RESUMEN – TRABAJO DE GRADO

AUTORES	**MARÍA ALEJANDRA ARRIETA SÁNCHEZ, MAGRETH ROSSIO SANGUINO REYES Y CINDY LORENA LOBO SÁNCHEZ**
FACULTAD	**FACULTAD DE INGENIERIAS**
PLAN DE ESTUDIOS	**ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS**
DIRECTOR	**Msc. TORCOROMA VELASQUEZ PÉREZ**
TÍTULO DE LA TESIS	**DISEÑO DE UN PLAN ESTRATÉGICO DE TECNOLOGÍAS DE INFORMACIÓN PARA LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA**

RESUMEN

(70 palabras aproximadamente)

EL PRESENTE PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI ESTÁ SUSTENTADO EN LA NECESIDAD DE PROVEER UN MARCO DE ACCIÓN QUE SIRVA DE ESTRATEGIA A LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA, PARA OPTIMIZAR LA GESTIÓN DE LOS RECURSOS TECNOLÓGICOS Y SU INCORPORACIÓN A TODOS Y CADA UNO DE LOS PROCESOS ADMINISTRATIVOS Y ACADÉMICOS, PARA EL LOGRO DE SUS OBJETIVOS INSTITUCIONALES.

CARACTERÍSTICAS

PÁGINAS: 138	PLANOS:	ILUSTRACIONES:	CD-ROM: 1

DISEÑO DE UN PLAN ESTRATÉGICO DE TECNOLOGÍAS DE INFORMACIÓN PARA LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

MARIA ALEJANDRA ARRIETA SANCHEZ
MAGRETH ROSSIO SANGUINO REYES
CINDY LORENA LOBO SÁNCHEZ

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERÍAS
ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS
OCAÑA
2015

DISEÑO DE UN PLAN ESTRATÉGICO DE TECNOLOGÍAS DE INFORMACIÓN PARA LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

MARIA ALEJANDRA ARRIETA SANCHEZ
MAGRETH ROSSIO SANGUINO REYES
CINDY LORENA LOBO SÁNCHEZ

Trabajo de grado presentado para optar al título de Especialista en Auditoría de Sistemas

Director
TORCOROMA VELÁSQUEZ PÉREZ
Msc. Ciencias Computacionales

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERÍAS
ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS
OCAÑA
2015

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE CUADROS

pág.

LISTA DE ANEXOS

pág.

INTRODUCCIÓN

Dentro de los procesos de apoyo implementados en el Sistema Integrado de Gestión de la Universidad Francisco de Paula Santander Ocaña, el **Sistema de Información, Telecomunicaciones y Tecnología SITT**, tiene como fin administrar y mantener la infraestructura tecnológica de la Universidad, necesaria para el desarrollo de los procesos institucionales de una manera eficaz, efectiva y oportuna, buscando siempre, la satisfacción de sus clientes. Su campo de acción, va "desde la identificación de las necesidades de actualización, modernización y mantenimiento, hasta el aseguramiento en la prestación del servicio de tecnología y telecomunicaciones"[1].

Además de lo anterior, el SITT debe garantizar que la información que se administra, pueda cumplir con los requerimientos mínimos necesarios para dar el soporte a la toma de decisiones a nivel institucional y se pueda llevar a cabo el cumplimiento de su misión. Pero para lograr esto, se necesita el esfuerzo de todos y cada uno de los estamentos que componen la Universidad, en la implementación de herramientas que permitan la eficiencia y la mejora continua de sus procesos institucionales.

Para cumplir con lo anterior, se propone el diseño de un Plan Estratégico de Tecnologías de la Información PETI, dentro del marco de Gobierno de Tecnologías de la Información, en adelante TI, el cual define el enfoque tecnológico para la Universidad y la manera como éste se aplica a cada uno de los procesos institucionales. Para la elaboración del presente plan estratégico fue necesario, realizar una revisión del estado actual de las tecnologías de la información que soportan los servicios ofrecidos por la Universidad; la definición de componentes estratégicos de TI aplicables a la Institución y posteriormente, la formulación de programas y proyectos que deben ser ejecutados en un tiempo definido, para alcanzar las metas estratégicas.

En lo que tiene que ver con el texto que recoge la investigación realizada, éste se estructuró de la siguiente manera: en un primer capítulo, se plantea el problema identificado, los objetivos, la justificación y las delimitaciones de la propuesta planteada.

En el segundo capítulo, se muestra el Marco Referencial. En él se sustenta la necesidad de contar con un Plan estratégico de Tecnologías de Información, a fin de que la Universidad Francisco de Paula Santander Ocaña, pueda optimizar la gestión de sus recursos tecnológicos.

En el tercer capítulo, se socializa el diseño metodológico propuesto para la realización de la investigación.

