validación,* están los resultados generados por el Directorio que representa a la ESPE utilizando el mapeo de la Tabla 2.
- La columna denominada *Resumen*, establece una fórmula matemática en la que el mayor valor obtenido por el Directorio (159) se lo divide para el mayor valor obtenido resultado de los grupos (73) y éste a su vez multiplicado por los resultados parciales de la fila ejemplo: (73/159)*159, (73/159)*148, (73/159)*82.
- En base a esta validación colocamos “P” que significa primario, cuando hay una importante relación y “S” que significa secundario, cuando todavía hay una relación fuerte, pero menos importante.

3.4.4 Mapeo de los Objetivos de TI Vs los Objetivos Corporativos de COBIT 5

La Tabla 4 contiene:

- En las columnas, los 17 Objetivos relacionados a Tecnologías de Información (TI), agrupados por dimensión del Cuadro de Mando Integral (CMI).
- En las filas, los 17 Objetivos Corporativos COBIT 5, también agrupados por dimensión del Cuadro de Mando Integral (CMI).

- Un mapeo de cómo cada objetivo de TI es soportado por la meta relacionada con COBIT 5, se expresa usando la siguiente escala: “P” significa primario, cuando hay una importante relación, es decir, la meta relacionada con COBIT 5 es un soporte primario para el objetivo TI de la compañía. “S” significa secundario, cuando todavía hay una relación fuerte, pero menos importante, es decir, la meta relacionada con COBIT 5 es un soporte secundario para el objetivo TI de la compañía.

3.4.5 Valoración numérica del mapeo de los Objetivos Corporativos de COBIT 5 Vs Objetivos de TI.

La Tabla 6 contiene:

- Las mismas denominaciones en filas y columnas de la Tabla 4 pero con un valor numérico de 1, 2, 3 según corresponda su importancia para el criterio de los evaluadores.
- En la columna denominada *Total*, se obtiene el resultado de la suma por filas, siendo el máximo valor 25.
- En la columna denominada *Ponderación*, aplicamos la fórmula matemática siguiente: 100 como valor base dividido para 25 que es el valor máximo obtenido de los resultados de las filas, ejemplo: (100/25)*25, (100/25)*4, etc. En base a esta relación se descarta los Objetivos COBIT 5 con menor puntaje.
- Los Objetivos que no son tomados en cuenta son:

  - Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas.
  - Transparencia de los costes, beneficios y riesgos de las TI.
  - Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.
  - Cumplimiento de las políticas internas por parte de las TI.

3.4.6 Mapeo de los Objetivos Corporativos de COBIT 5 Vs los Procesos de Entrega, Soporte y Servicio.

La Tabla 7 contiene:

- En las filas, los 6 procesos de Entrega, Soporte y Servicio establecidos por COBIT 5.
- En las columnas, las 17 metas de TI, agrupados por dimensión del CMI de TI.
- Se ha utilizado 1, 2, 3 para determinar una ponderación.
- Se suma las filas y de acuerdo a los resultados se obtiene los procesos con mejor puntaje para proceder a evaluarlos.

Tabla 1

Mapeo Obj. Corporativos COBIT 5 Vs Obj. Estratégicos ESPE

Mapeo Objetivos Corporativos COBIT 5 Vs Objetivos Estratégicos ESPE	Valor para las partes interesadas de las inversiones de negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activo)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basadas en información	Optimización de costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Personal entrenado y motivado	Cultura de innovación del producto y del negocio	**TOTAL**
TOTAL	**24**	**17**	**16**	**18**	**16**	**19**	**18**	**17**	**15**	**11**	**15**	**16**	**16**	**17**	**17**	**19**	**18**	
PRIORIDAD TOTAL	**P**	**P**	**S**	**P**	**S**	**P**	**P**	**P**	**S**	**S**	**S**	**S**	**S**	**P**	**P**	**P**	**P**	
1. Incrementar el reconocimiento de la Universidad de las Fuerzas Armadas – ESPE como una institución referente en educación superior.	3	2	3	3	3	3	1	2	2	2	2	3	2	2	1	2	1	**37**
2. Incrementar la calidad de los profesionales y postgraduados	3	2	3	2	1	3	3	2	2	1	2	2	2	2	3	3	3	**39**
3. Incrementar la producción científica - tecnológica y su calidad.	3	2	2	2	3	3	3	3	2	2	2	2	2	2	2	2	3	**40**
4. Incrementar el impacto social de los programas de vinculación	3	2	2	2	2	2	2	2	2	1	2	1	2	2	3	3	2	**35**

CONTINÚA

Mapeo Objetivos Corporativos COBIT 5 Vs Objetivos Estratégicos ESPE	Valor para las partes interesadas de las inversiones de negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activo)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basadas en información	Optimización de costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Personal entrenado y motivado	Cultura de innovación del producto y del negocio	**TOTAL**
5. Incrementar la eficiencia y eficacia del sistema formativo de grado y postgrado	3	2	2	3	2	2	2	2	2	1	2	2	2	2	2	2	2	**35**
6. Incrementar la capacidad del sistema de investigación integrándolo con el modelo formativo.	3	2	1	3	1	2	2	2	1	1	1	2	2	2	2	2	2	**31**
7. Incrementar la capacidad y calidad del sistema de vinculación integrándolo con el sistema de investigación y con el modelo formativo	3	2	1	2	1	2	2	2	2	1	1	2	2	2	2	2	2	**31**
8. Incrementar las capacidades de sustentación institucional. (Talento Humano Finanzas-Recursos Físicos y Tecnológicos).	3	3	2	1	3	2	3	2	2	2	3	2	2	3	2	3	3	**41**

Tabla 2

Consolidado de resultados del mapeo Obj. ESPE Vs Obj. COBIT 5

Consolidado de resultados del mapeo Objetivos ESPE Vs Objetivos Corporativos COBIT 5 por grupos de trabajo	Verónica Siguencia	Paul Cajamarca	Ángelo [illegible]	Ítalo Espín	Jhony Pruna	Wilfrido Rosero	Lorena Llumiquinga	Jackeline Becerra Henry León	Gabriel Enríquez	Carlos Chávez	Santiago Tapia
1. Valor para los interesados de las inversiones de Negocio	98	33	67	92	15	12	17	24	46	28	50
2. Cartera de productos y servicios competitivos	97	20	38	105	42	8	16	17	63	24	30
3. Riesgos de negocio gestionados (salvaguarda de activos)	64	20	7	87	43	2	5	16	14	23	7
4. Cumplimiento de leyes y regulaciones externas	80	23	21	76	42	1	15	18	5	14	13
5. Transparencia financiera	72	18	3	94	14	0	4	16	7	25	5
6. Cultura de servicio orientada al cliente	101	20	4	105	41	4	14	19	48	13	29
7. Continuidad y disponibilidad del servicio del negocio	73	18	3	88	42	5	13	18	15	22	14
8. Respuestas ágiles a un entorno de negocio cambiante	102	23	45	98	15	10	12	17	12	27	29
9.Toma Estratégica de decisiones basa en información	97	24	2	98	41	0	11	15	8	16	13
10. Optimización de costes de entrega de servicio	65	18	7	91	42	2	3	11	7	18	17
11. Optimización de la funcionalidad de los procesos del negocio	65	23	7	93	14	3	2	15	23	22	32
12. Optimización de los costos de los procesos del negocio	65	23	4	91	41	2	10	16	11	16	16
13. Programas gestionados de cambio en el negocio	68	21	19	98	15	0	9	16	13	18	6
14. Productividad operacional y de los empleados	67	23	28	79	42	2	8	17	18	19	16
15. Cumplimiento con las políticas internas	71	25	4	83	15	0	1	17	6	25	9
16. Personas preparadas y motivadas	106	24	7	85	42	2	7	19	23	21	0
17. Cultura de innovación de producto y negocio	99	25	39	100	15	8	6	18	50	19	38

Tabla 3

Validación de resultados del mapeo Obj. ESPE Vs COBIT 5

Validación de puntuación de la Alineación de Objetivos Corporativos ESPE Vs Objetivos Corporativos COBIT 5.	Verónica Siguencia	Paul Cajamarca	Ángelo Núñez	Ítalo Espín	Jhony Pruna	Wilfrido Rosero	Lorena Llumiquinga	Becerra / León	Gabriel Enríquez	Carlos Chávez	Santiago Tapia	Puntaje	Importancia	Validación	Resumen	FINAL	
1. Valor para los interesados de las inversiones de Negocio	13	17	17	9	4	17	17	17	14	17	17	159	**1**	71	73,00	73,00	P
2. Cartera de productos y servicios competitivos	11	5	14	17	16	15	16	10	17	13	14	148	**2**	70	67,95	67,95	P
3. Riesgos de negocio gestionados (salvaguarda de activos)	1	4	8	5	17	10	5	7	9	12	4	82	**11**	13	37,65	37,65	P
4. Cumplimiento de leyes y regulaciones externas	10	11	12	1	11	5	15	12	1	2	6	86	**9**	72	39,48	39,48	P
5. Transparencia financiera	8	2	2	11	2	1	4	4	4	15	2	55	**17**	46	25,25	25,25	S
6. Cultura de servicio orientada al cliente	15	6	4	16	10	12	14	16	15	1	12	121	**5**	66	55,55	55,55	P
7. Continuidad y disponibilidad del servicio del negocio	9	3	3	6	14	13	13	13	10	10	8	102	**7**	61	46,83	46,83	P
8. Respuestas ágiles a un entorno de negocio cambiante	16	12	16	14	6	16	12	11	7	16	13	139	**4**	73	63,82	63,82	P
9.Toma Estratégica de decisiones basadas en información	12	13	1	12	9	4	11	2	5	3	7	79	**12**	67	36,27	36,27	P
10. Optimización de costes de entrega de servicio	2	1	7	8	15	9	3	1	3	5	11	65	**16**	32	29,84	29,84	S
11. Optimización de la funcionalidad de los procesos del negocio	3	8	9	10	1	11	2	3	12	11	15	85	**10**	57	39,03	39,03	P
12. Optimización de los costos de los procesos del negocio	4	9	5	7	8	6	10	6	6	4	9	74	**14**	36	33,97	33,97	S
13. Programas gestionados de cambio en el negocio	6	7	11	13	5	3	9	5	8	6	3	76	**13**	60	37,00	37,00	P
14. Productividad operacional y de los empleados	5	10	13	2	12	7	8	9	11	7	10	94	**8**	62	43,16	43,16	P
15. Cumplimiento con las políticas internas	7	15	6	3	3	2	1	8	2	14	5	66	**15**	26	30,30	30,30	S
16. Personas preparadas y motivadas	17	14	10	4	13	8	7	15	13	9	1	111	**6**	68	50,96	50,96	P
17. Cultura de innovación de producto y negocio	14	16	15	15	7	14	6	14	16	8	16	141	**3**	69	64,74	64,74	P

Tabla 4

Mapeo de los Objetivos de TI Vs Objetivos de COBIT 5

Mapeando los Objetivos de TI Vs Objetivos Corporativos de COBIT 5	Alineamiento de TI y la estrategia de	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados.	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI.	Entrega de servicios de TI de acuerdo a los requisitos del negocio.	Uso adecuado de aplicaciones, información y soluciones tecnológicas.	Agilidad de las TI.	Seguridad de la información, infraestructura de procesamiento y	Optimización de activos, recursos y capacidades de las TI.	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
1. Valor para los interesados de las inversiones de Negocio	P		P		P	S	P	S	S		P	S	P	S		S	S
2. Cartera de productos y servicios competitivos.	P		S		P		P	S	P		S	P	S	S		S	P
3. Riesgos de negocio gestionados (salvaguarda de activos).	S	S	S	P		S	S	S	S	P		S	S	S	S	P	
4. Cumplimiento de leyes y regulaciones externas.		P		S			S			P				S	S		
5. Transparencia financiera.						P											
6. Cultura de servicio orientada al cliente.	P				S		P	S	S			S	S			S	S
7. Continuidad y disponibilidad del servicio del negocio.	S			P			S	S		P				P			
8. Respuestas ágiles a un entorno de negocio cambiante	P		S	S	S		P		P		S	S				S	P
9. Toma Estratégica de decisiones basadas en información.	P		S			S	S	S						P			S

CONTINÚA

Mapeando los Objetivos de TI Vs Objetivos Corporativos de COBIT 5	Alineamiento de TI y la estrategia de negocio.	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas.	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI.	Riesgos de negocio relacionados con las TI gestionados.	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI.	Transparencia de los costes, beneficios y riesgos de las TI.	Entrega de servicios de TI de acuerdo a los requisitos del negocio.	Uso adecuado de aplicaciones, información y soluciones tecnológicas.	Agilidad de las TI.	Seguridad de la información, infraestructura de procesamiento y aplicaciones.	Optimización de activos, recursos y capacidades de las TI.	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
10. Optimización de costes de entrega de servicio.	S			P	S	P		S			P	S	S				
11. Optimización de la funcionalidad de los procesos del negocio.	P		S		S		P	P	P		S	P		S			S
12. Optimización de los costos de los procesos del negocio.	S				P	P	S	S			P	S	S				
13. Programas gestionados de cambio en el negocio.	P		P	S			S		S		S	S	P				S
14. Productividad operacional y de los empleados.					S			P	S		S	S				P	
15. Cumplimiento con las políticas internas.		P		S						P					P		
16. Personas preparadas y motivadas.	S		S	S			S	S	S							P	S
17. Cultura de innovación de producto y negocio.	S		S		S		S	S	P		S	S				S	P

Tabla 5

Mapeo de Objetivos corporativos COBIT 5 Vs Objetivos de TI

Mapeando Objetivos Corporativos COBIT 5.Vs Objetivos De TI / **OBJ. DE TI**	**OBJ. CORPORATIVOS**	1. Valor para los interesados de las inversiones de Negocio	2. Cartera de productos y servicios competitivos	3. Riesgos de negocio gestionados (salvaguarda de activos)	4. Cumplimiento de leyes y regulaciones externas	5. Transparencia financiera	6. Cultura de servicio orientada al cliente	7. Continuidad y disponibilidad del servicio del negocio	8. Respuestas ágiles a un entorno de negocio cambiante	9.Toma Estratégica de decisiones basadas en información	10. Optimización de costes de entrega de servicio	11. Optimización de la funcionalidad de los procesos del negocio	12. Optimización de los costos de los procesos del negocio	13. Programas gestionados de cambio en el negocio	14. Productividad operacional y de los empleados	15. Cumplimiento con las políticas internas	16. Personas preparadas y motivadas	17. Cultura de innovación de producto y negocio
1.Alineamiento de TI y la estrategia de negocio		P	P	S			P	S	P	P	S	P	S	P			S	S
2.Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas				S	P											p		
3.Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI		P	S	S					S	S		S		P			S	S
4.Riesgos de negocio relacionados con las TI gestionados				P	S			P	S		P			S		S	S	
5.Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI		P	P				S		S		S	S	P		S			S
6.Transparencia de los costes, beneficios y riesgos de las TI		S		S		P				S	P		P					
7.Entrega de servicios de TI de acuerdo a los requisitos del negocio		P	P	S	S		P	S	P	S		P	S	S			S	S

CONTINÚA

Mapeando Objetivos Corporativos Vs Objetivos De TI	**OBJ. CORPORATIVOS**	1. Valor para los interesados de las inversiones de Negocio	2. Cartera de productos y servicios competitivos	3. Riesgos de negocio gestionados (salvaguarda de activos)	4. Cumplimiento de leyes y regulaciones externas	5. Transparencia financiera	6. Cultura de servicio orientada al cliente	7. Continuidad y disponibilidad del servicio del negocio	8. Respuestas ágiles a un entorno de negocio cambiante	9.Toma Estratégica de decisiones basadas en información	10. Optimización de costes de entrega de servicio	11. Optimización de la funcionalidad de los procesos del negocio	12. Optimización de los costos de los procesos del negocio	13. Programas gestionados de cambio en el negocio	14. Productividad operacional y de los empleados	15. Cumplimiento con las políticas internas	16. Personas preparadas y motivadas	17. Cultura de innovación de producto y negocio
OBJ. DE TI																		
8. Uso adecuado de aplicaciones, información y soluciones tecnológicas.		S	S	S			S	S		S	S	P	S		P		S	S
9.Agilidad de las TI		S	P	S			S		P			P		S	S		S	P
10.Seguridad de la información, infraestructura de procesamiento y aplicaciones				P	P			P								P		
11.Optimización de activos, recursos y capacidades de las TI		P	S						S		P	S	P	S	S			S
12.Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio		S	P	S			S		S		S	P	S	S	S			S
13. Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.		P	S	S			S				S		S	P				
14.Disponibilidad de información útil y relevante para la toma de decisiones		S	S	S	S			P		P		S						
15.Cumplimiento de las políticas internas por parte de las TI				S	S											P		

CONTINÚA

Mapeando Objetivos Corporativos Vs Objetivos De TI	**OBJ. CORPORATIVOS**	1. Valor para los interesados de las inversiones de Negocio	2. Cartera de productos y servicios competitivos	3. Riesgos de negocio gestionados (salvaguarda de activos)	4. Cumplimiento de leyes y regulaciones externas	5. Transparencia financiera	6. Cultura de servicio orientada al cliente	7. Continuidad y disponibilidad del servicio del negocio	8. Respuestas ágiles a un entorno de negocio cambiante	9.Toma Estratégica de decisiones basadas en información	10. Optimización de costes de entrega de servicio	11. Optimización de la funcionalidad de los procesos del negocio	12. Optimización de los costos de los procesos del negocio	13. Programas gestionados de cambio en el negocio	14. Productividad operacional y de los empleados	15. Cumplimiento con las políticas internas	16. Personas preparadas y motivadas	17. Cultura de innovación de producto y negocio
OBJ. DE TI																		
16.Personal del negocio y de las TI competente y motivado		S	S	P			S		S						P		P	S
17.Conocimiento, experiencia e iniciativas para la innovación de negocio		S	P				S		P	S		S		S			S	P

Tabla 6
Validación numérica del mapeo Obj. COBIT 5 Vs Obj. TI

Mapeando Objetivos Corporativos Vs Objetivos de TI / OBJ. DE TI	OBJ. CORPORATIVOS	1. Valor para los interesados de las inversiones de Negocio	2. Cartera de productos y servicios competitivos	3. Riesgos de negocio gestionados (salvaguarda de activos)	4. Cumplimiento de leyes y regulaciones externas	5. Transparencia financiera	6. Cultura de servicio orientada al cliente	7. Continuidad y disponibilidad del servicio del negocio	8. Respuestas ágiles a un entorno de negocio cambiante	9.Toma Estratégica de decisiones basadas en información	10. Optimización de costes de entrega de servicio	11. Optimización de la funcionalidad de los procesos del negocio	12. Optimización de los costos de los procesos del negocio	13. Programas gestionados de cambio en el negocio	14. Productividad operacional y de los empleados	15. Cumplimiento con las políticas internas	16. Personas preparadas y motivadas	17. Cultura de innovación de producto y negocio	TOTAL	VALIDACIÓN
1. Alineamiento de TI y la estrategia de negocio		3	3	1			3	1	3	3		3		3			1	1	25	100
2. Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas				1	3														4	16
3. Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI		3	1	1					1	1		1		3			1	1	13	52
4. Riesgos de negocio relacionados con las TI gestionados				3	1			3	1					1			1		10	40
5. Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI		3	3				1		1			1			1			1	11	44
6. Transparencia de los costes, beneficios y riesgos de las TI		1		1						1									3	12
7. Entrega de servicios de TI de acuerdo a los requisitos del negocio		3	3	1	1		3	1	3	1		3		1			1	1	22	88

CONTINÚA

Mapeando Objetivos Corporativos Vs Objetivos de TI	**OBJ. CORPORATIVOS**	1. Valor para los interesados de las inversiones de Negocio	2. Cartera de productos y servicios competitivos	3. Riesgos de negocio gestionados (salvaguarda de activos)	4. Cumplimiento de leyes y regulaciones externas	5. Transparencia financiera	6. Cultura de servicio orientada al cliente	7. Continuidad y disponibilidad del servicio del negocio	8. Respuestas ágiles a un entorno de negocio cambiante	9.Toma Estratégica de decisiones basadas en información	10. Optimización de costes de entrega de servicio	11. Optimización de la funcionalidad de los procesos del negocio	12. Optimización de los costos de los procesos del negocio	13. Programas gestionados de cambio en el negocio	14. Productividad operacional y de los empleados	15. Cumplimiento con las políticas internas	16. Personas preparadas y motivadas	17. Cultura de innovación de producto y negocio	TOTAL	**VVALIDACIÓN**
OBJ. DE TI																				
8. Uso adecuado de aplicaciones, información y soluciones tecnológicas.		1	1	1			1	1		1		3			3		1	1	14	56
9. Agilidad de las TI		1	3	1			1		3			3		1	1		1	3	18	72
10. Seguridad de la información, infraestructura de procesamiento y aplicaciones				3	3			3											9	36
11. Optimización de activos, recursos y capacidades de las TI		3	1						1			1		1	1			1	9	36
12. Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio		1	3	1			1		1			3		1	1			1	13	52
13. Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.		3	1	1			1							3					9	36

CONTINÚA

Mapeando Objetivos Corporativos Vs Objetivos de TI	**OBJ. CORPORATIVOS**	1. Valor para los interesados de las inversiones de Negocio	2. Cartera de productos y servicios competitivos	3. Riesgos de negocio gestionados (salvaguarda de activos)	4. Cumplimiento de leyes y regulaciones externas	5. Transparencia financiera	6. Cultura de servicio orientada al cliente	7. Continuidad y disponibilidad del servicio del negocio	8. Respuestas ágiles a un entorno de negocio cambiante	9.Toma Estratégica de decisiones basadas en información	10. Optimización de costes de entrega de servicio	11. Optimización de la funcionalidad de los procesos del negocio	12. Optimización de los costos de los procesos del negocio	13. Programas gestionados de cambio en el negocio	14. Productividad operacional y de los empleados	15. Cumplimiento con las políticas internas	16. Personas preparadas y motivadas	17. Cultura de innovación de producto y negocio	TOTAL	**VALIDACIÓN**
OBJ. DE TI																				
14. Disponibilidad de información útil y relevante para la toma de decisiones		1	1	1	1			3		3		1							11	44
15. Cumplimiento de las políticas internas por parte de las TI				1	1														2	8
16. Personal del negocio y de las TI competente y motivado		1	1	3			1		1						3		3	1	14	56
17. Conocimiento, experiencia e iniciativas para la innovación de negocio		1	3				1		3	1		1		1			1	3	15	60