[1] UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. División de Sistemas. Caracterización proceso Sistemas de Información, Telecomunicaciones y Tecnología, 2010.

En el cuarto capítulo, se muestran los resultados; esto es el análisis de la situación actual del proceso de adopción de tecnologías de la información en la Universidad y de la manera como se vienen gestionando, la identificación del estándar/metodología para el diseño del plan estratégico de tecnologías de información PETI y el documento que contiene todas las actividades relacionadas con el diseño del Plan Estratégico de Tecnologías de la Información PETI para la Universidad Francisco de Paula Santander Ocaña, para la vigencia 2016 – 2018.

Finalmente, el quinto y sexto capítulos, recogen las conclusiones y recomendaciones derivadas de la investigación.

1. TÍTULO

Diseño de un Plan Estratégico de Tecnologías de Información para la Universidad Francisco de Paula Santander Ocaña.

1.1 PLANTEAMIENTO DEL PROBLEMA

Dentro de los procesos institucionales de la Universidad Francisco de Paula Santander Ocaña, el proceso denominado Sistema de Información, Telecomunicaciones y Tecnología SITT, tiene como objetivo diseñar, administrar y mantener los sistemas de información, las telecomunicaciones y la infraestructura tecnológica utilizados para el desarrollo de los procesos académicos y administrativos de manera eficaz, efectiva y oportuna.

Dicho proceso, se encuentra alineado con el eje estratégico **Desarrollo Físico y Tecnológico,** contemplado en el *Plan de Desarrollo "Hacia la Excelencia Académica 2014 - 2019*"**,** que pretende "fortalecer la gestión tecnológica mediante una infraestructura adecuada para la realización de todas las actividades de la Institución, con el fin de garantizar el buen desarrollo de las mismas y brindar las herramientas necesarias para toda la comunidad"[2]. Sin embargo, hasta el momento el crecimiento tecnológico de la Universidad, se ha dado de forma coyuntural, en la medida en que las necesidades de administración de la información y de los demás recursos informáticos lo han requerido.

Una auditoría realizada a la seguridad física[3], permitió evidenciar que no ha existido una planeación apropiada en dicho crecimiento y que los procesos de implementación tanto de hardware como de software se han dado de manera espontánea en respuesta a los requerimientos propios del negocio. Existen actualmente sistemas de información independientes, -no integrados a los demás sistemas-, que en la mayoría de los casos, obligan a recurrir a métodos poco adecuados de aseguramiento de la información, generando así, redundancia de datos por no encontrarse centralizados y poniendo en riesgo su integridad, disponibilidad y confidencialidad, afectando notoriamente el producto de los procesos misionales (docencia, investigación y extensión) de la Universidad.

Lo anterior, conduce a evidenciar una serie de hechos que ponen en riesgo la adecuada utilización de las tecnologías de información en los procesos académicos y administrativos de la Universidad, reduciendo la posibilidad de ofrecer servicios académicos de calidad bajo un esquema de sostenibilidad, que solo puede darse, si se realiza una adecuada planeación en los procesos de incorporación de las tecnologías de información y comunicación, a todos y cada uno de los ejes estratégicos, de tal forma que se incrementen

[2] UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. Plan de Desarrollo Institucional 2014 – 2019.
[3] ARRIETA SÁNCHEZ, María Alejandra, et al. Evaluación de la Seguridad Física y Ambiental en la División de Sistemas de la Universidad Francisco de Paula Santander Ocaña, 2014.

las competencias institucionales de la Universidad, para dar cumplimiento a sus funciones e ingresar a un proceso de mejoramiento continuo y modernización.

1.2 FORMULACIÓN DEL PROBLEMA

¿Qué alternativa, enmarcada en el Gobierno de las Tecnologías de la Información, permitirá integrar los objetivos institucionales de la Universidad Francisco de Paula Santander con el enfoque de las Tecnologías de Información?

1.3 OBJETIVOS

1.3.1 General. Diseñar un Plan Estratégico de Tecnologías de Información para optimizar la gestión de los recursos tecnológicos de la Universidad Francisco de Paula Santander Ocaña.

1.3.2 Específicos. Realizar un análisis de la situación actual del proceso de adopción e implementación de las tecnologías de información en la Universidad Francisco de Paula Santander Ocaña.

Identificar la metodología más apropiada para el diseño del Plan Estratégico de Tecnologías de Información PETI para la Universidad Francisco de Paula Santander Ocaña.

Elaborar el documento que estructure el Plan Estratégico de Tecnologías de Información PETI para la Universidad Francisco de Paula Santander Ocaña.

1.4 JUSTIFICACIÓN

Durante los últimos años, la Universidad Francisco de Paula Santander Ocaña, ha estado impulsando su desarrollo institucional implementando diversos planes de desarrollo cada vez más ambiciosos, en los que se ha venido evidenciado un interés cada vez más creciente por la implementación de las Tecnologías de Información TI, las cuales se han constituido en el pilar fundamental sobre el cual se define su crecimiento y el fortalecimiento en la prestación de sus servicios académicos.