Tabla 7

Mapeo Objetivos de TI Vs Procesos DSS COBIT 5

Mapeo Objetivos de TI Vs Entregar, Soporte y Servicio		Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas.	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio	TOTAL
DSS01	Gestionar las Operaciones				3	1		3	1	1	1	3			1		1	1	16
DSS02	Gestionar las Peticiones y los Incidentes del Servicio				3			3	1		1				1			1	10
DSS03	Gestionar los Problemas				3	1		3	1	1		3	1		3			1	17
DSS04	Gestionar la Continuidad	1			3	1		3	1	1	1	1	1		3		1	1	18
DSS05	Gestionar los Servicios de Seguridad	2			3			1	1		3	1	1		1				13
DSS06	Gestionar los Controles de los Procesos del Negocio				2			3	1		1	1	1		1		1	1	12

Tabla 8

Ponderación de actividades del Proceso DSS COBIT 5

DSS01	**GESTIONAR OPERACIONES**			
DSS01 .01	**EJECUTAR PROCEDIMIENTOS OPERATIVOS**			
	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.	FB	HL	PROM
ACTIVIDADES	1. Desarrollar y mantener procedimientos operativos y actividades relacionadas para dar apoyo a todos los servicios entregados.	3	3	3
	2. Mantener una programación de actividades operativas, ejecutar las actividades y gestionar el desempeño y rendimiento (throughput) de las actividades programadas.	2	2	2
	3. Asegurar que se cumple con los estándares de seguridad aplicables para la recepción, procesamiento, almacenamiento y salida de datos de forma tal que se satisfagan los objetivos empresariales, la política de seguridad de la empresa y los requerimientos regulatorios.	3	3	3
	4. Verificar que todos los datos esperados para su procesamiento sean recibidos y procesados por completo y de una forma precisa y oportuna. Entregar los resultados de acuerdo con los requisitos de la empresa. Dar soporte a las necesidades de reinicio y reprocesamiento. Asegurar que los usuarios reciben los resultados adecuados de una forma segura y oportuna.	3	3	3
	5. Programar, realizar y registrar las copias de respaldo de acuerdo con las políticas y procedimientos establecidos.	3	3	3
PRAC DSS01 .02	**Gestionar servicios externalizados de TI.**			
	Gestionar la operación de servicios externalizados de TI para mantener la protección de la información empresarial y la confiabilidad de la entrega del servicio.	FB	HL	PROM
ACTIVIDADES	1. Asegurar que los procesos de información se adhieren a los requerimientos de seguridad de la empresa y conformes con los contratos y ANSs (Acuerdos de Nivel de Servicios) con terceros que alojan o proveen servicios.	3	3	3
	2. Asegurar que los requerimientos operativos del negocio y de procesamiento de TI, así como a las prioridades en la entrega del servicio se adhieren y son conformes a los contratos y ANSs con terceros que alojan o proveen servicios.	2	3	2,5
	3. Integrar los procesos críticos de gestión interna de TI con los de los proveedores de servicios externalizados cubriendo, por ejemplo, la planificación de la capacidad y el rendimiento, la gestión del cambio, la gestión de la configuración, la gestión de peticiones de servicio y de incidentes, la gestión de problemas, la gestión de la seguridad, la continuidad del negocio y la monitorización y notificación del desempeño de los procesos.	1	1	1
	4. Planificar la realización de auditorías y aseguramientos independiente de los entonos operativos de los proveedores de externalización (outsourcing) para confirmar que los requerimientos acordados están recibiendo el tratamiento adecuado.	1	2	1,5

CONTINÚA

PRAC DSS01 .03	**Supervisar la infraestructura de TI.**			
	Supervisar la infraestructura TI y los eventos relacionados con ella. Almacenar la suficiente información cronológica en los registros de operaciones para permitir la reconstrucción, revisión y examen de las secuencias de tiempo de las operaciones y las actividades relacionadas con el soporte a esas operaciones.	FB	HL	PROM
ACTIVIDADES	1. Registrar eventos, identificando el nivel de información a ser grabada sobre la base de una consideración del riesgo y el rendimiento.	3	3	3
	2. Identificar y mantener una lista de activos de infraestructura que necesiten ser monitorizados en base a la criticidad del servicio y la relación entre los elementos de configuración y los servicios que de ellos dependen.	3	3	3
	3. Definir e implantar reglas que identifiquen y registren violaciones de umbral y condiciones de eventos. Encontrar un equilibrio entre la generación de eventos falsos menores y eventos significativos, de forma tal que los registros de eventos no estén sobrecargados con información innecesaria.	3	3	3
	4. Producir registros de eventos y retenerlos por un periodo apropiado para asistir en investigaciones futuras.	3	2	2,5
	5. Establecer procedimientos para supervisar los registros de eventos y llevar a cabo revisiones periódicas.	3	2	2,5
	6. Asegurar que se crean oportunamente los tiques de incidente cuando la monitorización identifica desviaciones de los umbrales definidos.	1	2	1,5
PRAC DSS01 .04	**Gestionar el entorno.**			
	Mantener las medidas para la protección contra factores ambientales. Instalar equipamiento y dispositivos especializados para supervisar y controlar el entorno.	FB	HL	PROM
ACTIVIDADES	1. Identificar desastres naturales y causados por el ser humano que puedan ocurrir en el área donde se encuentran las instalaciones de TI. Evaluar el efecto potencial en las instalaciones de TI.	3	3	3
	2. Identificar de qué manera el equipamiento de TI, incluyendo el equipamiento móvil y el ubicado fuera de las instalaciones, está protegido contra las amenazas del entorno. Asegurar que la política limite o impida comer, beber y fumar en áreas sensibles y que se prohíba el almacenamiento de material de oficina y otros suministros que puedan representar un riesgo de incendio en los centros de procesamiento de datos.	3	3	3
	3. Ubicar y construir las instalaciones de TI para minimizar y mitigar la susceptibilidad ante las amenazas del entorno.	3	3	3
	4. Supervisar y mantener de forma periódica a los dispositivos que detectan proactivamente las amenazas del entorno (p. ej. fuego, agua, humo, humedad).	3	3	3

CONTINÚA

	5. Responder a las alarmas y otras notificaciones del entorno. Documentar y probar los procedimientos, lo que debería incluir la priorización de alarmas y el contacto con las autoridades locales de respuesta ante emergencias y entrenar al personal en estos procedimientos.	3	3	3
	6. Comparar medidas y planes de contingencia respecto a los requerimientos de las pólizas de seguros e informar de los resultados. Atender a los puntos de no-conformidad de manera oportuna.	2	3	2,5
	7. Asegurar que los sitios de TI están construidos y diseñados para minimizar el impacto del riesgo del entorno (p.ej. robo, aire, fuego, humo, agua, vibración, terrorismo, vandalismo, productos químicos, explosivos). Considerar zonas específicas de seguridad o celdas a prueba de incendio (p. ej. ubicando los entornos/servidores de producción y de desarrollo alejados entre sí).	3	3	3
	8. Mantener en todo momento a los sitios de TI y las salas de servidores limpias y en una condición segura (es decir, sin desorden, sin papel ni cajas de cartón, sin papeleras llenas, sin productos químicos o materiales inflamables).	3	3	3
PRAC DSS01 .05	**Gestionar las instalaciones.**			
	Gestionar las instalaciones, incluyendo equipos de electricidad y comunicaciones, en línea con las leyes y regulaciones, requerimientos técnicos y de negocio y directrices de salud y seguridad en el trabajo.	FB	HL	PROM
ACTIVIDADES	1. Examinar los requerimientos de las instalaciones de TI respecto de la protección frente a la fluctuación y cortes de la energía eléctrica, en relación con otros requerimientos de la planificación de la continuidad del negocio. Disponer de equipamiento adecuado de alimentación ininterrumpida (p. ej. baterías, generadores) para dar soporte a la planificación de continuidad del negocio.	3	3	3
	2. Probar periódicamente los mecanismos del sistema de alimentación ininterrumpida (SAI) y asegurar que la electricidad puede ser conmutada al sistema sin efectos significativos en las operaciones del negocio.	3	2	2,5
	3. Asegurar que las instalaciones que alojan los sistemas de TI tienen más de un proveedor para los servicios públicos indispensables (p. ej. Electricidad, telecomunicaciones, agua, gas). Separar la acometida de cada servicio.	3	3	3
	4. Confirmar que el cableado externo al sitio TI está bajo tierra o que tiene una protección alternativa adecuada. Determinar que el cableado en el sitio TI está contenido en conductos asegurados y que los armarios de cableado tienen su acceso restringido al personal autorizado. Proteger adecuadamente al cableado contra el daño causado por fuego, humo, agua, interceptación e interferencia.	3	3	3
	5. Asegurar que el cableado y el patching físico (datos y telefonía) están estructurados y organizados. Las estructuras de cableado y de conductos debieran estar documentadas (p.ej. plano del edificio y diagramas de cableado).	3	3	3

CONTINÚA

	6. Analizar las instalaciones que alojan los sistemas de alta disponibilidad para verificar el cumplimiento de los requerimientos de cableado (externo e interno) en cuanto a redundancia y tolerancia a fallos.	3	3	3
	7. Asegurar que los sitios e instalaciones de TI cumplen de manera sistemática con la legislación, regulaciones, directrices y especificaciones relevantes de salud y seguridad en el trabajo.	1	2	1,5
	8. Proporcionar periódicamente formación al personal en la legislación, regulaciones y directrices relevantes de salud y seguridad en el trabajo. Capacitar al personal en simulacros de incendio y rescate para asegurar el adecuado conocimiento y las acciones apropiadas a tomar en caso de incendio o incidentes similares.	1	2	1,5
	9. Registrar, supervisar, gestionar y resolver incidentes en las instalaciones siguiendo los procesos de gestión de incidentes de TI. Poner a disposición informes sobre incidentes en instalaciones donde la legislación y las regulaciones requieran su divulgación.	1	2	1,5
	10. Asegurar que los sitios y el equipamiento de TI son mantenidos de acuerdo con los intervalos de servicio y las especificaciones recomendados por el proveedor. El mantenimiento debe ser realizado únicamente por personal autorizado.	2	2	2
	11. Analizar las alteraciones físicas a los sitios o localizaciones de TI para reevaluar el riesgo del entorno (p.ej. daño por fuego o agua). Informar los resultados de este análisis a los niveles directivos de continuidad de negocio y de gestión de edificios.	2	2	2
DSS03	**GESTIONAR PROBLEMAS**			
PRAC DSS03 .01	**Identificar y clasificar problemas.**			
	Definir e implementar criterios y procedimientos para informar de los problemas identificados, incluyendo clasificación, categorización y priorización de problemas.	FB	HL	PROM
ACTIVIDADES	1. Identificar problemas a través de la correlación de informes de incidentes, registros de error y otros recursos de identificación de problemas. Determinar niveles de prioridad y categorización para dedicarse a la resolución de problemas en tiempo basándose en los riesgos de negocio y en la definición del servicio.	2	2	2
	2. Manejar formalmente todos los problemas con acceso a todos los datos relevantes, incluyendo información sobre el sistema de gestión de cambios y los detalles de incidentes sobre configuración/activos TI.	3	2	2,5
	3. Definir grupos de soporte adecuados para ayudar en la identificación de problemas, en el análisis de la causa raíz, y en la determinación de la solución, para respaldar la gestión de problemas. Determinar grupos de soporte basados en categorías predefinidas, tales como hardware, redes, software, aplicaciones y software de soporte.	3	3	3

CONTINÚA

	4. Definir niveles de prioridad mediante consultas con el negocio para asegurar que la identificación de problemas y el análisis de la causa raíz se llevan a cabo a tiempo de acuerdo con los ANSs acordados. Basar los niveles de prioridad en el impacto en el negocio y en la urgencia.	1	1	1
	5. Informar del estado de problemas identificados al centro de servicios de forma que los clientes y la gestión de TI pueden mantenerse informados.	3	3	3
	6. Mantener un catálogo de gestión de problemas único para registrar e informar sobre problemas identificados y para establecer pistas de auditoría sobre los procesos de gestión de problemas, incluyendo el estado de cada problema (p. ej., abierto, reabierto, en progreso o cerrado).	3	3	3
PRAC DSS03 .02	**Investigar y diagnosticar**			
	Investigar y diagnosticar problemas utilizando expertos en las materias relevantes para valorar y analizar las causas raíz.	FB	HL	PROM
ACTIVIDADES	1. Identificar problemas que pueden ser errores conocidos comparando datos de incidentes con la base de datos de errores conocidos y posibles (p. ej., los comunicados por los proveedores externo) y clasificar problemas como errores conocidos.	2	2	2
	2. Asociar los elementos de configuración afectados con el error conocido/establecido.	1	1	1
	3. Producir informes para comunicar el progreso de la resolución de problemas y para supervisar el impacto continuado de los problemas no resueltos. Supervisar el estado del proceso de gestión de problemas a través de su ciclo de vida, incluyendo aportaciones de la gestión de cambios y de configuración.	3	2	2,5
PRAC DSS03 .03	**Levantar errores conocidos.**			
	Tan pronto como las causas raíz de los problemas se hayan identificado, crear registros de errores conocidos y una solución temporal apropiada, e identificar soluciones potenciales.	FB	HL	PROM
ACTIVIDADES	1. Tan pronto como las causas raíz de los problemas se han identificado, crear registros de errores conocidos y desarrollar una solución temporal adecuada.	3	3	3
	2. Identificar, evaluar, priorizar y procesar (a través de la gestión de cambios) soluciones a los errores conocidos basándose en un caso de negocio coste-beneficio y en el impacto de negocio y la urgencia.	3	3	3
PRAC DSS03 .04	**Resolver y cerrar problemas.**			
	Identificar e iniciar soluciones sostenibles refiriéndose a la causa raíz, levantando peticiones de cambio a través del proceso de gestión de cambios establecido si se requiere para resolver errores. Asegurarse de que el personal afectado está al tanto de las acciones tomadas y de los planes desarrollados para prevenir que vuelvan a ocurrir futuros incidentes.	FB	HL	PROM

CONTINÚA

ACTIVIDADES	1. Cerrar registros de problemas, bien después de la confirmación de la eliminación satisfactoria del error conocido, bien tras acordar con el negocio cómo gestionar el problema de una manera alternativa.	1	2	1,5
	2. Informar al centro de servicio del calendario de cierre del problema, p. ej., del calendario para solucionar los errores conocidos, la posible solución alternativa o el hecho de que el problema permanecerá hasta que el cambio se haya implementado, y las consecuencias de la solución escogida. Mantener adecuadamente informados a los usuarios y a los clientes afectados.	2	2	2
	3. A través del proceso de resolución, obtener informes periódicos de gestión de cambios acerca del progreso en la resolución de problemas y errores.	3	2	2,5
	4. Supervisar el continuo impacto de los problemas y errores conocidos en los servicios.	3	3	3
	5. Revisar y confirmar la resolución satisfactoria de problemas graves.	3	3	3
	6. Asegurar que el conocimiento aprendido de esta revisión se incorpora en una reunión de revisión del servicio con el cliente de negocio.	3	3	3
PRAC DSS03 .05	**Realizar una gestión de problemas proactiva.**			
	Recoger y analizar datos operacionales (especialmente registros de incidentes y cambios) para identificar tendencias emergentes que puedan indicar problemas. Registrar problemas para permitir la valoración.	FB	HL	PRO M
ACTIVIDADES	1. Capturar información de problemas relacionada con cambios e incidentes TI y comunicarla a las partes interesadas clave. Esta comunicación podría tomar la forma de informes y reuniones periódicas entre los responsables de los procesos de gestión de incidentes, problemas, cambios y configuración para considerar problemas recientes y acciones correctivas potenciales.	3	3	3
	2. Asegurar que los responsables de los procesos y los responsables de gestión de incidentes, problemas, cambios y configuración se reúnen regularmente para discutir problemas conocidos y cambios futuros planificados.	3	3	3
	3. Permitir a la empresa supervisar los costes totales de problemas, capturar esfuerzos de cambio resultantes de las actividades del proceso de gestión de problemas (p. ej., soluciones a problemas y errores conocidos) e informar de ellos.	3	3	3
	4. Producir informes para supervisar la resolución de problemas respecto a los requisitos de negocio y ANSs. Asegurar el adecuado escalado de problemas, p. ej., escalado a un nivel de gestión superior de acuerdo con los criterios acordados, contactando proveedores externos, o enviando al comité de gestión de cambios para incrementar la prioridad de una petición de cambio urgente para implementar una solución temporal.	1	2	1,5
	5. Optimizar el uso de recursos y reducir las soluciones temporales y hacer seguimiento de las tendencias de problemas.	2	2	2
	6. Identificar e iniciar soluciones sostenibles (soluciones permanentes) identificando la causa raíz, y levantar peticiones de cambio a través de los procesos de gestión de cambios establecidos.	3	2	2,5

CONTINÚA

DSS04	**GESTIONAR LA CONTINUIDAD**			
PRAC DSS04 .01	**Definir la política de continuidad de negocio, objetivos y alcance.**			
	Definir la política y alcance de continuidad de negocio alineada con los objetivos de negocio y de las partes interesadas.	FB	HL	PROM
ACTIVIDADES	1. Identificar procesos de negocio internos y subcontratados y actividades de servicio que son críticas para las operaciones de la empresa o necesarias para cumplir con las obligaciones legales y/o contractuales.	3	3	3
	2. Identificar las partes interesadas clave y los roles y responsabilidades para definir y acordar la política de continuidad y su alcance.	3	3	3
	3. Definir y documentar los objetivos y el alcance mínimos acordados de la política de continuidad del negocio e imbricar la planificación de continuidad en la cultura empresarial.	3	3	3
	4. Identificar procesos de soporte al negocio esenciales y servicios TI relacionados.	3	3	3
PRAC DSS04 .02	**Mantener una estrategia de continuidad.**			
	Evaluar las opciones de gestión de la continuidad de negocio y escoger una estrategia de continuidad viable y efectiva en coste, que pueda asegurar la continuidad y recuperación de la empresa frente a un desastre u otro incidente mayor o disrupción.	FB	HL	PROM
ACTIVIDADES	1. Identificar escenarios potenciales probables que puedan dar pie a eventos que puedan causar incidentes disruptivos importantes.	3	3	3
	2. Realizar un análisis de impacto en el negocio para evaluar el impacto en tiempo de una disrupción en funciones críticas del negocio y el efecto que tendría en ellas.	2	2	2
	3. Establecer el tiempo mínimo necesario para recuperar un proceso de negocio y su soporte de TI, basándose en una duración aceptable de interrupción del negocio y la interrupción máxima tolerable.	1	2	1,5
	4. Analizar la probabilidad de amenazas que puedan causar pérdidas de continuidad de negocio e identificar medidas que puedan reducir la probabilidad y el impacto, mejorando la prevención e incrementando la resiliencia.	1	2	1,5
	5. Analizar los requerimientos de continuidad para identificar las posibles estrategias de negocio y opciones técnicas.	3	2	2,5
	6. Determinar las condiciones y los responsables de decisiones clave que puedan causar la invocación de los planes de continuidad.	3	2	2,5
	7. Identificar los requerimientos de recursos y costes para cada opción técnica estratégica y realizar recomendaciones estratégicas.	3	2	2,5
	8. Obtener la aprobación de los ejecutivos de negocio para las opciones estratégicas seleccionadas.	3	3	3

CONTINÚA

PRAC DSS04 .03	**Desarrollar e implementar una respuesta a la continuidad del negocio.**			
	Desarrollar un plan de continuidad de negocio (BCP) basado en la estrategia que documente los procedimientos y la información lista para el uso en un incidente para facilitar que la empresa continúe con sus actividades críticas	FB	HL	PROM
ACTIVIDADES	1. Definir las acciones y comunicaciones de respuesta a incidentes que deben ser realizadas en un evento de disrupción. Definir los roles y responsabilidades relacionados, incluyendo la responsabilidad para la política y la implementación.	3	3	3
	2. Desarrollar y mantener planes de continuidad de negocio operativos que contengan los procedimientos que deben ser seguidos para permitir continuar operando los procesos críticos de negocio y/o planes temporales de proceso, incluyendo enlaces a los planes de proveedores de servicio externalizados.	3	3	3
	3. Asegurar que los proveedores y socios externos clave tengan implantados planes de continuidad efectivos. Obtener evidencias auditadas si es necesario.	2	2	2
	4. Definir las condiciones y procedimientos de recuperación que permitan la reanudación de los procesos de negocio, incluyendo la actualización y conciliación de las bases de datos para preservar la integridad de la información.	3	3	3
	5. Definir y documentar los recursos necesarios para soportar los procedimientos de continuidad y recuperación, considerando personas, instalaciones e infraestructura de TI.	3	3	3
	6. Definir y documentar los requerimientos de información de respaldo para soportar los planes, incluyendo planes y documentos en papel así como ficheros de datos y considerar las necesidades de seguridad y almacenamiento en otra ubicación.	3	3	3
	7. Determinar las habilidades necesarias para los individuos implicados en la ejecución de los planes y procedimientos.	3	3	3
	8. Distribuir los planes y la documentación de soporte de modo seguro a las partes interesadas y apropiadamente autorizadas y asegurar que estén accesibles en escenarios de desastre.	3	3	3
PRAC DSS04 .04	**Ejercitar, probar y revisar el BCP.**			
	Probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera.	FB	HL	PROM
ACTIVIDADES	1. Definir los objetivos para ejercitar y probar los sistemas del plan (de negocio, técnicos, logísticos, administrativos, procedimentales y operacionales) para verificar la completitud del plan de continuidad de negocio (BCP) para enfrentarse a los riesgos de negocio.	3	3	3
	2. Definir y acordar ejercicios que sean razonables con las partes interesadas, validar los procedimientos de continuidad, e incluir roles y responsabilidades y acuerdos de retención de datos que ocasionen la mínima disrupción en los procesos de negocio.	2	2	2
	3. Asignar roles y responsabilidades para realizar ejercicios y pruebas del plan de continuidad.	1	2	1,5

CONTINÚA

	4. Planificar ejercicios y actividades de prueba tal como esté definido en el plan de continuidad.	1	2	1,5
	5. Realizar un análisis y revisión post-ejercicio para considerar el logro.	1	1	1
	6. Desarrollar recomendaciones para mejorar el plan de continuidad actual en base a los resultados de la revisión.	1	2	1,5
PRAC DSS04 .05	**Revisar, mantener y mejorar el plan de continuidad.**			
	Realizar una revisión por la Dirección de la capacidad de continuidad a intervalos regulares para asegurar su continua idoneidad, adecuación y efectividad. Gestionar los cambios en el plan de acuerdo al proceso de control de cambios para asegurar que el plan de continuidad se mantiene actualizado y refleja continuamente los requerimientos actuales del negocio.	FB	HL	PROM
ACTIVIDADES	1. Revisar el plan y la capacidad de continuidad de forma regular frente a las asunciones hechas y los objetivos de negocio actuales, tanto estratégicos como operativos.	2	2	2
	2. Considerar si es necesario una revisión del análisis de impacto en el negocio, dependiendo en la naturaleza de los cambios.	1	2	1,5
	3. Recomendar y comunicar los cambios en la política, planes, procedimientos, infraestructura, roles y responsabilidades para la aprobación de la dirección y su realización mediante el proceso de gestión de cambios.	2	2	2
	4. Revisar el plan de continuidad regularmente para considerar el impacto de cambios nuevos o mayores en: organización de la empresa, procesos de negocio, acuerdos de externalización, tecnologías, infraestructura, sistemas operativos y sistemas de aplicaciones.	1	1	1
PRAC DSS04 .06	**Proporcionar formación en el plan de continuidad.**			
	Proporcionar a todas las partes implicadas, internas y externas, de sesiones formativas regulares que contemplen los procedimientos y sus roles y responsabilidades en caso de disrupción.	FB	HL	PROM
ACTIVIDADES	1. Definir y mantener los planes y requerimientos de formación para quienes realicen de manera continuada planificación de la continuidad, análisis de impacto, evaluaciones de riesgos, comunicación con los medios y respuesta a incidentes. Asegurar que los planes de formación consideren la frecuencia de formación y los mecanismos de entrega de la formación.	1	1	1
	2. Desarrollar competencias basadas en formación práctica que incluyan la participación en ejercicios y pruebas.	1	1	1
	3. Supervisar habilidades y competencias basándose en los resultados de los ejercicios y las pruebas.	1	1	1
PRAC DSS04 .07	**Gestionar acuerdos de respaldo.**			
	Mantener la disponibilidad de la información crítica del negocio.	FB	HL	PROM
ACTIVIDADES	1. Hacer copias de seguridad de sistemas, aplicaciones, datos y documentación de acuerdo a una planificación definida, considerando:	3	3	3
	• Frecuencia (mensual, semanal, diaria, etc.)			

CONTINÚA

	• Modo de copias de seguridad (por ejemplo, discos espejo para copias de seguridad en tiempo real frente a DVD-ROM para retenciones de larga duración). • Tipo de copias de seguridad (por ejemplo, completa frente a incremental) • Tipo se soporte • Copias de seguridad automatizadas en línea • Tipos de datos (por ejemplo, voz, óptica) • Creación de registros • Datos de cálculos críticos de usuario final (por ejemplo, hojas de cálculo) • Localización física y lógica de las fuentes de los datos • Seguridad y derechos de acceso • Cifrado			
	2. Asegurar que los sistemas, aplicaciones, datos y documentación mantenidos o procesados por terceras partes están adecuadamente respaldados o asegurados de otra forma. Considerar el hecho de requerir el retorno de las copias de seguridad de terceras partes. Considerar acuerdos de depósito (escrow).	3	3	3
	3. Definir los requerimientos del almacenamiento de las copias de seguridad, dentro y fuera de la propia ubicación, que satisfagan los requerimientos del negocio. Considerar la accesibilidad requerida a las copias de seguridad.	3	3	3
	4. Extender la concienciación y la formación en Planes de Continuidad de Negocio (BCP).	3	3	3
	5. Probar y mantener legibles las copias de seguridad y las archivadas periódicamente.	3	3	3
PRAC DSS04 .08	**Ejecutar revisiones post-reanudación.**			
	Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.	FB	HL	PROM
ACTIVIDADES	1. Evaluar la observancia del Plan de Continuidad de Negocio (BCP) documentado.	2	3	2,5
	2. Determinar la efectividad del plan, capacidades de continuidad, roles y responsabilidades, habilidades y competencias, resiliencia a incidentes, infraestructura técnica y estructuras organizativas y relaciones.	2	2	2
	3. Identificar debilidades u omisiones en el plan y las capacidades y hacer recomendaciones para la mejora.	2	2	2
	4. Obtener la aprobación de la dirección para los cambios en el plan y aplicarlos mediante el proceso de control de cambios de la empresa.	2	2	2

CONTINÚA

DSS05	**GESTIONAR SERVICIOS DE SEGURIDAD**			
DSS05.01	Proteger contra software malicioso (malware)			
	Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, software espía –spyware- y correo basura).	FB	HL	PROM
ACTIVIDADES	1. Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención.	3	3	3
	2. Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automáticamente).	3	3	3
	3. Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.	3	3	3
	4. Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad).	3	3	3
	5. Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de phishing).	3	3	3
	6. Realizar formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado.	3	3	3
PRAC DSS05.02	**Gestionar la seguridad de la red y las conexiones.**			
	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.	FB	HL	PROM
ACTIVIDADES	1. Basándose en el análisis de riesgos y en los requerimientos del negocio, establecer y mantener una política de seguridad para las conexiones.	3	3	3
	2. Permitir sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa. Configurar estos dispositivos para forzar la solicitud de contraseña.	3	3	3
	3. Implementar mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.	3	3	3
	4. Cifrar la información en tránsito de acuerdo con su clasificación.	2	2	2
	5. Aplicar los protocolos de seguridad aprobados a las conexiones de red.	2	3	2,5
	6. Configurar los equipamientos de red de forma segura.	3	3	3
	7. Establecer mecanismos de confianza para dar soporte a la transmisión y recepción segura de información.	3	3	3
	8. Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.	3	3	3
	9. Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.	3	3	3

CONTINÚA

PRAC DSS05. 03	**Gestionar la seguridad de los puestos de usuario final.**			
	Asegurar que los puestos de usuario final (es decir, portátil, equipo sobremesa, servidor y otros dispositivos y software móviles y de red) están asegurados a un nivel que es igual o mayor al definido en los requerimientos de seguridad de la información procesada, almacenada o transmitida.	FB	HL	PROM
ACTIVIDADES	1. Configurar los sistemas operativos de forma segura.	3	3	3
	2. Implementar mecanismos de bloqueo de los dispositivos.	3	3	3
	3. Cifrar la información almacenada de acuerdo a su clasificación.	3	3	3
	4. Gestionar el acceso y control remoto.	3	3	3
	5. Gestionar la configuración de la red de forma segura.	3	3	3
	6. Implementar el filtrado del tráfico de la red en dispositivos de usuario final.	3	3	3
	7. Proteger la integridad del sistema.	3	3	3
	8. Proveer de protección física a los dispositivos de usuario final.	3	3	3
	9. Deshacerse de los dispositivos de usuario final de forma segura.	3	3	3
PRAC DSS05.0 4	**Gestionar la identidad del usuario y el acceso lógico.**			
	Asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio.	FB	HL	PROM
ACTIVIDADES	1. Mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad de tener y necesidad de conocer.	3	3	3
	2. Identificar unívocamente todas las actividades de proceso de la información por roles funcionales, coordinando con las unidades de negocio y asegurando que todos los roles están definidos consistentemente, incluyendo roles definidos por el propio negocio en las aplicaciones de procesos de negocio.	3	3	3
	3. Autenticar todo acceso a los activos de información basándose en su clasificación de seguridad, coordinando con las unidades de negocio que gestionan la autenticación con aplicaciones usadas en procesos de negocio para asegurar que los controles de autenticación han sido administrados adecuadamente.	3	3	3
	4. Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados.	3	3	3
	5. Segregar y gestionar cuentas de usuario privilegiadas.	3	3	3
	6. Realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.	3	3	3
	7. Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicaciones de negocio, infraestructura de TI, operaciones de sistema, desarrollo y mantenimiento) son identificables unívocamente. Identificar unívocamente todas las actividades de proceso de información por usuario.	3	3	3

CONTINÚA

	8. Mantener una pista de auditoría de los accesos a la información clasificada como altamente sensible.	3	3	3
PRAC DSS05. 05	**Gestionar el acceso físico a los activos de TI.**			
	Definir e implementar procedimientos para conceder, limitar y revocar acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a locales, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Esto aplicará a todas las personas que entren en los locales, incluyendo empleados, empleados temporales, clientes, vendedores, visitantes o cualquier otra tercera parte.	FB	HL	PROM
ACTIVIDADES	1. Gestionar las peticiones y concesiones de acceso a las instalaciones de procesamiento. Las peticiones formales de acceso deben ser completadas y autorizadas por la dirección de la ubicación de TI, y guardado el registro de petición. Los formularios deberían identificar específicamente las áreas a las que el individuo tiene acceso concedido.	2	3	2,5
	2. Asegurar que los perfiles de acceso están actualizados. El acceso a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) debe basarse en funciones de trabajo y responsabilidades.	3	3	3
	3. Registrar y supervisar todos los puntos de entrada a las ubicaciones de TI. Registrar todos los visitantes de la ubicación, incluyendo contratistas y vendedores.	3	3	3
	4. Instruir a todo el personal para mantener visible la identificación en todo momento. Prevenir la expedición de tarjetas o placas de identidad sin la autorización adecuada.	3	3	3
	5. Escoltar a los visitantes en todo momento mientras estén en la ubicación. Si se encuentra a un individuo que no va acompañado, que no resulta familiar y que no lleva visible la identificación de empleado, se deberá alertar al personal de seguridad.	2	2	2
	6. Restringir el acceso a ubicaciones de TI sensibles estableciendo restricciones en el perímetro, tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores. Asegurar que los dispositivos registren el acceso y disparen una alama en caso de acceso no autorizado. Ejemplos de estos dispositivos incluyen placas o tarjetas llave, teclados (keypads), circuitos cerrados de televisión y escáneres biométricos.	3	3	3
	7. Realizar regularmente formación de concienciación de seguridad física.	3	3	3
PRAC DSS05. 06	**Gestionar documentos sensibles y dispositivos de salida.**			
ACTIVIDADES	Establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para activos de TI sensibles, tales como formularios especiales, títulos negociables, impresoras de propósito especial o credenciales (*token*) de seguridad.	FB	HL	PROM
	1. Establecer procedimientos para gobernar la recepción, uso, eliminación y destrucción de formularios especiales y	1	2	1,5

CONTINÚA

	dispositivos de salida, dentro, en y fuera de la empresa.			
	2. Asignar privilegios de acceso a documentos sensibles y dispositivos de salida basados en el principio del menor privilegio, equilibrando riesgo y requerimientos de negocio.	3	3	3
	3. Establecer un inventario de documentos sensibles y dispositivos de salida, y realizar regularmente conciliaciones.	1	1	1
	4. Establecer salvaguardas físicas apropiadas sobre formularios especiales y dispositivos sensibles.	1	1	1
	5. Destruir la información sensible y proteger dispositivos de salida (por ejemplo, desmagnetizando soportes magnéticos, destruir físicamente dispositivos de memoria, poniendo trituradoras o papeleras cerradas disponibles para destruir formularios especiales y otros documentos confidenciales).	3	2	2,5
PRAC DSS05. 07	**Supervisar la infraestructura para detectar eventos relacionados con la seguridad.**			
	Usando herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.	FB	HL	PROM
ACTIVIDADES	1. Registrar los eventos relacionados con la seguridad reportados por las herramientas de monitorización de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse en base a la consideración de riesgo. Retenerla por un periodo apropiado para asistir en futuras investigaciones.	3	3	3
	2. Definir y comunicar la naturaleza y características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos para permitir una respuesta conmensurada.	2	2	2
	3. Revisar regularmente los registros de eventos para detectar incidentes potenciales.	2	2	2
	4. Mantener un procedimiento para la recopilación de evidencias en línea con los procedimientos de evidencias forenses locales y asegurar que todos los empleados están concienciados de los requerimientos.	2	2	2
	5. Asegurar que los tiques de incidentes de seguridad se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales.	1	2	1,5

3.5 REQUERIMIENTOS ESPECÍFICOS A EVALUAR

Tabla 9

Requerimientos específicos a evaluar UTIC

REQUERIMIENTOS ESPECÍFICOS DE UTIC	CUMPLIMIENTO		EVIDENCIA		
	SI/NO		Cod.	Tipo	Documento
GESTIONAR OPERACIONES					
Ejecutar procedimientos operativos					
1.Plan Operativo en uso		NO			
2. Procedimientos operativos.		NO			
3. Programación de actividades operativas.	SI		E001	DIGITAL	PLANIFICACIÓN UTIC 2014
4. Políticas de seguridad y requerimientos regulatorios.		NO	IN-CH-UTIC-005	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN
5. Cronograma de copias de respaldo.		NO			
6. Registros de copias de respaldos.		NO			
Gestionar servicios externalizados de TI.					
1. Identificación y registro de procesos críticos.		NO	E010	DIGITAL	PLAN DE CONTINGENCIA 2014
2. Están asegurados los procesos de información conformes con los contratos y ANSs con terceros que alojan o proveen servicios.		NO			

CONTINÚA

Supervisar la infraestructura de TI.						
1. Registro de eventos.			NO			
2. Lista de activos de infraestructura			NO			
3. Registro de monitoreo de equipos:						
	Alimentación ininterrumpida	SI		E008	DIGITAL	MONITOREO SISTEMA ENERGÍA ELECTRICA, GENERADOR
	Data Center	SI		E008	DIGITAL	MONITOREO SISTEMA ENERGÍA ELECTRICA, GENERADOR
4. Registro de supervisión de eventos.			NO			
Gestionar el entorno.						
	Dispone de detectores de Humo.	SI		IN-CH-UTIC-001	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN
	Dispone de extintores.	SI		IN-CH-UTIC-001, EF-0018	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN
	- CO2 para servidores y PCs. - Polvo químico para archiveros de documentos.	SI		IN-CH-UTIC-001	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN
	Dispone de hidrantes cercanos.		NO	IN-CH-UTIC-001	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN
	Dispone de cámaras de seguridad.	SI		IN-CH-UTIC-001	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN
	Dispone de personal de seguridad.	SI		IN-CH-UTIC-001	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN

CONTINÚA

	Dispone alarmas de seguridad.	SI		IN-CH-UTIC-001, EF-020	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN
	Dispone con iluminación adecuada y con iluminación de emergencia en casos de contingencia.	SI		IN-CH-UTIC-001, EF-019	IMPRESO DIGITAL	PRUEBAS SUSTANTIVAS OBSERVACIÓN
	Dispone de cubre ventanas metálicos para planta baja en instalaciones de TI.	SI		IN-CH-UTIC-001	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN
	Dispone de cuartos fríos para servidores.	SI		IN-CH-UTIC-001	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN
	Dispone de zonas contra incendios para servidores.	SI		IN-CH-UTIC-001	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN
	Dispone de detectores de metales y explosivos.		NO	IN-CH-UTIC-001	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN
	Se encuentran los servidores de producción y desarrollos alejados entre sí.		NO	IN-CH-UTIC-001	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN
	Existe protección física para el equipamiento de TI, incluyendo el equipamiento móvil y el ubicado fuera de las instalaciones.		NO	IN-CH-UTIC-001 EF-021	IMPRESO DIGITAL	PRUEBAS SUSTANTIVAS OBSERVACIÓN
	Biométrico	SI		IN-CH-UTIC-001-2	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN
				EF-012 EF-013	DIGITAL DIGITAL	BIOMÉTRICO DATA CENTER Y UTIC
	Reconocimiento facial		NO	IN-CH-UTIC-001-2	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN

CONTINÚA

	código de barras		NO	IN-CH-UTIC-001-2	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN
	Banda magnética	SI		IN-CH-UTIC-001-2	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN
	Registro de visitas al Data Center	SI		IN-CH-UTIC-001-2	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN
3. Señalética en Instalaciones de TI.						
	Señalética informativa (Ejm: asuntos, horarios, recorridos, instrucciones)	SI		IN-CH-UTIC-001-2, EF-014	IMPRESO DIGITAL	PRUEBAS SUSTANTIVAS OBSERVACIÓN
	Señalética preventiva (alerta sobre peligros posibles para el usuario. Ejm: cuidado pisos húmedos).		NO	IN-CH-UTIC-001-2	IMPRESO DIGITAL	PRUEBAS SUSTANTIVAS OBSERVACIÓN
	Señalética restrictivas (especifican límites de acción para el usuario. Ejm: solo personal autorizado).	SI		IN-CH-UTIC-001-2	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN
	Señalética prohibitivas (imponen la prohibición de determinadas acciones. Ejm: prohibido comer en este lugar).	SI		IN-CH-UTIC-001-2	IMPRESO DIGITAL	PRUEBAS SUSTANTIVAS OBSERVACIÓN
	Señalética de seguridad (Ejm: salida de emergencia)	SI		IN-CH-UTIC-001-2, EF-016	IMPRESO DIGITAL	PRUEBAS SUSTANTIVAS OBSERVACIÓN
4. Ubicación de las Instalaciones de TI.						
	Primer Piso()	SI		EF-002, EF003	DIGITAL	INSTALACIONES UTIC
	Segundo Piso()		NO			
	Tercer Piso()		NO			

CONTINÚA

	Cuarto Piso()		NO			
	Otro()		NO			
	Fuego		NO			
	Agua		NO			
	Humo		NO			
	Humedad		NO			
6. Lista de autoridades locales y de respuesta ante emergencias.		SI		EF-011	DIGITAL	CONTACTOS DE EMERGENCIA
	Desorden	SI		EF-008	DIGITAL	DESORDEN EN ENTORNOS UTIC
	Papeles	SI				
	Cajas de cartón		NO			
	Papeleras llenas		NO			
	Productos químicos	SI		EF-007	DIGITAL	PRODUCTOS QUÍMICOS
	Materiales inflamables		NO			
Gestionar las instalaciones.						
	UPS (baterías) o generadores	SI		EF-004 IN-CH-UTIC-002	DIGITAL IMPRESO	GENERADOR UTIC
	Planta de emergencia.		NO	IN-CH-UTIC-002	IMPRESO	CUESTIONARIO
	Acometidas separadas para cada servicio.	SI		IN-CH-UTIC-002	IMPRESO	CUESTIONARIO
	Cableado externo al sitio TI bajo tierra.	SI		EF-006 IN-CH-UTIC-002	DIGITAL IMPRESO	CUARTO DE MANDO CALBEADO EXTERNO
	Protección alternativa (conductos asegurados o armarios).	SI		EF-005 IN-CH-UTIC-002	DIGITAL IMPRESO	PROTECCIÓN ALTERNATIVA EQUIPOS
	Dispone de instalación eléctrica específicamente	SI		IN-CH-UTIC-002	IMPRESO	CUESTIONARIO

CONTINÚA

	para centros de cómputo e instalaciones de TI.					
	La acometida llega a un tablero de distribución.	SI		IN-CH-UTIC-002	IMPRESO	CUESTIONARIO
	El tablero de distribución está en la sala, visible y accesible.	SI		IN-CH-UTIC-002	IMPRESO	CUESTIONARIO
	Se cuenta con interruptores por secciones o aulas.	SI		IN-CH-UTIC-002	IMPRESO	CUESTIONARIO
2.Registros periódicos de los mecanismos del sistema de alimentación ininterrumpida (SAI)		SI		E008	DIGITAL	MONITOREO SISTEMA ENERGÍA ELÉCTRICA GENERADOR
	Electricidad	SI		E010	DIGITAL	PLAN DE CONTINGENCIA 2014
	Agua		NO			
	Telecomunicaciones	SI		E010	DIGITAL	PLAN DE CONTINGENCIA 2014
	Para datos	SI				
	Para telefonía	SI				
	Dispone de cableado estructurado	SI		EF-022	DIGITAL	
	Existe organización en el cableado.		NO	EF-010	DIGITAL	
	Codificación en los RACKS.	SI		IN-CH-UTIC-002	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN
5. Diagramas de cableado de la ESPE			NO	E003	DIGITAL	ESTRUCTURA DE LA RED 2014
6. Plan de mantenimiento de equipamiento de TI			NO	E001	DIGITAL	PLANIFICACIÓN UTIC 2014

CONTINÚA

7.Registro de mantenimiento del equipamiento de TI			NO			
GESTIONAR PROBLEMAS						
1.Registros de Errores			NO			
2. Registros de Incidentes		SI		E004	DIGITAL	REGISTRO INCIDENTES 032015-052015
3. Informes de incidentes		SI		E006	DIGITAL	INFORME DE INCIDENTES ESTADO
4. Informe de soluciones a problemas conocidos		SI		E005	DIGITAL	SOLUCIÓN PROBLEMAS CONOCIDOS
	Hardware	SI		E010	DIGITAL	PLAN DE CONTINGENCIA 2014
	Software	SI		E010	DIGITAL	PLAN DE CONTINGENCIA 2014
	Redes	SI		E010	DIGITAL	PLAN DE CONTINGENCIA 2014
	Aplicaciones y software de soporte	SI		E010	DIGITAL	PLAN DE CONTINGENCIA 2014
6. Los grupos de soporte tienen definido sus roles y responsabilidades dentro de UTIC.			NO	EC-INC-DECC.C001-1	DIGITAL	ENCUESTA
7. Informes o comunicados a los usuarios de problemas, errores o incidentes.		SI		E009	DIGITAL	COMUNICADOS SERVICIOS DE TI
8. Informes de gestión de cambios en base de problemas y errores.			NO	IN-CH-UTIC-006	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN
9. Informes sobre captura de información de problemas relacionada con cambios e incidentes TI para comunicarla a las partes interesadas clave.			NO	IN-CH-UTIC-006	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN

CONTINÚA

10. Documentos de supervisión de impacto de errores en los servicios conocidos.			NO	IN-CH-UTIC-006	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN
11. Actas de reuniones periódicas entre los responsables de los procesos de gestión de incidentes, problemas, cambios y configuración para considerar problemas recientes y acciones correctivas potenciales.			NO	IN-CH-UTIC-006	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN
11. Documento de análisis de los costes totales por causa de problemas			NO	IN-CH-UTIC-006	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN
Política de continuidad de negocio, objetivos y alcance.						
1. Registro de procesos de negocio internos y subcontratados críticos necesarios para cumplir obligaciones legales.		SI		E010	DIGITAL	PLAN DE CONTINGENCIA 2014
2. Identificar las partes interesadas clave.			NO	IN-CH-UTIC-007	IMPRESO	PRUEBAS SUSTANTIVAS OBSERVACIÓN
3. Roles y responsabilidades de los funcionarios para ejecutar eventos de contingencia.		SI		E010	DIGITAL	PLAN DE CONTINGENCIA 2014
4. Objetivos y alcance mínimos acordados de la política de continuidad del negocio.		SI		E010	DIGITAL	PLAN DE CONTINGENCIA 2014
1. Respaldos de la información		SI		CUE-HL-04-PLAN		CUESTIONARIO
2. Bitácora de Respaldos de Información o Bases de Datos (BDD)		SI		CUE-HL-04-PLAN		CUESTIONARIO
3. Frecuencia se obtienen respaldos de la data						
	Diario	SI		CUE-HL-04-PLAN		CUESTIONARIO

CONTINÚA

	Semanal		NO	CUE-HL-04-PLAN		CUESTIONARIO
	Mensual	SI		CUE-HL-04-PLAN		CUESTIONARIO
	Otros		NO			CUESTIONARIO
4. Los respaldos se almacenan en:						
	Discos magnéticos.	SI		CUE-HL-04-PLAN		CUESTIONARIO
	CD		NO	CUE-HL-04-PLAN		CUESTIONARIO
	DVD		NO	CUE-HL-04-PLAN		CUESTIONARIO
	Casetes		NO	CUE-HL-04-PLAN		CUESTIONARIO
5.Normas para la obtención y almacenamiento de los respaldos		SI		CUE-HL-04-PLAN		CUESTIONARIO
6. Pruebas de consistencia de los datos respaldados			NO	CUE-HL-04-PLAN		CUESTIONARIO
1. Conoce sobre Software malicioso		SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
2. Se puede prevenir la intrusión en un equipo		SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
3. Conoce alguna herramienta que permita protegerse contra Software Malicioso		SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
4. El Software es administrable		SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
5. El Software incluye módulos tales como: anti espía, anti pishing, etc.		SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
6. política de seguridad para las conexiones de cableado:				CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
	DHCP	SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO

CONTINUA 

	MAC		NO	CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
	DHCP CON MAC		NO	CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
	OTROS		NO	CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
7. Monitoreo constantemente del tráfico entrante y saliente de la RED		SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
8. La información en la RED está cifrada			NO	CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
9. Aplican medidas de seguridad para las conexiones de red		SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
10. Realizan pruebas de intrusión en la Red (Ethical Hacking)			NO	CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
11. Clase de pruebas:						
	Pruebas de penetración con objetivo		NO	CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
	Pruebas de penetración sin objetivo		NO	CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
	Pruebas de penetración a ciegas	SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
	Pruebas de penetración informadas	SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
	Pruebas de penetración externas	SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
	Pruebas de penetración internas			CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
12. Utiliza políticas de seguridad en los equipos		SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
13. Acceso remoto está habilitado para cualquier persona			NO	CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
14. Tiene implantado algún mecanismo que permita restringir el acceso a la red		SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO

CONTINÚA

15. La RED garantiza la Integridad del Sistema		SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
16. Están habilitados los puertos USB, CD-ROM		SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
17. Definición de roles para los diferentes usuarios			NO	CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
18. Tienen habilitados LOGs de Auditoria, en lo referente a usuarios de la Institución.		SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
19. Cuentan con usuarios privilegiados de prueba		SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
20. Personal encargado de verificar los LOGs de usuarios		SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
21. Bitácoras del manejo de la información, usuarios, etc		SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
22. El acceso a cualquier departamento (puertas) es:						
	Global		NO			
	De acuerdo a las funciones	SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
23. registro sobre el uso de las tarjetas de acceso		SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
24. Socialización del uso de las tarjetas de acceso		SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
25. Sabe que debe hacer en caso de encontrar a una persona desconocida en un área restringida.		SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
26. Políticas de seguridad para la destrucción de formularios de la empresa.			NO	CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
27. Control acerca de quién puede acceder a algún documento en especia.		SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
28. Inventario de documentos sensibles y dispositivos de salida.			NO	CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
29. Herramientas de software para monitorear la seguridad de la infraestructura.		SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
30. Análisis para determinar si pudieran presentar incidentes potenciales.		SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO

CONTINÚA

31. Registro del número de vulnerabilidades descubiertas o de rupturas (breaches) de cortafuegos.	SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
32. Registro del número de porcentaje de individuos que reciben formación de concienciación relativa al uso de dispositivos de usuario final.		NO	CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
33. Registro del número de incidentes que impliquen dispositivos de usuario final o de dispositivos de usuario final no autorizados detectados en la red o en el entorno.		NO	CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
34. Registro del porcentaje de pruebas periódicas de los dispositivos de seguridad del entorno.	SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO
35. Registro del número de incidentes de seguridad física y accesos no autorizados de la información.	SI		CUE-HL-05-PLAN	IMPRESO	CUESTIONARIO

3.6 APLICACIÓN DE INSTRUMENTO DE INVESTIGACION

3.6.1 Encuesta de satisfacción de Usuario de los servicios de UTIC.

3.6.1.1 Población y Muestra

Los datos que se utilizan para la aplicación de la presente encuesta fueron proporcionados por la Secretaria general y la Unidad de Talento Humano de la Universidad de la Fuerzas Armadas ESPE. Siendo un total de 13409 usuarios para la *Entrega, Servicio y Soporte de la UTIC*.

Fórmula para el cálculo de la muestra.

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

Tabla 10

Cálculo de la muestra de la población de Estudiantes

Población Estudiantes	Variables	Significado	Valores
11846	e	Error	0,05
	N	Población	11846
	σ	Desviación estándar	0,5
	confianza		95
	Z	Nivel de Confianza	1,96
	n	Muestra	372

Tabla 11

Cálculo de la muestra de Docentes

Población Docentes	Variables	Significado	Valores
1116	e	Error	0,05
	N	Población	1116
	σ	Desviación estándar	0,5
	confianza		95
	Z	Nivel de Confianza	1,96
	n	Muestra	286

Tabla 12 Cálculo de la muestra de P. Administrativos

Población Administrativos	Variables	Significado	Valores
447	E	Error	0,05
	N	Población	447
	Σ	Desviación estándar	0,5
	confianza		95
	Z	Nivel de Confianza	1,96
	N	Muestra	206,85111

3.6.2 Tabulación de La encuesta

La presente encuesta se enfoca en identificar el grado de satisfacción de los usuarios sobre la *Entrega, Servicio y Soporte de la UTIC.* Los usuarios están identificados en tres grupos: Estudiantes, Docentes y Personal Administrativo.

Pregunta 1.

Tabla 13

Número de Estudiantes encuestados

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
1	Seleccione el grupo de usuarios a la que pertenece dentro de la Comunidad Universitaria. "ESPE".	A	Alumnos	372
		B	Docentes	
		C	Administrativos	

Pregunta 2.

Tabla 14

Satisfacción ante la gestión del servicio de la UTIC

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
2	¿Está satisfecho con la gestión realizada por el Servicio de la UTIC?	a	Nada satisfecho	18
		b	Poco satisfecho	179
		c	Satisfecho	151
		d	Muy Satisfecho	24
		e	Totalmente Satisfecho	0

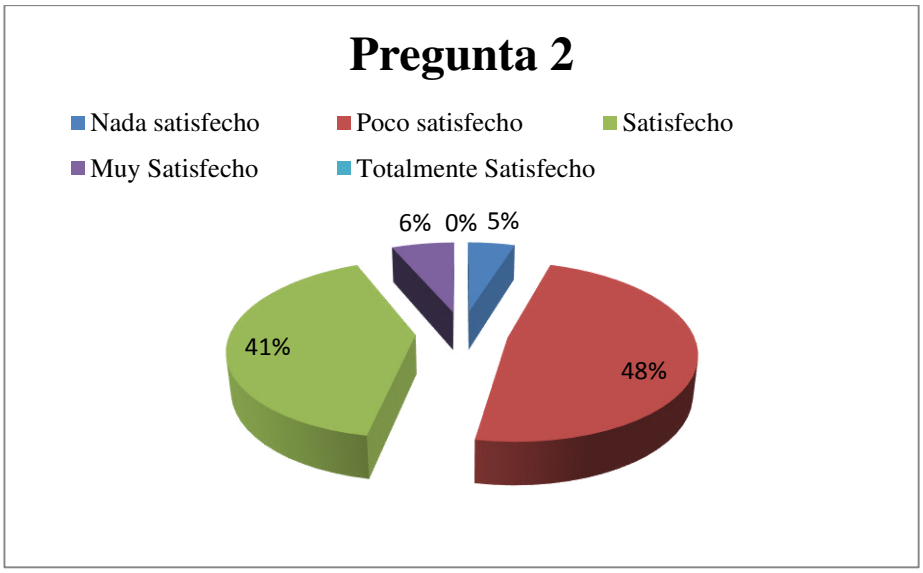


Figura 8. Pregunta 2

La pregunta 2, hace referencia a la satisfacción del usuario ante la gestión realizada por el Servicio de la UTIC. El 5% indica que está **nada satisfecho**, el 48% manifiesta que se encuentran **poco satisfechos**, el 41% de los encuestados indicaron que están **satisfechos**, y el 6% menciona que están **muy satisfechos**.

Pregunta 3.

Tabla 15

Expectativas del Usuario ante el servicio de la UTIC

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
3	¿El Servicio de la UTIC ha cumplido con sus expectativas?	A	Nunca	18
		B	A veces	212
		C	Normalmente	114
		D	Casi Siempre	20
		E	Siempre	8

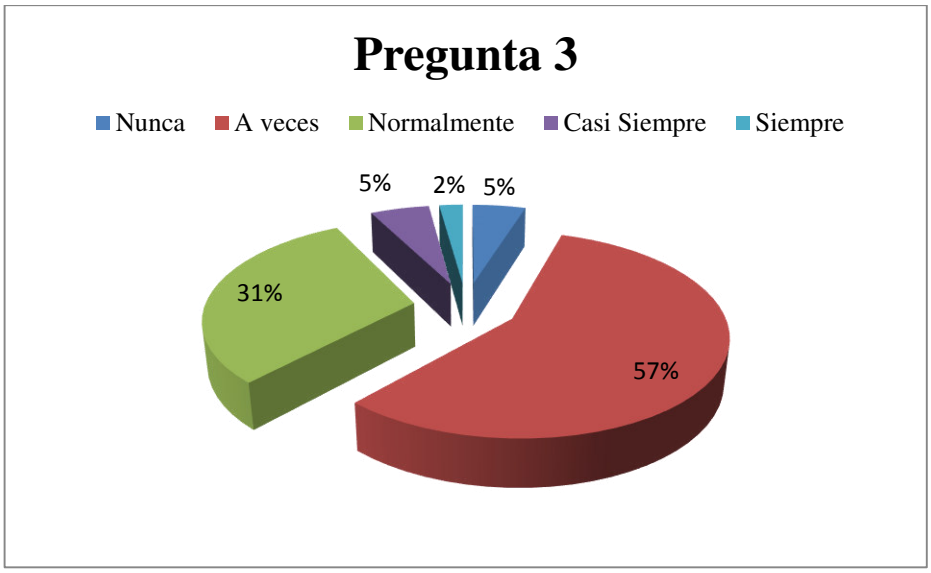


Figura 9. Pregunta 3

La pregunta 3, da a conocer si el Servicio de la Unidad de Tecnologías de Información y Comunicación (UTIC) ha cumplido con las expectativas del usuario. El 5% indica que **nunca**, el 57% manifiesta que **a veces**, el 31% de los encuestados menciona que **normalmente si**, el 5% dice que **casi siempre** y un 2% dicen que **siempre**.

Pregunta 4.

Tabla 16

Satisfacción de las necesidades específicas del Usuario

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
4	¿El Servicio de la UTIC ha satisfecho sus necesidades específicas?	a	Nunca	31
		b	A veces	224
		c	Normalmente	89
		d	Casi Siempre	20
		e	Siempre	8

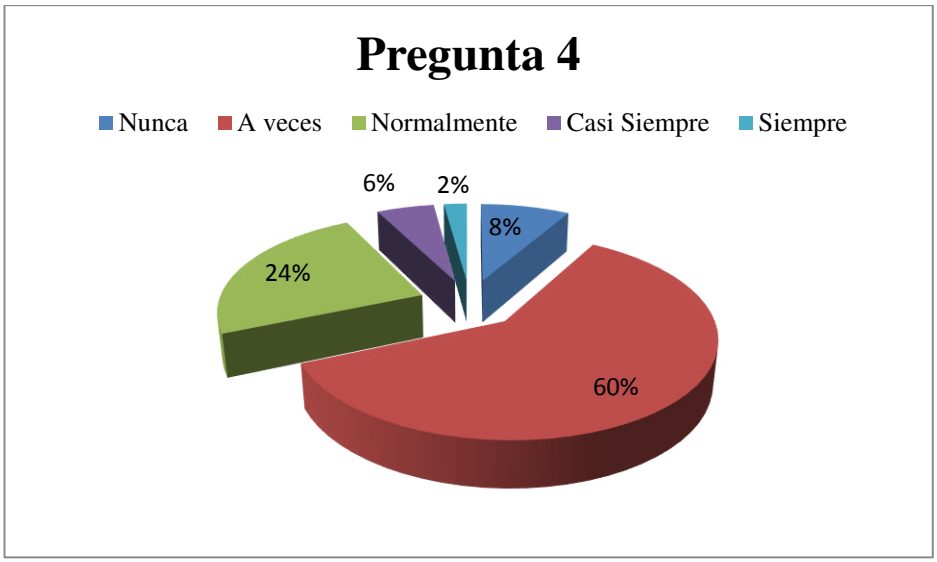


Figura 10. Pregunta 4

La pregunta 4, hace referencia a que si el Servicio de la Unidad de Tecnologías de Información y Comunicación (UTIC) ha satisfecho las necesidades específicas del usuario. El 8% indica que **nunca**, el 60% dice que **a veces**, el 24% de los encuestados menciona que **normalmente**, el 6% dice que **casi siempre** y un 8% indica que **siempre**.

Pregunta 5.

Tabla 17

Horarios del servicio de la UTIC

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
5	¿Los horarios del Servicio de la UTIC son adecuados?	A	Nunca	43
		B	A veces	102
		C	Normalmente	134
		D	Casi Siempre	73
		E	Siempre	20

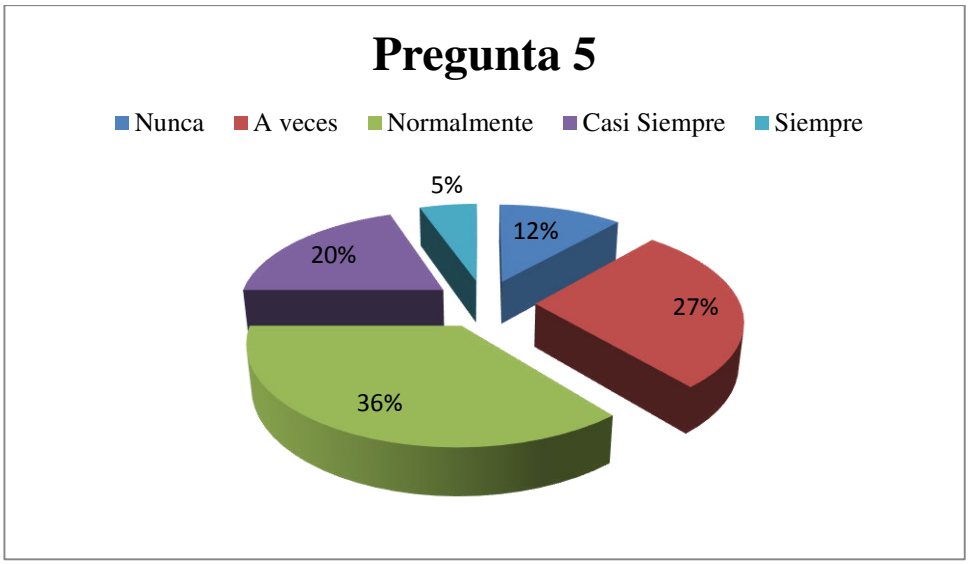


Figura 11. Pregunta 5

La pregunta 5, hace referencia a que si los horarios del Servicio de la Unidad de Tecnologías de Información y Comunicación (UTIC) son adecuados. El 12% de los encuestados menciona **nunca**, el 27% dice que **a veces**, el 36% menciona que **normalmente**, el 20% dice que **casi siempre** y un 5% indica que **siempre**.

Pregunta 6.

Tabla 18

Interés de la UTIC en lo no producción de errores

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
6	¿Cree que el Servicio de la UTIC muestra claro interés en que no se produzcan errores en los servicios que ofrece a la comunidad Universitaria?	a	Nunca	47
		b	A veces	171
		c	Normalmente	114
		d	Casi Siempre	28
		e	Siempre	12

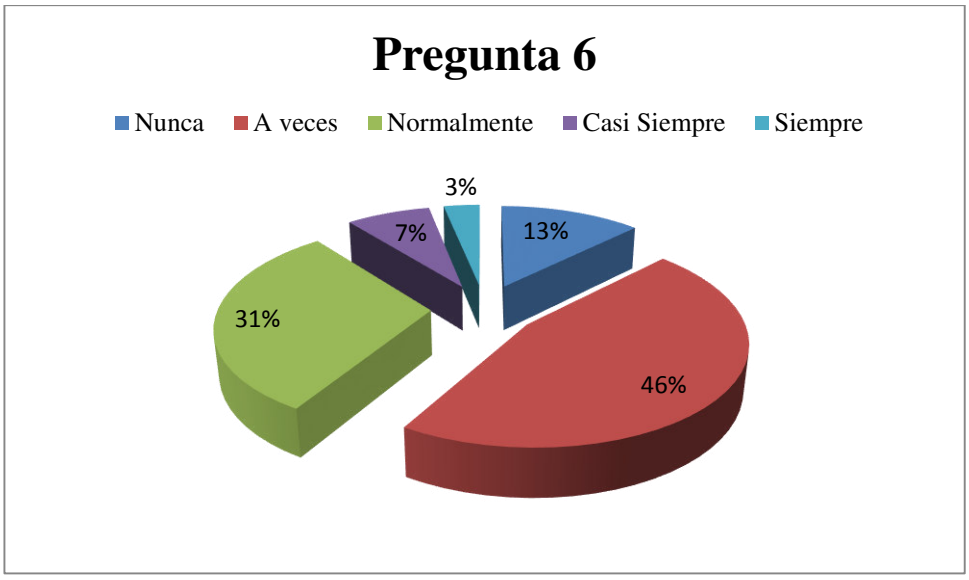


Figura 12. Pregunta 6.

La pregunta 6, hace referencia a que si cree que el Servicio de la Unidad de Tecnologías de Información y Comunicación (UTIC) muestra claro interés en que no se produzcan errores en los servicios que ofrece a la comunidad Universitaria. El 13% de los encuestados indica que **nunca**, el 46% manifiesta que **a veces**, el 31% dice que **normalmente**, el 7% indica que **casi siempre** y un 3% indica que **siempre**.

Pregunta 7.

Tabla 19

Disponibilidad del personal de UTIC

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
7	¿El personal del Servicio de la UTIC está disponible para responder a sus preguntas?	a	Nunca	48
		b	A veces	138
		c	Normalmente	122
		d	Casi Siempre	44
		e	Siempre	20

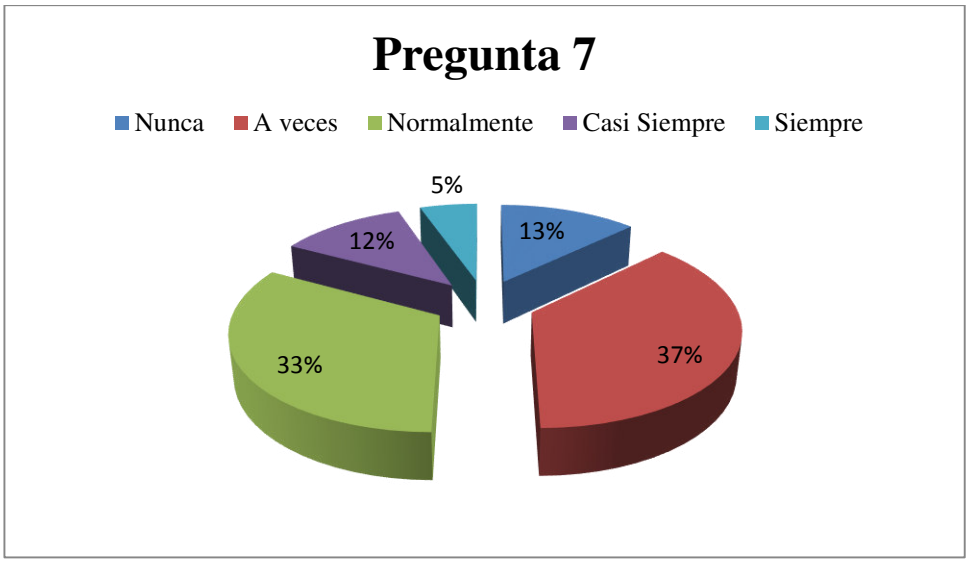


Figura 13. Pregunta 7

La pregunta 7, trata de verificar si el personal del Servicio de la Unidad de Tecnologías de Información y Comunicación (UTIC) está disponible para responder a las preguntas del usuario. El 13% de los encuestados indica que **nunca**, el 37% manifiesta que **a veces**, el 33% dice que **normalmente**, el 12% indica que **casi siempre** y un 5% indica que **siempre**.

Pregunta 8.

Tabla 20

Atención y capacidad técnica del personal UTIC

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
8	¿La atención y capacidad técnica del personal del Servicio de la UTIC le transmite confianza y seguridad?	a	Nunca	44
		b	A veces	153
		c	Normalmente	106
		d	Casi Siempre	61
		e	Siempre	8

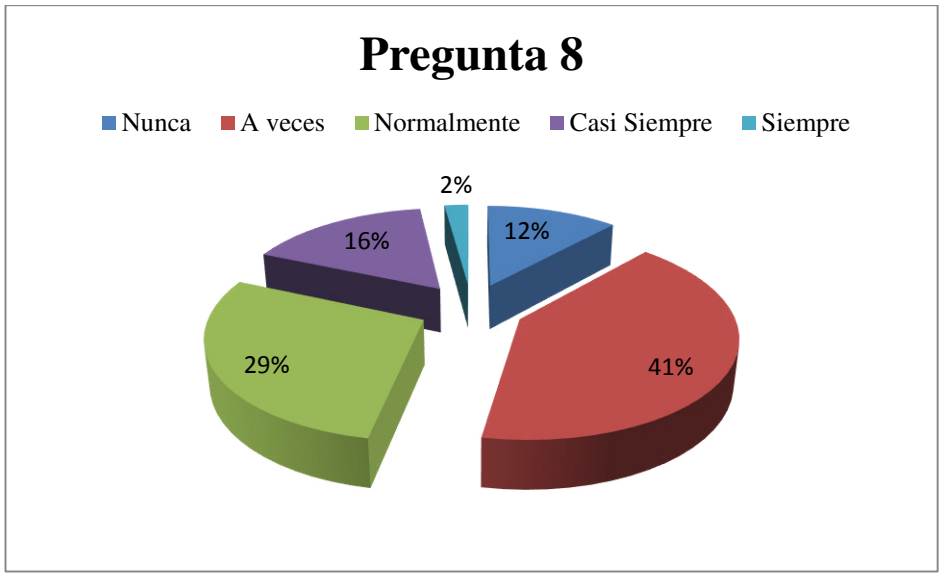


Figura 14. Pregunta 8

La pregunta 8, hace referencia a que si la atención y capacidad técnica del personal del Servicio de la Unidad de Tecnologías de Información y Comunicación (UTIC) transmite confianza y seguridad al usuario. El 12% de los encuestados indica que **nunca**, el 41% dice que **a veces**, el 29% indica que **normalmente**, el 16% menciona que **casi siempre** y el 2% indica que **siempre**.

Pregunta 9.

Tabla 21

Lenguaje del personal del servicio UTIC

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
9	¿El personal del Servicio de la UTIC utiliza un lenguaje comprensible e intenta transmitirle de forma sencilla y clara sus explicaciones?	a	Nunca	32
		b	A veces	121
		c	Normalmente	134
		d	Casi Siempre	61
		e	Siempre	24

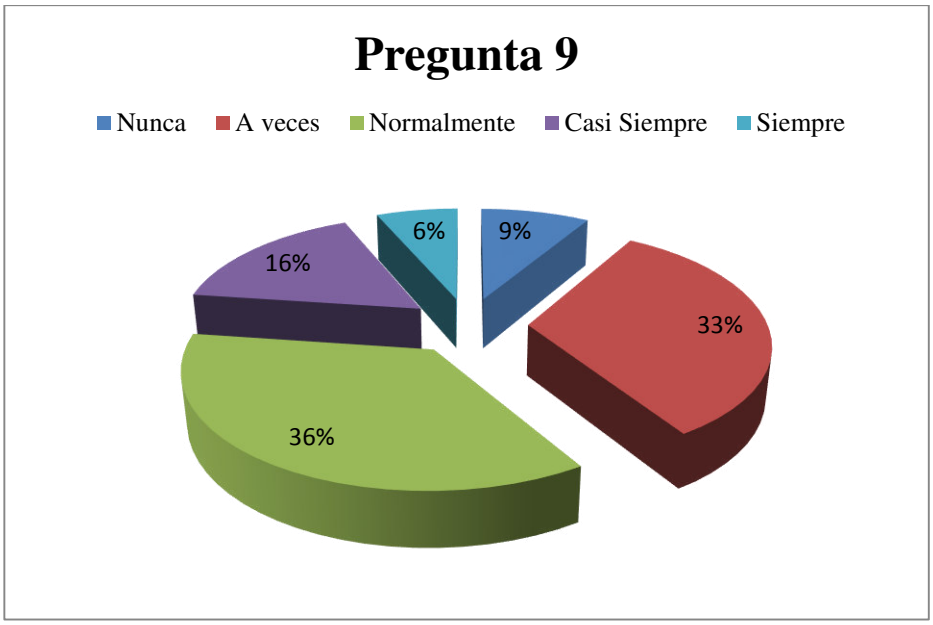


Figura 15. Pregunta 9

La pregunta 9, hace referencia a que si el personal del Servicio de la Unidad de Tecnologías de Información y Comunicación (UTIC) utiliza un lenguaje comprensible e intenta transmitirle de forma sencilla y clara sus explicaciones. El 9% de los encuestados mencionan que **nunca**, el 33% dice que **a veces**, el 36% indica que **normalmente**, el 16% menciona que **casi siempre** y el 6% indica que **siempre**.

Pregunta 10.

Tabla 22

Disponibilidad de ayuda por parte de UTIC

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
10	¿El personal del Servicio de la UTIC está dispuesto a prestar ayuda?	A	Nunca	8
		B	A veces	136
		C	Normalmente	155
		D	Casi Siempre	57
		E	Siempre	16

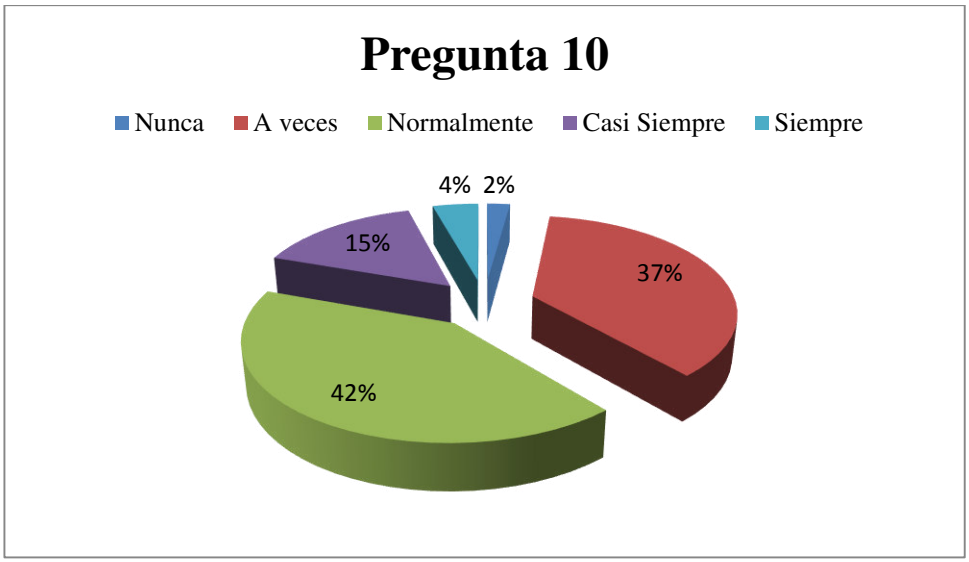


Figura 16. Pregunta 10

La pregunta 10, hace referencia a que si el personal del Servicio de la Unidad de Tecnologías de Información y Comunicación (UTIC) está dispuesto a prestar ayuda. El 2% de los encuestados establecen que **nunca**, el 37% menciona que **a veces**, el 42% indica que **normalmente**, el 15% menciona que **casi siempre** y el 4% indica que **siempre**.

Pregunta 11.

Tabla 23

Información de los plazos de inicio y fin de servicios

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
11	¿El personal del Servicio de la UTIC le informa con precisión acerca de los plazos de inicio y conclusión del servicio que se está prestando?	a	Nunca	32
		b	A veces	137
		c	Normalmente	118
		d	Casi Siempre	53
		e	Siempre	32

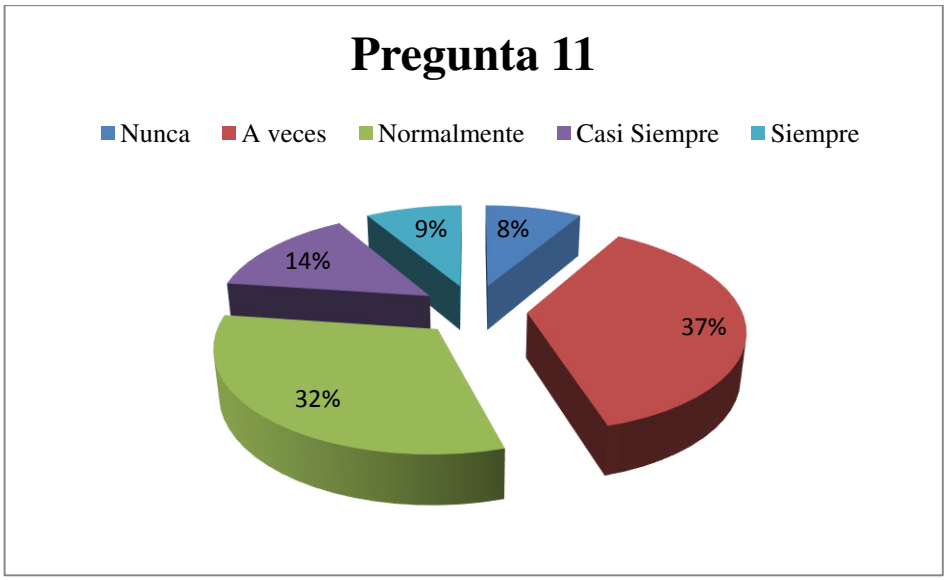


Figura 17. Pregunta 11.

La pregunta 11, se refiere a que si el personal del Servicio de la Unidad de Tecnologías de Información y Comunicación (UTIC) le informa con precisión acerca de los plazos de inicio y conclusión del servicio que se está prestando. El 8% manifiesta que **nunca**, el 37% menciona que **a veces**, el 32% indica que **normalmente**, el 14% menciona que **casi siempre** y el 9% indica que **siempre**.

Pregunta 12.

Tabla 24

Solución de peticiones e incidencias por UTIC

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
12	¿El personal del Servicio de la UTIC soluciona correctamente sus peticiones e incidencias?	a	Nunca	36
		b	A veces	166
		c	Normalmente	114
		d	Casi Siempre	48
		e	Siempre	8

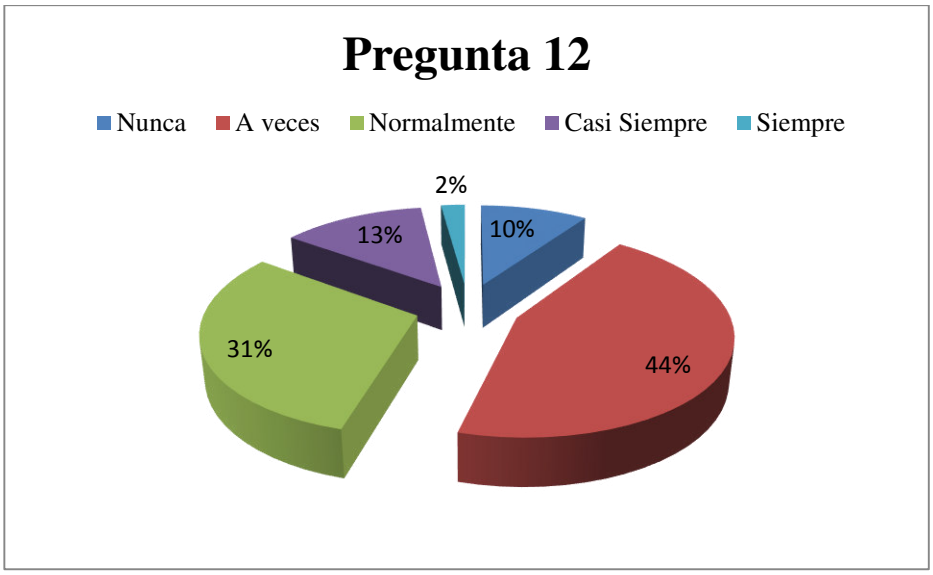


Figura 18. Pregunta 12

La pregunta 12, da a conocer si el personal del Servicio de la Unidad de Tecnologías de Información y Comunicación (UTIC) soluciona correctamente sus peticiones e incidencias. El 10% manifiesta que **nunca**, el 44% menciona que **a veces**, el 31% indica que **normalmente**, el 13% menciona que **casi siempre** y el 2% indica que **siempre**.

Pregunta 13.

Tabla 25

Conocimientos suficientes por el personal de UTIC

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
13	¿El personal del Servicio de la UTIC demuestra conocimientos e información suficientes para responder a las preguntas que le hace?	a	Nunca	24
		b	A veces	149
		c	Normalmente	122
		d	Casi Siempre	61
		e	Siempre	16

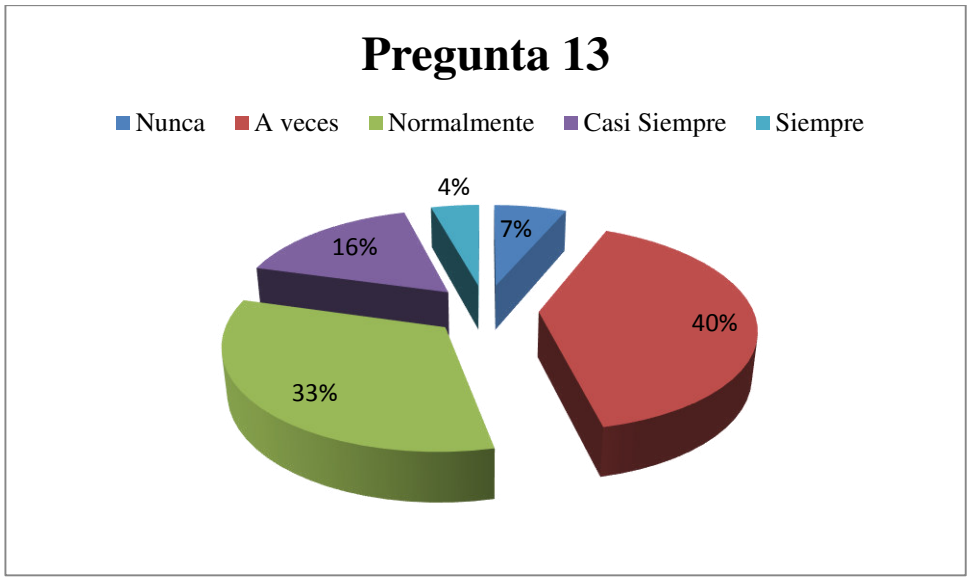


Figura 19. Pregunta 13

La pregunta 13, da a conocer si el personal del Servicio de la Unidad de Tecnologías de Información y Comunicación (UTIC) demuestra conocimientos e información suficientes para responder a las preguntas que le hace el usuario. El 7% indica que **nunca**, el 40% menciona que **a veces**, el 33% indica que **normalmente**, el 16% menciona que **casi siempre** y un 4% dice que **siempre**.

Pregunta 14.

Tabla 26

Cumplimiento de plazos por UTIC

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
14	¿El Servicio de la UTIC cumple los plazos cuando se compromete a hacer algo en un tiempo determinado?	a	Nunca	28
		b	A veces	173
		c	Normalmente	114
		d	Casi Siempre	53
		e	Siempre	4

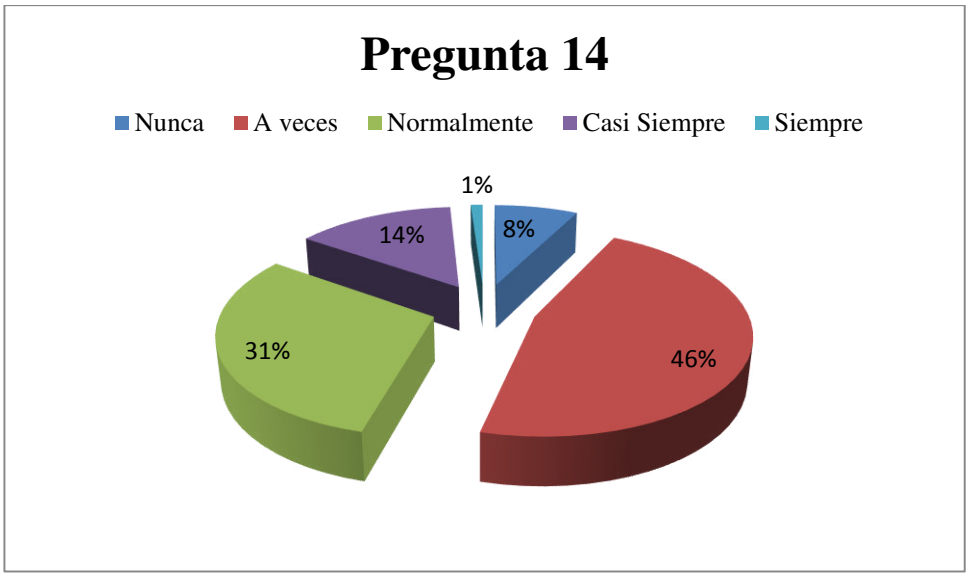


Figura 20. Pregunta 14

La pregunta 14, hace referencia a que si el Servicio de la Unidad de Tecnologías de Información y Comunicación (UTIC) cumple los plazos cuando se compromete a hacer algo en un tiempo determinado. El 8% indica que **nunca**, el 46% menciona que **a veces**, el 31% indica que **normalmente**, el 14% menciona que **casi siempre** y un 1% dice que **siempre**.

Pregunta 15.

Tabla 27

Información a los usuarios por problemas o incidentes graves

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
15	¿El Servicio de la UTIC informa a los usuarios cuando se ha producido un problema o incidente grave a nivel general?	a	Nunca	89
		b	A veces	93
		c	Normalmente	97
		d	Casi Siempre	61
		e	Siempre	32

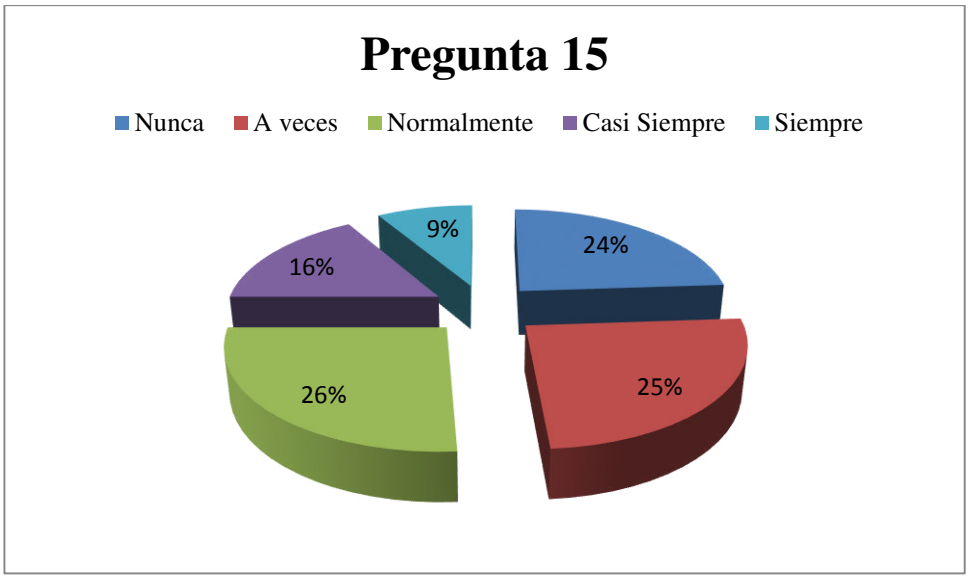


Figura 21. Pregunta 15

La pregunta 15, hace referencia a que si el Servicio de la Unidad de Tecnologías de Información y Comunicación (UTIC) informa a los usuarios cuando se ha producido un problema o incidente grave a nivel general. El 24% indica que **nunca**, el 25% menciona que **a veces**, el 26% indica que **normalmente**, el 16% menciona que **casi siempre** y un 9% dice que **siempre**.

Pregunta 16.

Tabla 28

Solución de incidencias en tiempo adecuado

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
16	¿El Servicio de la UTIC soluciona sus incidencias en un tiempo adecuado?	a	Nunca	48
		b	A veces	158
		c	Normalmente	134
		d	Casi Siempre	24
		e	Siempre	8

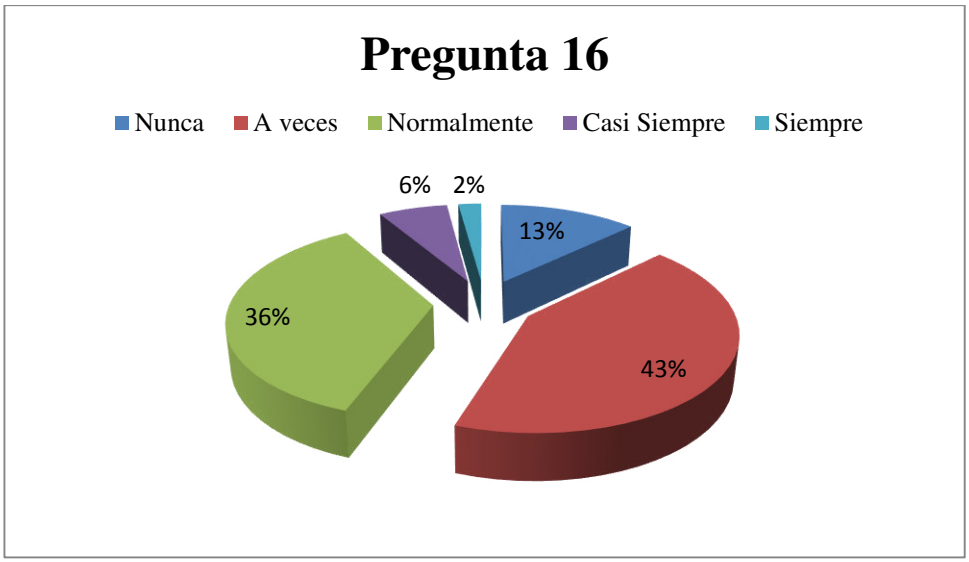


Figura 22. Pregunta 16

La pregunta 16, da a conocer si el Servicio de la Unidad de Tecnologías de Información y Comunicación (UTIC) soluciona sus incidencias en un tiempo adecuado. El 13% indica que **nunca**, el 43% menciona que **a veces**, el 36% indica que **normalmente**, el 6% menciona que **casi siempre** y un 2% dice que **siempre**.

Pregunta 17.

Tabla 29

Satisfacción del Usuario por SGA, Sistema Banner

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
17	¿Se encuentra satisfecho con el servicio del Sistema de Gestión Académica, así como el Sistema Banner?	a	Nada Satisfecho	81
		b	Poco Satisfecho	145
		c	Satisfecho	134
		d	Muy Satisfecho	12
		e	Totalmente Satisfecho	0

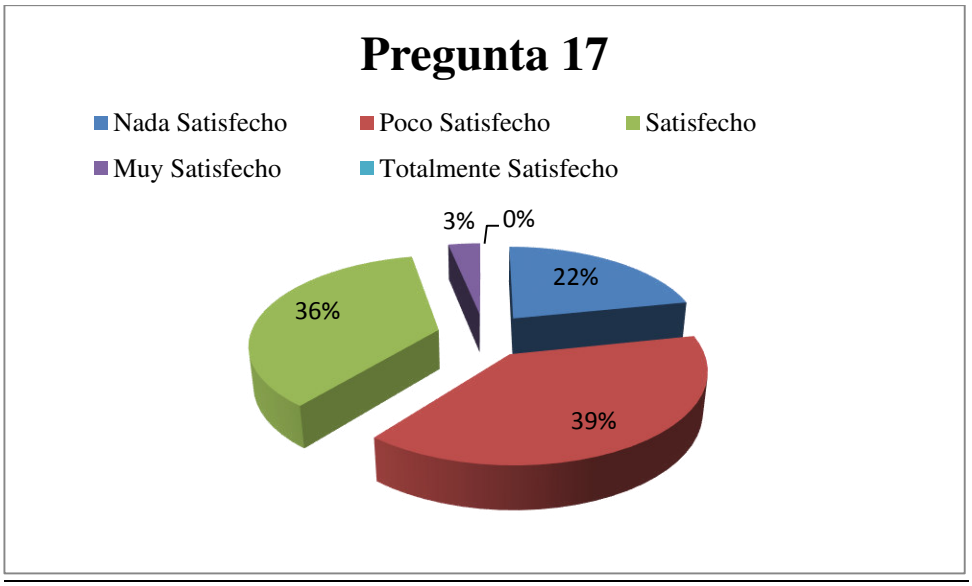


Figura 23. Pregunta 17

La pregunta 17, da a conocer la satisfacción con el servicio del Sistema de Gestión Académica, así como el Sistema Banner. El 22% indica que **nada satisfecho**, el 39% menciona que **poco satisfecho**, el 36% indica que **satisfecho**, y el 3% menciona que **muy satisfecho**.

Pregunta 18.

Tabla 30

Satisfacción con los servicios WEB

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
18	¿Se encuentra satisfecho con los Servicios Web tales como: Portal público actual y en desarrollo, micro sitios y blogs?	a	Nada Satisfecho	53
		b	Poco Satisfecho	149
		c	Satisfecho	138
		d	Muy Satisfecho	28
		e	Totalmente Satisfecho	4

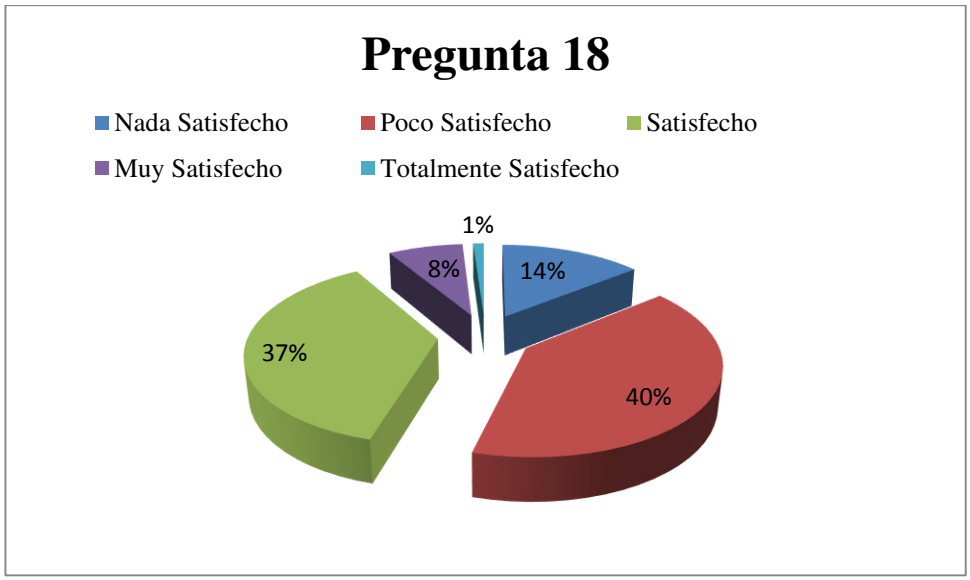


Figura 24. Pregunta 18

La pregunta 18, hace referencia a la satisfacción de los Servicios Web tales como: Portal público actual y en desarrollo, micro sitios y blogs. El 14% indica que **nada satisfecho**, el 40% menciona que **poco satisfecho**, el 37% indica que **satisfecho**, el 8% menciona que **muy satisfecho** y 1% **totalmente satisfecho**.

Pregunta 19.

Tabla 31

Satisfacción de los usuarios por los servicios WEB intranet

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
19	¿Se encuentra satisfecho con los Servicios Web intranet: Sistema Banner (Autoservicios, Portal Luminis) y Sistema Web POSTGRADOS?	a	Nada Satisfecho	99
		b	Poco Satisfecho	123
		c	Satisfecho	134
		d	Muy Satisfecho	16
		e	Totalmente Satisfecho	0

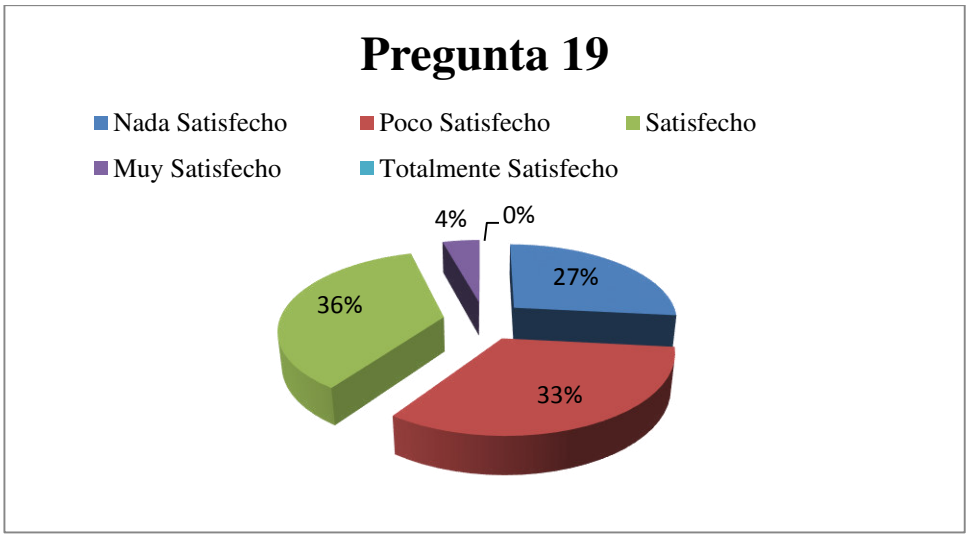


Figura 25. Pregunta 19

La pregunta 19, hace referencia a la satisfacción de los usuarios con los Servicios Web intranet: Sistema Banner (Autoservicios, Portal Luminis) y Sistema Web POSTGRADOS. El 27% indica que **nada satisfecho**, el 33% menciona que **poco satisfecho**, el 36% indica que **satisfecho**, y el 4% menciona que **muy satisfecho.**

Pregunta 20.

Tabla 32

Satisfacción de servicios del Sistema de Gestión Administrativa

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
20	¿Se encuentra satisfecho con los Servicios del Sistema de Gestión Administrativa tales como: Sistema Banner (Administrativo-RRHH, Digitalización, Workflow), Sistema Agrown, ESIGEF, Olympo etc.?	a	Nada Satisfecho	33
		b	Poco Satisfecho	140
		c	Satisfecho	155
		d	Muy Satisfecho	44
		e	Totalmente Satisfecho	0

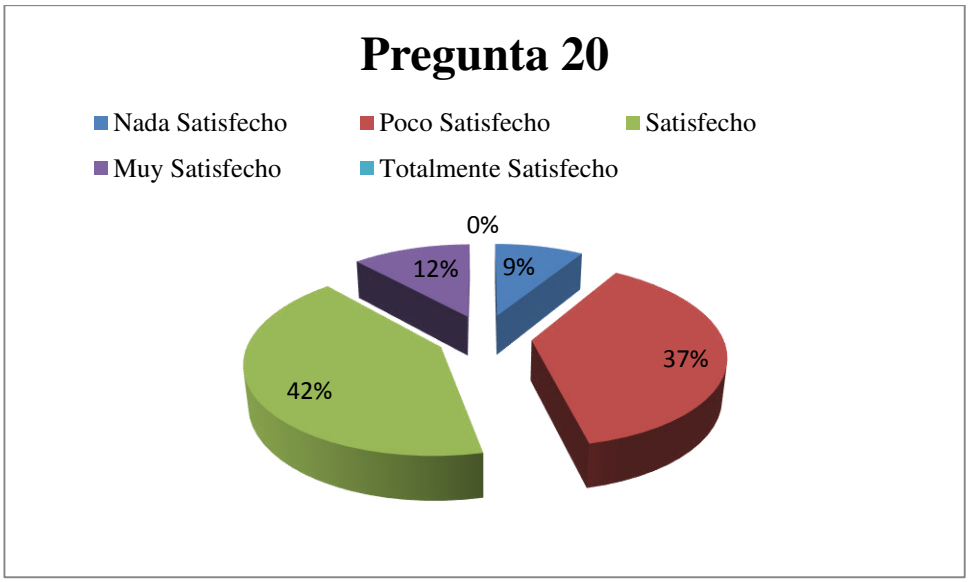


Figura 26. Pregunta 20

La pregunta 20, hace referencia a la satisfacción de los Servicios del Sistema de Gestión Administrativa tales como: Sistema Banner (Administrativo-RRHH, Digitalización, Workflow), Sistema Agrown, ESIGEF, Olympo etc. El 9% indica que **nada satisfecho**, el 37% menciona que **poco satisfecho**, el 42% indica que **satisfecho**, y el 12% menciona que **muy satisfecho.**

Pregunta 21.

Tabla 33

Satisfacción del Usuario por el servicio de Internet

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
21	¿Se encuentra satisfecho con el Servicio de INTERNET que ofrece la Universidad?	a	Nada Satisfecho	110
		b	Poco Satisfecho	173
		c	Satisfecho	73
		d	Muy Satisfecho	16
		e	Totalmente Satisfecho	0

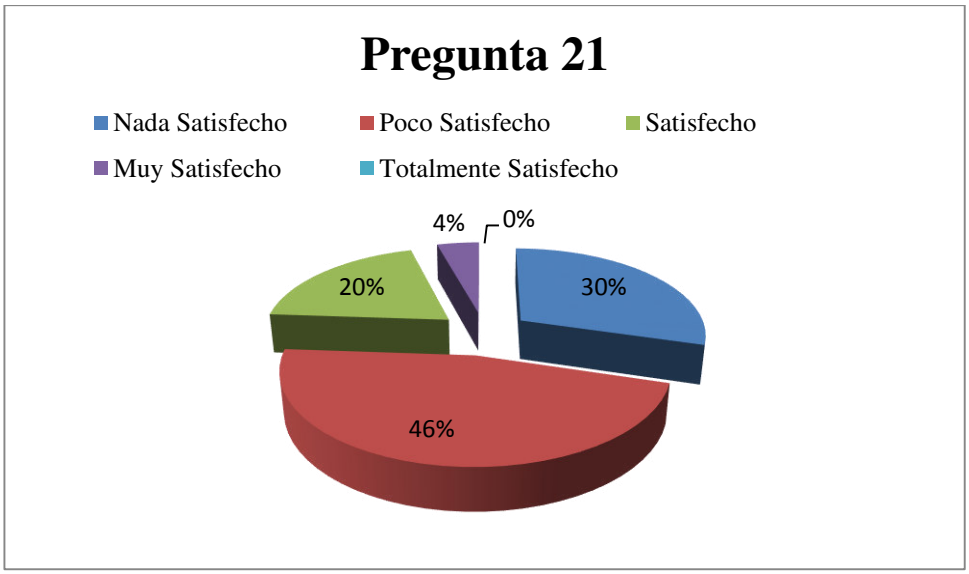


Figura 27. Pregunta 21

La pregunta 21, da a conocer si se encuentra satisfecho con el Servicio de INTERNET que ofrece la Universidad. El 30% indica que **nada satisfecho**, el 46% menciona que **poco satisfecho**, el 20% indica que **satisfecho**, y el 4% menciona que **muy satisfecho.**

Pregunta 22.

Tabla 34

Satisfacción por el mantenimiento de equipos informáticos

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
22	¿Está satisfecho con el mantenimiento de los equipos informáticos pertenecientes a la Universidad?	a	Nada Satisfecho	45
		b	Poco Satisfecho	141
		c	Satisfecho	150
		d	Muy Satisfecho	28
		e	Totalmente Satisfecho	8

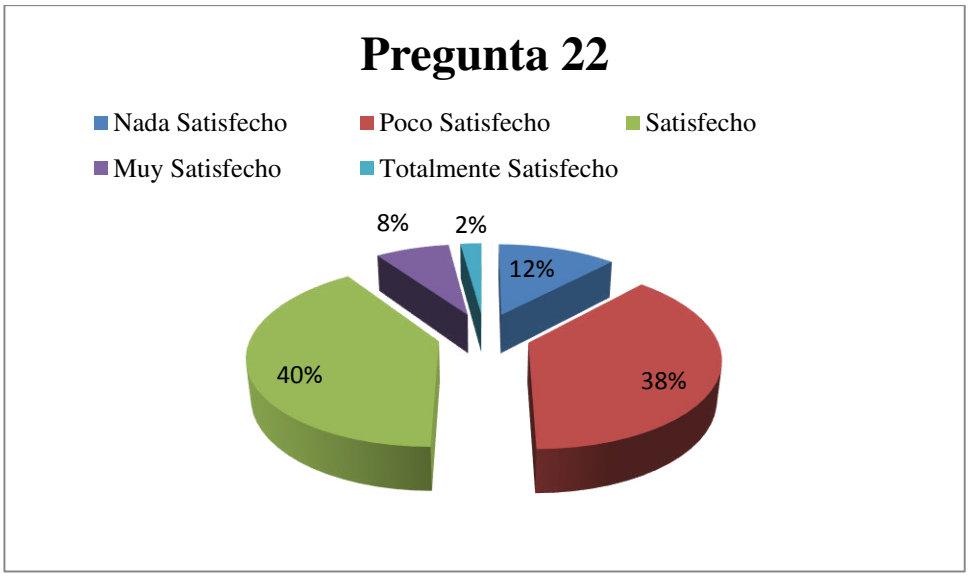


Figura 28. Pregunta 22

La pregunta 22, da a conocer la satisfacción por el mantenimiento de los equipos informáticos pertenecientes a la Universidad. El 12% indica que **nada satisfecho**, el 38% menciona que **poco satisfecho**, el 40% indica que **satisfecho**, el 8% menciona que **muy satisfecho** y 2% indica que **totalmente satisfecho.**

Pregunta 23.

Tabla 35

Expectativas del usuario por el servicio de Videoconferencia

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
23	¿El servicio de Videoconferencia cumple sus expectativas?	a	Nunca	91
		b	A veces	135
		c	Normalmente	118
		d	Casi Siempre	28
		e	Siempre	0

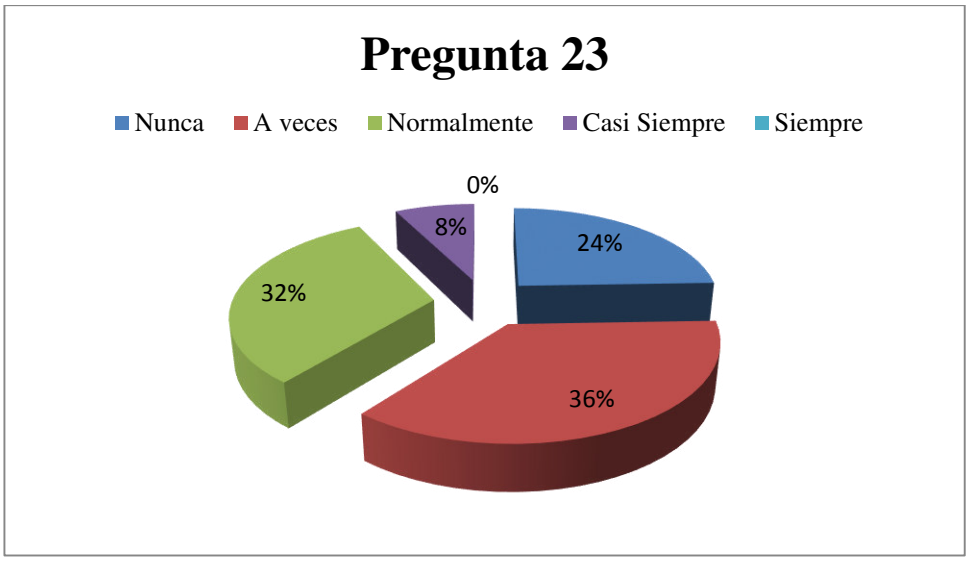


Figura 29. Pregunta 23

La pregunta 23, se refiere a que si el servicio de Videoconferencia cumple sus expectativas. El 24% indica que **nunca**, el 36% menciona que **a veces**, el 32% indica que **normalmente**, y el 8% menciona que **casi siempre.**

Pregunta 24.

Tabla 36

Satisfacción con el servicio de repositorio digital Biblioteca

N°	Pregunta	Código de respuesta	Opciones de respuesta	#
24	¿Se encuentra satisfecho con el servicio de Repositorio Digital de Archivos de la Biblioteca?	a	Nada Satisfecho	46
		b	Poco Satisfecho	102
		c	Satisfecho	167
		d	Muy Satisfecho	53
		e	Totalmente Satisfecho	4

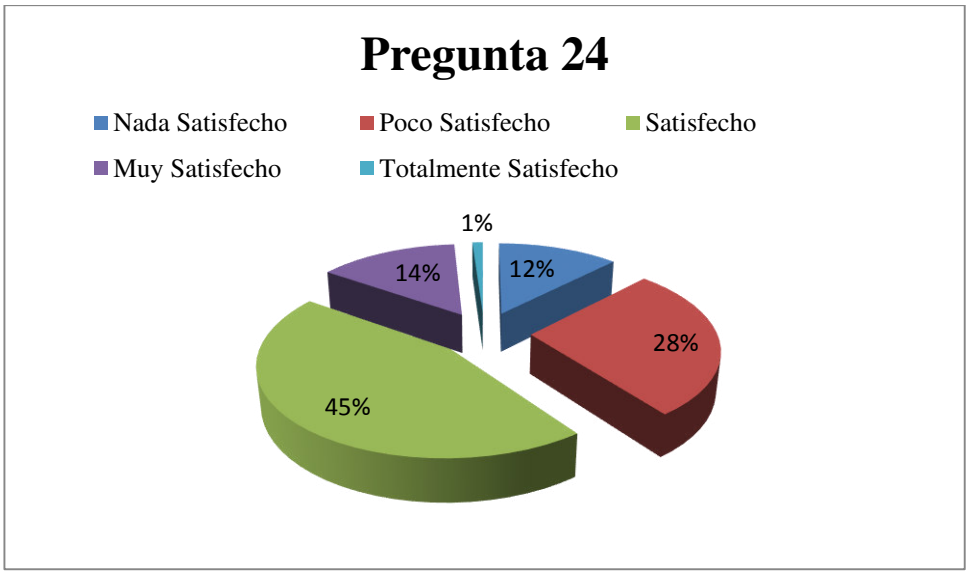


Figura 30. Pregunta 24

La pregunta 24, se refiere a que si el usuario se encuentra satisfecho con el servicio de Repositorio Digital de Archivos de la Biblioteca. El 12% indica que **nada satisfecho**, el 28% menciona que **poco satisfecho**, el 45% indica que **satisfecho**, el 14% menciona que **muy satisfecho** y el 1% **totalmente satisfecho.**

CAPÍTULO IV

INFORME DE EVALUACIÓN TÉCNICA INFORMÁTICA

CONSULTORES INDEPENDIENTES
PROYECTO INSTITUCIONAL DE LA ESPE
Ing. Fernanda Becerra
Ing. Henry León

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE
SEDE MATRIZ

Inicio Evaluación Técnica Informática: 04 de Marzo de 2015.
Fin Evaluación Técnica Informática: 30 de Abril de 2015.

Fecha entrega del informe: 14 de mayo de 2015

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE, Av. Gral. Rumiñahui s/n Sangolquí – Ecuador.

El presente informe contiene los resultados de la "Evaluación Técnica Informática de la Entrega, Servicio y Soporte de la Universidad de las Fuerzas Armadas Sede Matriz", la misma que fue realizada en un período comprendido entre el 04 de Marzo de 2015 al 30 de Abril de 2015. Dicho informe incluye una descripción breve de las etapas llevadas a cabo durante la evaluación y posteriormente exponer las conclusiones y/o recomendaciones de los procesos de soporte, con base a los hallazgos y evidencias encontrados durante esta fase. Además cabe señalar que la metodología utilizada es COBIT 5 establecida por ISACA en conformidad con la auditoría de Sistemas de Información (SI) y las normas de aseguramiento y auditoría. Las pruebas obtenidas proporcionan un soporte razonable que permiten tomar decisiones a las autoridades correspondientes y puedan gestionar cambios que ayuden a mejorar la calidad en los diferentes servicios.

Ing. Fernanda Becerra
Consultor Auditor
C.C. 0401288139
Quito – Ecuador

Ing. Henry León
Consultor Auditor
C.C. 1712399151
Quito – Ecuador

4.1 Tabla de Contenidos

Sección **Pág.**

4.2 Introducción

4.2.1 Descripción del negocio

La Universidad de las Fuerzas Armadas - ESPE, es una Institución Educativa de prestigio, que brinda servicios académicos de alta calidad, cuenta con una Unidad de Tecnologías de Información y Comunicación (UTIC) que centraliza la administración y gestión de las actividades de TI, es decir se encarga del análisis, desarrollo e implantación de los sistemas requeridos en la ESPE y se preocupa por el adecuado funcionamiento de las aplicaciones existentes, redes y comunicaciones.

Se rige por la Constitución de la República del Ecuador, la Ley Orgánica de Educación Superior y su reglamento; otras leyes conexas; su Estatuto aprobado por el Consejo de Educación Superior-CES y los reglamentos internos expedidos de acuerdo con la ley.

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

Entre sus objetivos estratégicos institucionales están:

- Incrementar el reconocimiento de la Universidad de las Fuerzas Armadas-ESPE como una institución referente en educación superior.
- Incrementar la calidad de los profesionales y postgraduados.
- Incrementar la producción científica - tecnológica y su calidad.
- Incrementar el impacto social de los programas de vinculación.
- Incrementar la eficiencia y eficacia del sistema formativo de grado y postgrado.
- Incrementar la capacidad del sistema de investigación integrándolo con el modelo formativo.

El campus Politécnico (Sede Matriz) está ubicado en: Av. Gral. Rumiñahui s/n Sangolquí – Ecuador.

4.2.2 Propósito

La evaluación realiza un análisis basado en los dominios de COBIT 5, específicamente el dominio de Entrega, Servicio y Soporte. El cual hace referencia a Gestionar Operaciones, Gestionar Peticiones e incidentes de servicio, Gestionar Problemas, Gestionar la Continuidad, Gestionar Servicios de Seguridad y Gestionar Controles de Procesos de Negocio. Que tienen por objetivo establecer lineamientos y/o controles para llevar por buen camino a la Unidad de Tecnologías de Información y Comunicación (UTIC).

4.2.3 Área de TI que es objeto de la evaluación

El área de la Universidad de las Fuerzas Armadas ESPE que es objeto esta evaluación es la Unidad de Tecnologías de Información y Comunicación (UTIC).

4.3 Resumen Ejecutivo

Considerando que la Universidad de las Fuerzas Armadas ESPE, es una Institución que se preocupa por la optimización de sus recursos con base al mejoramiento de los procesos, la aplicación de políticas reglas y procedimientos y el aseguramiento de sus sistemas de información; se hizo necesario aplicar una evaluación técnica informática del entorno de Entrega, Servicio y Soporte a cargo de la Unidad de Tecnologías de Información y Comunicación (UTIC). Para este efecto se estableció un procedimiento basado en el estándar internacional COBIT 5, que establece parámetros para conocer el estado de la situación actual, actividades, funcionamiento y esfuerzos por mejorar su organización.

Se realizó una serie de procedimientos, entre ellos, la alineación de los Objetivos del Plan Estratégico de Desarrollo Institucional ESPE y los Objetivos Estratégicos de COBIT® 5, obteniendo como resultado ciertos hallazgos en los procesos y actividades más relevantes correspondientes a la Entrega, Soporte y Servicio tales como:

- Gestión de Operaciones
- Gestión de Problemas
- Gestión de la Continuidad
- Gestionar los Servicios de Seguridad

Los hallazgos evidencian inconformidades en los servicios prestados por la Unidad de Tecnologías de Información y Comunicación (UTIC), que reflejan la insatisfacción de los usuarios. Así como por ejemplo la falta de políticas clave para seguridad empresarial, la elaboración de planes y programas que permitan asegurar la confiabilidad, la integridad y disponibilidad de la información. No existe evidencia de comunicación entre las partes interesadas clave, lo que impide el correcto seguimiento y monitoreo a los procesos.

4.4 Alcance a la Evaluación

En conformidad al Proyecto Institucional de la Universidad de las Fuerzas Armadas ESPE, dirigida por el Ing. Mario Ron Egas, se procedió a realizar una Evaluación Técnica Informática para los procesos de Entrega, Servicio y Soporte a cargo de la Unidad de Tecnologías de Información y Comunicación (UTIC) utilizando la metodología COBIT 5 establecido por ISACA, se toma como base el período de gestión del año 2014. Cabe señalar que se tomaron en cuenta a ciertos subprocesos relevantes después de la alineación o mapeo de los Objetivos Estratégicos de la ESPE, los Objetivos de TI y los Objetivos de COBIT 5, es así: Gestión de Operaciones, Problemas, Continuidad y Servicios de Seguridad.

4.5 Objetivos de la Evaluación

La Evaluación Técnica Informática se enfoca en los procesos de Entrega, Soporte y Servicio de la Universidad de las Fuerzas Armadas ESPE sede matriz, siendo responsable de su gestión la Unidad de Tecnologías de Información y Comunicación (UTIC). Para ello se plantearon los siguientes objetivos:

- Determinar la situación actual de los procesos de Entrega, Soporte y Servicio a cargo de la Unidad de Tecnologías de Información y Comunicación (UTIC), así como las actividades realizadas para lograr los objetivos propuestos de la ESPE.
- Aplicar el marco de referencia COBIT 5 publicado por ISACA en la evaluación técnica informática.

- Analizar la información proporcionada durante la evaluación y confrontarla con los parámetros que establece COBIT 5, específicamente en temas de gestión de operaciones, problemas, continuidad, servicios de seguridad.
- Identificar la satisfacción del usuario sobre los servicios que ofrece Unidad de Tecnologías de Información y Comunicación (UTIC) a través de una encuesta.
- Elaborar y presentar el informe con las respectivas conclusiones y recomendaciones.

4.6 Metodología de la Evaluación

Pre-evaluación / planificación de la evaluación

Para determinar el alcance y los objetivos, se realiza una pre-evaluación (planificación de la evaluación), la cual incluye la obtención y registro de una comprensión de la misión de la UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE sede Matriz, de las operaciones de negocios relevantes y tecnología de apoyo.

Se identifica las necesidades operacionales, legales y reglamentarias y la infraestructura de la organización de TI, mediante la revisión de la documentación relevante y realizando entrevistas al equipo de trabajo a evaluar. Además se llevan a cabo visitas a las instalaciones de la ESPE, áreas operativas de TI y una evaluación de los procesos.

El Plan de Evaluación incluye:

- Obtención y revisión de políticas y procedimientos.
- Obtención y revisión de contratos y/o pólizas con terceros.
- Obtención y revisión de planes.
- Obtención y revisión de seguridad de la información.
- Identificar debilidades en la prestación de servicios.
- Identificar los criterios de la evaluación y determinar la idoneidad de los controles.

Se desarrollan objetivos de la evaluación en relación con los controles identificados y objetivos operativos. La estrategia de evaluación está en relación con el alcance y los objetivos de la evaluación.

4.7 Ejecución de la Evaluación

Para el desarrollo del presente trabajo se utiliza la metodología Auditoría de Cumplimiento, se utilizan también Estándares Internacionales y Nacionales, Normas y Leyes del Estado Ecuatoriano. Además de ciertos métodos que ayudan a fundamentar la investigación, tal como el método Deductivo -Inductivo con el que se analiza todo el entorno actual del proceso de entrega y soporte de la ESPE para posteriormente analizar sus componentes; cabe mencionar que el método analítico estudia a detalle cada parte o elemento que lo integra y su relación entre sí, tomando en cuenta herramientas como: encuestas, entrevistas, observación directa, análisis comparativo y elaboración de informes.

La evaluación se realiza de acuerdo con la Auditoría de Sistemas de Información (SI), normas de aseguramiento y directrices de aseguramiento emitidos por ISACA y prácticas de la industria generalmente aceptados. Los criterios de evaluación que se utilizan en este trabajo incluyen políticas de gestión y procedimientos, y las directrices de control de gestión que se exponen en COBIT® 5, según lo que publica ISACA.

4.8 Resultados de la Evaluación

El propósito de esta sección es proporcionar una explicación detallada de los resultados de la evaluación, recomendaciones y respuestas de la administración.

4.8.1 Procedimiento de gestión de operaciones.

Observación SS-01

No existe evidencia de procedimientos documentados para la gestión de operaciones dentro de la Unidad de Tecnologías de Información y Comunicación (UTIC).

Condición

Con base a los documentos enviados por la Unidad de Tecnologías de Información y Comunicación (UTIC), se evidencia que no existen procedimientos o

programaciones documentados sobre actividades relacionadas al apoyo de los servicios entregados. Se encentra una Planificación de la UTIC 2014 a nivel general por áreas (Evidencia. E001), donde se detallan acciones a llevarse a cabo tales como: mantenimiento, inventarios, implementaciones, ejecuciones, y la elaboración de algunos planes. Al aplicar el cuestionario de control a través de la observación directa de gestión de operaciones se comprueba la falta de estos documentos (Evidencia. IN-CH-UTIC-005-1).

Criterio

COBIT V5, en el proceso: Gestionar Operaciones, DSS01.01 Ejecutar procedimientos operativos. Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.

Causa

- No existe evidencia de gestión por parte de la Unidad de Tecnologías de Información y Comunicación (UTIC) para la elaboración de dichos procedimientos, programaciones operativas.
- No se da la debida importancia a la planificación propuesta, de tal forma que se ha incumplido con tiempos y plazos establecidos.

Efecto

Al no contar con procedimientos o programaciones de actividades operativas no se podría brindar el apoyo necesario a los servicios entregados por la Unidad de Tecnologías de Información y Comunicación (UTIC), de tal forma que dificultaría la gestión, el desempeño y rendimiento, e impidan que los usuarios reciban los resultados esperados de una forma segura, precisa y oportuna. RIESGO ALTO.

Recomendación SS-01

El Director de la Unidad de Tecnologías de Información y Comunicación (UTIC), dentro de sus atribuciones y responsabilidades emitirá directrices y/o lineamientos, o la implementación de planes, políticas, normas, estándares, procesos y procedimientos para la ejecución y agilidad de los procesos de la gestión de TIC, de forma inmediata en conformidad con lo que se explica en el Art. 38 del Reglamento Orgánico de la Universidad ESPE. (Evidencia.E012)

4.8.2 Políticas de Seguridad y Lineamientos regulatorios

Observación SS-02

No existe evidencia de políticas de seguridad en la Institución y lineamientos regulatorios.

Condición

Durante la verificación de los documentos proporcionados por la Unidad de Tecnologías de Información y Comunicación (UTIC), no se encontraron políticas de seguridad documentadas, (Evidencia. IN-CH-UTIC-005-1 "Control de documentos Gestión de Operaciones"), pese a que en la Planificación de UTIC 2014 (Evidencia. E001) está registrada la siguiente actividad: elaboración, aprobación e implementación de políticas de TICs, junto a la implementación del proceso de seguridad informática con tiempos estimados de 70 y 90 días respectivamente. Además, se evidencia que en el Plan de capacitación UTIC 2014 (Evidencia. E011) se considera que el personal se capacite en temas de seguridad informática con base en la norma ISO 27000, para ampliar sus conocimientos y destrezas, la misma que se desarrolló en los meses de mayo, junio, agosto y septiembre del 2014.

Criterio

COBIT V5, en el proceso: DSS DSS01.01 Ejecutar procedimientos operativos. Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.

- Asegurar que se cumple con los estándares de seguridad aplicables para la recepción, procesamiento, almacenamiento y salida de datos de forma tal que se satisfagan los objetivos empresariales, la política de seguridad de la empresa y los requerimientos regulatorios.
- Verificar que todos los datos esperados para su procesamiento sean recibidos y procesados por completo y de una forma precisa y oportuna. Entregar los resultados de acuerdo con los requisitos de la empresa. Dar soporte a las necesidades de reinicio y reprocesamiento. Asegurar que los usuarios reciben los resultados adecuados de una forma segura y oportuna.
- Programar, realizar y registrar las copias de respaldo de acuerdo con las políticas y procedimientos establecidos.

Causa

- No existe evidencia de marcos de referencia, procedimientos, estándares, guías o mejores prácticas que permitan desarrollar políticas que aseguren la correcta aplicación de las medidas de seguridad.
- No se evidencia la gestión por parte de la Unidad de Tecnologías de Información y Comunicación (UTIC) para iniciar con la elaboración y posterior implementación de políticas de seguridad.

Efecto

Si no se establecen e implementan políticas de seguridad documentadas, no se podría proporcionar la guía adecuada para que se cumplan normas, directrices o procedimientos relacionados a seguridad; de tal manera que el personal actúe como necesita la gerencia bajo un entorno de regulación legal o técnico. Así mismo no se podría proveer de las condiciones apropiadas de protección de los activos de

información, incrementando el riesgo de pérdida de la misma, por ende evitando que se cumplan los atributos de confidencialidad, integridad y disponibilidad. RIESGO ALTO.

Recomendación SS-02.1

El Director de la Unidad de Tecnologías de la Información y Comunicación (UTIC), debe desarrollar e implementar de manera inmediata Políticas de seguridad empresarial y lineamientos regulatorios que abarquen niveles corporativos y departamentales tal como lo establece el Art. 38 del Reglamento Orgánico de Gestión Organizacional de procesos codificado de la Universidad ESPE (Evidencia. E012); cubriendo temas como: requerimientos de seguridad infraestructura de la organización, directrices y procedimientos, clasificación de la información, estrategias de gestión de riesgos, planes de contingencia, obligaciones legales, subcontratación, manejo de incidentes, etc., es decir que se enfoquen en la protección de los sistemas, servicios y recursos. Este documento debe darse a conocer a todo el contingente de la empresa, de acuerdo con lo estipulado en el proceso (COBIT 5- DSS05 Gestionar Servicios de Seguridad).

Recomendación SS-02.2

El Director de la Unidad de Tecnologías de Información y Comunicación (UTIC) con su equipo de trabajo, deberá comprobar la efectividad de las políticas de seguridad de forma periódica y así verificar que los controles implantados se cumplan. Dichas revisiones también pueden ser solicitadas a empresas o consultores externos, en base a lo establecido en el proceso (COBIT 5- DSS05 Gestionar Servicios de Seguridad).

4.8.3 Uso de Diagramas de cableado TI

Observación SS-03

No existe Diagramas de cableado de Tecnología de Información (TI) en la Unidad de Tecnologías de Información y Comunicación (UTIC).

Condición

En la revisión de los documentos presentados por la Unidad de Tecnologías de Información y Comunicación (UTIC), no se encontró diagramas de cableado de Tecnología de Información (TI), (Evidencia. IN-CH-UTIC-005-Cuestionario de control). Durante la visita a sus instalaciones se evidencia desorganización en el cableado de la red (Evidencia. EF010).

Criterio

COBIT V5, en el proceso: DSS01.05 Gestionar las instalaciones.- Gestionar las instalaciones, incluyendo equipos de electricidad y comunicaciones, en línea con las leyes y regulaciones, requerimientos técnicos y de negocio y directrices de salud y seguridad en el trabajo.

- Núm. 5.- Asegurar que el cableado y el *patching* físico (datos y telefonía) están estructurados y organizados. Las estructuras de cableado y de conductos debieran estar documentadas (p.ej. plano del edificio y diagramas de cableado).
- Num6**.-** Analizar las instalaciones que alojan los sistemas de alta disponibilidad para verificar el cumplimiento de los requerimientos de cableado (externo e interno) en cuanto a redundancia y tolerancia a fallos.

Causa

- No existe evidencia de gestión por parte de la Dirección de la Unidad de Tecnologías de Información y Comunicación (UTIC), para desarrollar el

levantamiento de información a través de diagramas sobre el cableado tanto de la UTIC así como de la Universidad en general.

- No se evidencia el aseguramiento del estado o mantenimiento que se le da a la red cableada dentro de la Unidad de Tecnologías de Información y Comunicación (UTIC).

Efecto

La no diagramación impide que exista una buena administración de la infraestructura de TI especialmente cuando existen cambios en la ubicación de personas y equipos informáticos, donde se puede requerir una inversión adicional, con lo cual no se puede llevar un control adecuado donde se verifique las necesidades de los usuarios finales. RIESGO MEDIO.

Recomendación SS-03.1

El Director de la Unidad de Tecnologías de Información y Comunicación (UTIC), con su equipo de trabajo deberán asegurar que el cableado esté organizado y estructurado de forma documentada, es decir a través de la elaboración del diagrama de cableado de TI con base a los planos del edificio, de forma inmediata. Esto mejorará la oportunidad de tomar decisiones respecto a la configuración e instalación de la red de la Institución según lo establecido por COBIT 5 - Proceso DSS01.05 num5 en el tema gestión de instalaciones.

4.8.4 Ubicación de Centro de Datos

Observación SS-04

Incorrecta ubicación de las Instalaciones de Unidad de Tecnologías de Información y Comunicación (UTIC), (Centro de Datos).

Condición

En la visita realizada a las instalaciones de la Unidad de Tecnologías de Información y Comunicación (UTIC), se observa que el Centro de Datos se ubica en el primer piso del edificio Bloque A de la ESPE matriz y una de las puertas está cerca a uno de los pasillos donde existe transito frecuente de personas. (Evidencia.EF-021-fotografía del Centro de Datos).

Criterio

COBIT V5, en los procesos: DSS01.04 Gestionar el entorno. Mantener las medidas para la protección contra factores ambientales. Instalar equipamiento y dispositivos especializados para supervisar y controlar el entorno.

- Núm. 1.- Identificar desastres naturales y causados por el ser humano que puedan ocurrir en el área donde se encuentran las instalaciones de TI. Evaluar el efecto potencial en las instalaciones de TI.
- Núm. 2.- Identificar de qué manera el equipamiento de TI, incluyendo el equipamiento móvil y el ubicado fuera de las instalaciones, está protegido contra las amenazas del entorno. Asegurar que la política limite o impida comer, beber y fumar en áreas sensibles y que se prohíba el almacenamiento de material de oficina y otros suministros que puedan representar un riesgo de incendio en los centros de procesamiento de datos.
- Num3.- Ubicar y construir las instalaciones de TI para minimizar y mitigar la susceptibilidad ante las amenazas del entorno.
- Num7.- Asegurar que los sitios de TI están construidos y diseñados para minimizar el impacto del riesgo del entorno (p.ej. robo, aire, fuego, humo, agua, vibración, terrorismo, vandalismo, productos químicos, explosivos). Considerar zonas específicas de seguridad o celdas a prueba de incendio (p. ej. ubicando los entornos/servidores de producción y de desarrollo alejados entre sí).

DSS01.05 Gestionar las instalaciones. Gestionar las instalaciones, incluyendo equipos de electricidad y comunicaciones, en línea con las leyes y regulaciones, requerimientos técnicos y de negocio y directrices de salud y seguridad en el trabajo.

- Núm. 11.- Analizar las alteraciones físicas a los sitios o localizaciones de TI para reevaluar el riesgo del entorno (p.ej. daño por fuego o agua). Informar los resultados de este análisis a los niveles directivos de continuidad de negocio y de gestión de edificios.

Causa

- No existe una evaluación técnica sobre la ubicación de las instalaciones de la Unidad de Tecnologías de Información y Comunicación (UTIC), especialmente del Centro de Datos donde se analice el riesgo de desastres naturales y los provocados por el hombre. No existe evidencia de gestión de la Dirección de UTIC.
- No existe evidencia de normas, procedimientos o estándares que se apliquen para establecer las condiciones y por ende la adecuada ubicación del Centro de Datos.

Efecto

La incorrecta ubicación de las instalaciones de la Unidad de Tecnologías de Información y Comunicación (UTIC) y el Centro de Datos puede provocar que la información tenga un RIESGO ALTO de pérdida, pues no tiene las seguridades suficientes como por ejemplo las estipuladas en el estándar TIA 942.

Recomendación SS-04.1

Dentro de la responsabilidades que tiene el Director de la Unidad de Tecnologías de Información y Comunicación (UTIC) en cuanto a tecnologías de Infraestructura de TIC operativas (Centro de Datos, sitios de redundancia, cuartos de comunicación, servidores físicos y virtuales); deberá realizar inmediatamente una evaluación técnica a las instalaciones de dicha Unidad y el Centro de Datos tomando en cuenta el criterio técnico del Director de Seguridad Física, considerando los posibles riesgos naturales y los provocados por el hombre con el fin de salvaguardar la información en relación a lo mencionado al Art. 38. Lit. k del Reglamento orgánico de gestión organizacional de procesos codificados de la Universidad ESPE. (Evidencia. E012) y de acuerdo a lo

que establece COBIT 5. Proceso DSS01.04 en la gestión del entorno, donde se analiza la ubicación y construcción de las instalaciones de TI para minimizar y mitigar la susceptibilidad ante las amenazas del entorno.

Recomendación SS-04.2

El Director de la Unidad de Tecnologías de Información y Comunicación (UTIC) como una de sus atribuciones y responsabilidades debe coordinar de forma inmediata la formulación de iniciativas y mecanismos, para la implementación de políticas, normas, estándares, procesos y procedimientos para agilizar los procesos de la gestión de Tecnologías de Información y Comunicación (TIC), para el caso, lo relacionado a la correcta ubicación de las instalaciones de UTIC y el Centro de Datos, de acuerdo a lo mencionado en el Art. 38, lit. u del Reglamento orgánico de gestión organizacional de procesos codificados de la Universidad ESPE.

4.8.5 Catálogo de problemas

Observación SS-05

No existe evidencia de un catálogo de gestión de problemas.

Condición

Entre los documentos entregados por la Unidad de Tecnologías de Información y Comunicación (UTIC), se verifica que no existe evidencia de un catálogo de problemas; se identifican reportes generales de incidentes, errores y problemas de acuerdo al control de documentos sobre gestión de problemas (Evidencia. IN-CH-UTIC-006-1).

Criterio

COBIT V5, en el proceso: DSS03.01 Identificar y clasificar problemas. Definir e implementar criterios y procedimientos para informar de los problemas identificados, incluyendo clasificación, categorización y priorización de problemas.
DSS03.02 Investigar y diagnosticar problemas. Investigar y diagnosticar problemas utilizando expertos en las materias relevantes para valorar y analizar las causas raíz.
DSS03.03 Levantar errores conocidos. Tan pronto como las causas raíz de los problemas se hayan identificado, crear registros de errores conocidos y una solución temporal apropiada, e identificar soluciones potenciales.
DSS03.05 Realizar una gestión de problemas proactiva. Recoger y analizar datos operacionales (especialmente registros de incidentes y cambios) para identificar tendencias emergentes que puedan indicar problemas. Registrar problemas para permitir la valoración.

Causa

- No existe bitácora de registros de problemas detallados.
- No existen grupos definidos de soporte para el análisis de la causa raíz de problemas.
- No existe evidencia de un catálogo de gestión de problemas.
- No existen informes sobre problemas identificados y a su vez el análisis de impacto y costos en los servicios de la Unidad de Tecnologías de Información y Comunicación (UTIC).

Efecto

La falta de un catálogo de gestión de problemas en la Unidad de Tecnologías de Información y Comunicación (UTIC), evita la oportuna identificación de problemas y a su vez la generación de pistas de auditoría sobre los procesos de gestión de los mismos, incluyendo el estado de cada uno de ellos. RIESGO ALTO.

Recomendación SS-05.1

El Director de la Unidad de Tecnologías de Información y Comunicación (UTIC), deberá implementar de forma inmediata una bitácora del registro y la clasificación de problemas de información, con el fin de mantener registrado dichos problemas y determinar ciertas estrategias para su resolución y futuras referencias, de acuerdo a sus atribuciones y responsabilidades de la provisión del servicio de TICs establecidos en el Art. 38. Lit. e del Reglamento Orgánico de gestión organizacional de procesos codificado (Evidencia. E012) y COBIT 5. Proceso DSS03.01.

Recomendación SS-05.2

El Director de la Unidad de Tecnologías de Información y Comunicación (UTIC) deberá definir de forma inmediata, grupos de soporte adecuados tales como: hardware, software, aplicaciones y software de soporte, para ayudar en la identificación de dichos problemas y su posterior solución, a través del análisis de la causa raíz, con lo cual también se pueda mantener un catálogo de gestión de problemas, conforme a COBIT 5. Proceso DSS03.01. Numeral 3 y 6.

Recomendación SS-05.3

El Director de la Unidad de Tecnologías de Información y Comunicación (UTIC), deberá solicitar informes mensuales del progreso de la resolución de problemas, así como supervisar el continuo impacto de los problemas, incidentes y errores conocidos en los servicios y analizar los costes totales con los responsables de los procesos, en relación a lo que establece COBIT 5. Proceso DSS03.05.

4.8.6 Gestión de Cambios

Observación SS-06

No existe evidencia de gestión de cambios con base a problemas.

Condición

Entre los instrumentos y técnicas de investigación utilizados para realizar la respectiva evaluación, se aplica el cuestionario de control en relación a gestión problemas (Evidencia. IN-CH-UTIC-006-1), dentro del cual también se menciona el tema de gestión de cambios, donde se verifica que la Unidad de Tecnologías de Información y Comunicación (UTIC) no posee evidencia sobre gestión de cambios, específicamente informes en base a problemas.

Criterio

COBIT V5, en el proceso: DSS03.05 Realizar una gestión de problemas proactiva. Recoger y analizar datos operacionales (especialmente registros de incidentes y cambios) para identificar tendencias emergentes que puedan indicar problemas. Registrar problemas para permitir la valoración.

Causa

- No hay documentos que evidencie la gestión de cambios.
- No existe evidencia de informes, documentos de supervisión o actas de reuniones periódicas entre los responsables de gestión de cambios y los responsables de los procesos.

Efecto

La no elaboración de Informes, documentos de supervisión y actas de reuniones en base a la gestión de cambios evitará que exista una evaluación y planificación de los procesos de cambios y calidad de continuidad del servicio de TI. RIESGO MEDIO.

Recomendación SS-06

Es necesario que el Director de la Unidad de Tecnologías de Información y Comunicación (UTIC) implemente de forma inmediata una bitácora de cambios,

además documentar periódicamente a través de minutas las decisiones del comité de cambios y las partes interesadas de acuerdo a lo estipulado en el Art. 38. Lit. d y e, en relación a las aplicaciones y desarrollo de servicios de TICs del Reglamento orgánico de gestión organizacional de procesos codificados de la Universidad ESPE. (Evidencia. E012).

4.8.7 Plan Continuidad del Negocio.

Observación SS-07

No existe evidencia de un Plan de Continuidad.

Condición

Entre los documentos solicitados a la Unidad de Tecnologías de Información y Comunicación (UTIC), no se encuentra el Plan de Continuidad del Negocio (BCP), (Evidencia. IN-CH-UTIC-007-1- Control de documentos en la Gestión de Continuidad), pero se evidencia la existencia de un Plan de contingencia de TI que contiene los parámetros básicos como, objetivos, políticas, personal encargado, actividades críticas, planes de prevención, ejecución, recuperación, pruebas, etc. (Evidencia. E010. Plan de Contingencia 2014); el mencionado Plan de Contingencia no presenta evidencia sobre implementación, ejercicios o pruebas y socialización del mismo. (Evidencia. IN-CH-UTIC-007-1, control de documentos-Gestionar la Continuidad).

Criterio

COBIT V5, en el proceso: DSS04 Gestionar la Continuidad**.-** Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.

DSS04.01 Definir la política de continuidad de negocio, objetivos y alcance. Definir la política y alcance de continuidad de negocio alineada con los objetivos de negocio y de las partes interesadas.
DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.
Desarrollar un plan de continuidad de negocio (BCP) basado en la estrategia que documente los procedimientos y la información lista para el uso en un incidente para facilitar que la empresa continúe con sus actividades críticas.

Causa

- No existe evidencia de la gestión de quienes conforman las partes interesadas del negocio junto con los propietarios de los diferentes procesos, gestores de la continuidad, servicios y operaciones del negocio, para la elaboración del Plan de Continuidad del Negocio (PCN).
- No existe un marco de referencia o procedimiento para desarrollar una Plan de continuidad del negocio.

Efecto

Al no contar con un Plan de Continuidad del negocio (PCN) no se podrá cubrir la parte preventiva, puesto que el Plan de Contingencia es utilizado únicamente cuando ha habido un desastre; el mencionado plan es parte del BCP, y es aquí donde se analizan las posibles vulnerabilidades y soluciones para mitigar los riesgos a nivel de todo el negocio o Institución, de esta manera garantizar que se pueda operar con las actividades críticas, evaluar y hacer mejoras al mismo. RIESGO ALTO.

Recomendación SS-07.1

El Director de seguridad integrada deberá elaborar de forma inmediata el Plan de Continuidad del Negocio, de acuerdo a lo que establece COBIT 5 en el proceso DSS04- Gestionar la continuidad.

Recomendación SS-07.2

El Director de la Unidad de Tecnologías de Información y Comunicación (UTIC), emitirá un plan de contingencia y recuperación de desastres informáticos y realizar informes de ejecución del mencionado plan, evaluar y mejorar el Plan de Contingencia anualmente de acuerdo al Art 38. Lit. f y m del Reglamento Orgánico de Gestión Organizacional procesos codificado de la Universidad ESPE. (Evidencia. E012)

4.8.8 Seguridad de la Información.

Observación SS-08

No existe evidencia de Seguridad de la Información.

Condición

A través de cuestionarios aplicados al Jefe de la Unidad de Tecnologías de Información y Comunicación (UTIC), se establece que no se realizan pruebas de consistencia de los datos respaldados, (Evidencia. CUE-HL-04-PLAN-2); además la información de la red no está cifrada, no se realizan pruebas de intrusión en la red, el acceso remoto está habilitado para cualquier persona, no se han definido roles para los diferentes usuarios, no existen políticas de seguridad para la destrucción de formularios, no se registra inventarios de documentos sensibles y dispositivos de salida, como tampoco existe un registro con el número de porcentaje de individuos que reciben formación de concientización relativa al uso de dispositivos de usuario final, o registro con el número de incidentes que impliquen dispositivos de usuario final y están habilitados los puertos USB, CD-ROM.(Evidencia. CUE-HL-05-PLAN).

Criterio

COBIT V5, en el proceso: DSS05 Gestionar Servicios de Seguridad.- Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.

Causa

- No existe evidencia de informes donde analice los incidentes suscitados que atentan contra la seguridad de la información, es decir un detalle de costos, impactos, volumen.
- No existen políticas de seguridad documentadas que guíen el desarrollo de criterios en situaciones concretas y así mismo sean soportadas por procedimientos o buenas prácticas.

Efecto

Al no contar con mecanismos de protección o medidas preventivas de seguridad, el bien más importante como es la información se ve afectado enormemente siendo un RIESGO ALTO para la organización, con lo cual no se puede garantizar la confidencialidad, disponibilidad e integridad de la misma, por ende registrar grandes impactos económicos.

Recomendación SS-08.1

El Director de la Unidad de Tecnologías de la Información y Comunicaciones entre sus atribuciones y responsabilidades con respecto al tema de infraestructura de TICs, deberá adecuar de forma inmediata procedimientos para las Tecnologías de la seguridad de la información operativas (cortafuegos, administración de cuentos de usuarios, detección y prevención de intrusos, antivirus, capas de socket segura (SSL), conexión única "Single Sign on- 550", biometría, cifrado, acceso remoto, firma digital,

transferencia electrónica segura "SET", tecnologías de monitoreo, de acuerdo a lo indicado en el Artículo 38, lit. l, del Reglamento Orgánico de Gestión Organizacional procesos codificado de la Universidad ESPE (Evidencia. E012) y COBIT 5 en el proceso DSS05.02.

Recomendación SS-08.2

Es necesario que el Director de la Unidad de Tecnologías de Información y Comunicación (UTIC), establezca inmediatamente mecanismos de divulgación y concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención de acuerdo a COBIT 5, proceso DSS05. 01.

Recomendación SS-08.3

El Director de la Unidad de Tecnologías de Información y Comunicación (UTIC), emitirá políticas de seguridad de forma inmediata, con la finalidad de apalancar las medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión en relación a COBI 5, proceso DSS05.02.

4.9 Conclusiones de la Evaluación

- A través de la evaluación técnica informática al proceso de Entrega, Soporte y Servicio bajo el marco de parámetros y criterios de COBIT 5 publicado por ISACA, se obtuvo como resultado que la Gestión de Operaciones tuvo más deficiencias, seguida por la Gestión de Problemas, Gestión de Continuidad y servicios de seguridad.
- La Unidad de Tecnologías de Información y Comunicación (UTIC), no dispone de un Plan Operativo que establezca información definida en cuanto a los procedimientos y actividades operativas a desarrollarse como apoyo a los servicios entregados.
- La Unidad de Tecnologías de Información y Comunicación (UTIC) no dispone de un Plan de Continuidad del Negocio, que analice las estrategias, los procedimientos para mitigar, prevenir y corregir de forma integral ante la

posibilidad de que incidentes inesperados ocurran, de tal manera que la productividad de la Institución no se detenga, o dicha situación tenga menores impactos.

- En el Plan de capacitaciones 2014 de la Unidad de Tecnologías de Información y Comunicación (UTIC) no se ha considerado una capacitación en temas de COBIT 5, publicado por ISACA que aporte o proporcione un marco integral que ayude a la Institución a lograr sus metas y entregar valor, donde además se mejore el gobierno y la administración de los activos de TI y de la información.
- Se elaboró un informe que contemple la información recopilada durante la evaluación y sea analizada por las partes interesadas de la Institución.

4.10 Recomendaciones de la Evaluación

- El Director de la Unidad de Tecnologías de la Unidad de Tecnologías de Información y Comunicación (UTIC), debe definir de forma inmediata políticas, lineamientos regulatorios, metodologías y procedimientos que no se evidenciaron en esta evaluación como parte de la gestión de cambios y por ende mejorando la calidad de los servicios.

- Es necesaria la capacitación en marcos integrales tal como COBIT 5 que involucran un alineamiento con los marcos y normas relevantes usados por organizaciones, ejm: COSO ERM, COSO, ISO/9000, 31000, 38500, 27000, TOGAF, PMBOK ITIL, CMMI etc.

- Desarrollar un plan operativo por parte de la Unidad de Tecnologías de Información y Comunicación (UTIC), donde se mantenga una programación de actividades operativas y se gestione el desempeño y rendimiento de las dichas actividades, aplicando estándares de seguridad para la recepción, procesamiento, almacenamientos y salida de datos.

- Elaborar un Plan de Continuidad de forma urgente, tomando en cuenta que éste incluye al Plan de Contingencia. Puesto que la diferencia radica en que el

Plan de Contingencia es utilizado cuando ya ha habido un desastre, mientras que el de Continuidad aparte de establecer medidas en casos de desastre también analiza vulnerabilidades y desarrolla contramedidas que mitiguen las mismas, es decir que este plan no solo es curativo sino además preventivo.

- Tomar en cuenta el informe presentado posterior a la evaluación donde se muestra información concisa de las deficiencias encontradas en los diferentes procesos, y puedan servir como base para tomar decisiones que implique cambio y mejora continua.

.

CAPÍTULO V

5.1 Conclusiones

- COBIT 5 es un modelo o marco de referencia que permite evaluar y auditar el gobierno y la gestión de los sistemas de información y sus recursos tecnológicos, en conformidad con las buenas prácticas y el control que debe mantenerse en la Institución.

- Es importante contar con la documentación requerida a las unidades organizacionales involucradas en la evaluación, en el momento oportuno, porque de lo contrario el proyecto se retrasa y no se consigue cumplir con los tiempos programados.

- Dentro de la evaluación técnica informática se aplicaron algunos instrumentos de investigación así como por ejemplo: encuestas dirigidas a Estudiantes, Docentes y Administrativos, a través de las cuales se pudo identificar que los estudiantes siendo el grupo de usuarios más numeroso e importante de la Universidad, manifiestan no tener completa satisfacción por los servicios que ofrece la Unidad de Tecnologías de Información y Comunicación (UTIC) en cuanto a la Entrega, Servicio y Soporte, a la vez hacen partícipe la opinión los dos grupos de usuarios restantes para solicitar que se analice la situación y se gestionen cambios inmediatos en servicios como Banner e Internet.

- Los informes presentados permitieron recopilar información concisa sobre la evaluación realizada y mostrarla como resultado de la verificación al estado actual de los procesos perteneciente a la Entrega, Servicio y Soporte donde se destacan la deficiencia en cuanto a: implementación de políticas de seguridad empresarial, roles y responsabilidades definidos, evaluaciones, seguimiento y monitoreo de procesos, y comunicaciones permanentes entre las partes interesadas plasmadas como compromisos.

5.2 Recomendaciones

- Para mejorar las deficiencias en los controles de los procesos especialmente en la Entrega, Servicio y Soporte a cargo de la Unidad de Tecnologías de Información y Comunicación (UTIC) se puede tomar como marco de referencia COBIT 5, para ello se sugiere la capacitación oportuna a todo el personal de esta unidad para que esté involucrada y en conocimiento de las mejoras que esta herramienta brinda.

- Desarrollar e implementar de manera urgente un Plan de seguridad informático en base a políticas de seguridad y lineamientos regulatorias que permitan normar acciones que busquen cumplir con los requerimientos de confidencialidad, autenticidad integridad y disponibilidad de la información.

- Es necesario mejorar la calidad a nivel de todos los servicios de la Universidad y para ello se requiere que el personal conozca sus roles y responsabilidades evitando el innecesario acaparamiento de otras actividades que se traducen en retraso para la entrega del producto final hacia el usuario.

- Que los informes presentados, sean una muestra de conocimiento que motive la preocupación más profunda hacia procesos de TI y haya el compromiso de apoyo parte de las autoridades; además dichos informes sirvan como base para posteriores auditorias y así evidenciar y monitorear la evolución que mantiene la Unidad de Tecnologías de Información y Comunicación (UTIC).

6. Bibliografía

Academia de Administración. (12 de 2011). *Auditoría Informática.* Recuperado el 12 de 04 de 2015, de http://www.uaeh.edu.mx/docencia/P_Presentaciones/tlahuelilpan/sistemas/auditoria_informatica/auditoria_informatica.pdf

ANF, A. (2013). *Auditoría Informática*. Recuperado el 12 de 02 de 2015, de https://www.anf.ec/ec/servicios/actividades/auditoria-informatica.html

Arter, D. R. (2004). *Auditorías de la Calidad para su Comportamiento.* Recuperado el 02 de 05 de 2015, de https://books.google.com.ec/books?id=NpNx1iQVGwMC&pg=PT16&dq=SIGNIFICADO+DE+AUDITAR&hl=es&sa=X&ei=RtVVVb_XHIzdsASm6ID4Ag&ved=0CBsQ6AEwAA#v=onepage&q=SIGNIFICADO%20DE%20AUDITAR&f=false

Ferrer, J. (2010). *Blog-Conceptos Básicos de Metología de Investigación.* Recuperado el 03 de 12 de 2015, de http://metodologia02.blogspot.com/p/tecnicas-de-la-investigacion.html

ISACA. (2012). *COBIT 5 Introducción - Presentación de Power Point - Isaca.* Recuperado el 12 de 04 de 2015, de http://www.isaca.org/COBIT/Documents/COBIT5-Introduction-Spanish.ppt

ISACA. (2012). *COBIT 5 Introduction Spanish.* Panamá.

ISO 31000:2009, I. (2011). *Herramientas para evaluar la gestión de riesgos.* Recuperado el 01 de 05 de 2015, de http://www.isaca.org/chapters8/Montevideo/cigras/Documents/cigras2011-cserra-presentacion1%20modo%20de%20compatibilidad.pdf

KIT, I. E. (2015). *¿Qué es la Administración de Riesgo?* Recuperado el 06 de 04 de 2015, de http://www.kit.com.ar/boletines-a.php?id=0000037

Otalora Chisco, A. F. (1 de 10 de 2014). *Aseguramientos de Sistemas de Información*. Recuperado el 02 de 04 de 2015, de http://aseguramientosistemasdeinformacion.blogspot.com/

Peinado, J. I. (2015). Observación. En J. I. Peinado, *Métodos, Técnicas e Instrumentos de la Investigación criminológica* (pág. 525). Madrid: DYKINSON, S.L.

Razo, C. M. (1998). Instrumentos de la Investigación. En C. M. Razo, *Cómo Elaborar y Asesorar una Investigación de Tesis* (pág. 1524). México: Prentice Hall Hispanoamerican, S.A.

Summers, D. C. (2006). *Books.google.com*. Recuperado el 03 de 05 de 2015, de https://books.google.com.ec/books?id=xBgQ9R2io5oC&pg=PA35&dq=que+significa++NORMA+ISO&hl=es&sa=X&ved=0CCoQ6AEwAWoVChMI_9K76t7HxwIVBtUeCh0cXQ03#v=onepage&q=que%20significa%20%20NORMA%20ISO&f=false

Torrealba, C. (11 de 03 de 2009). *Blog-Técnicas de investigación Documental.* Recuperado el 03 de 12 de 2015, de http://dani14238551.blogspot.com/2009/03/la-recopilacion-documental-como-tecnica.html

Universidad de Sevilla. (13 de 05 de 2015). *Certificaciones:Seguridad de la Información*. Recuperado el 2015, de http://guiasbus.us.es/ingenieriacertificaciones/seguridadinformacion

VIRTUAL, E. (s.f.). *EUMET.NET.* Recuperado el 03 de 12 de 2015, de EUMET.NET.

Yuni, J. (2006). La investigación por Encuestas. En J. Yuni, *Técnicas para investigar* (pág. 66). Argentina: Editorial Brujas.