Como consecuencia del avance vertiginoso que han tenido las Tecnologías de Información TI durante los últimos años, la Universidad se ha venido preocupando por potenciar su quehacer académico y administrativo a través de la incorporación de estas tecnologías en sus procesos estratégicos, misionales y de apoyo. Prueba de ello es la implementación de los sistemas de información académico, financiero, bibliográfico, entre otros, la ampliación de la cobertura del servicio de Internet para todos los estamentos universitarios, la incorporación de una plataforma virtual como apoyo a la educación presencial, y otros procesos que se vienen dando con el fin de contribuir al logro de los objetivos

institucionales. Sin embargo, las acciones emprendidas no han cumplido cabalmente sus objetivos y a veces pareciera que cada una se da desligada de las otras.

Un plan estratégico de tecnologías de información se constituye en una herramienta que permite alinear los objetivos de TI con los objetivos institucionales, estableciendo las políticas requeridas para la adquisición, uso y administración de los recursos informáticos de tal manera que respondan a las necesidades organizacionales y contribuyan al éxito institucional.

Lo que se pretende con esta investigación es diseñar un Plan Estratégico de TI, a partir del diagnóstico de la situación actual de la Universidad Francisco de Paula Santander Ocaña, en cuanto a infraestructura tecnológica se refiere, de tal manera que se pueda establecer un modelo organizacional que integre un plan de tecnologías de información con los objetivos misionales de la Universidad, de tal forma que se haga un uso más eficiente de ella y pueda incluso, servir de referente para futuros estudios dentro de la misma institución o de otras afines.

1.5 DELIMITACIONES

1.5.1 Geográfica

La presente propuesta de Diseño de un Plan Estratégico de Tecnologías de Información, se desarrolló en la Universidad Francisco de Paula Santander Ocaña y abarcó los procesos estratégicos, misionales y de apoyo de la misma.

1.5.2 Temporal

La presente propuesta se desarrolló en un tiempo mínimo de seis (6) meses, a partir de la fecha de su aprobación.

1.5.3 Conceptual

El marco conceptual del presente proyecto abordó los siguientes desarrollos conceptuales:

Sistemas de Información SI, Tecnologías de Información TI, Telecomunicaciones, Gobierno de TI, Modelos de TI, Modelo de Organización, Planeación Estratégica y Plan Estratégico de TI.

1.5.4 Operativa

Para el desarrollo del proyecto propuesto, se llevaron a cabo las siguientes acciones:
En primer lugar, se realizó un diagnóstico de la situación actual del proceso de adopción de tecnologías de la información en la Universidad y de la manera como se vienen

gestionando, a través de una auditoría de cumplimiento bajo el estándar ISO/IEC 27002:2013.

En segundo lugar, se identificó la metodología más apropiada para el diseño del Plan Estratégico de Tecnologías de Información PETI para la Universidad Francisco de Paula Santander Ocaña.

Finalmente, se elaboró el documento del Plan Estratégico de Tecnologías de Información PETI para la Universidad Francisco de Paula Santander Ocaña, identificando y priorizando los proyectos tecnológicos y la forma como van a ser incorporados en las actividades académicas y administrativas desarrolladas por la Universidad.

2. MARCO REFERENCIAL

2.1 MARCO HISTÓRICO

El proceso evolutivo de la planeación estratégica se remonta a la Grecia antigua cuando Sócrates comparó las actividades de un empresario con las de un general, señalando que en toda tarea quienes se encarguen de llevar a cabo su debida ejecución debe hacer planes y mover recursos para alcanzar los objetivos deseados[4].

Años más tarde, Von Neumann y Morgenstern en su obra *La teoría del juego,* empiezan a combinar el concepto de estrategia y negocio, estableciendo que la estrategia "Es una serie de actos que ejecuta una empresa, los cuales son seleccionados de acuerdo con una situación concreta"[5].

Peter Drucker, considerado el padre del management, publica en 1954 *The Practice Of Management*, donde expresa que "La estrategia requiere que los gerentes analicen su situación presente y que la cambien en caso necesario, saber que recursos tiene la empresa y cuáles debería tener"[6].

Es en 1962 cuando Alfred D. Chandler, basándose en su conocimiento por la historia empresarial, especialmente la obtenida después de la segunda guerra mundial y enfrentando la evolución que presentaban las compañías establece que "Es el elemento que determina las metas básicas de la empresa, a largo plazo, así como la adopción de cursos de acción y asignación de recursos para alcanzar las metas", considerándose como la primera definición moderna "Estrategia y estructura"[7].

La expresión estrategia a nivel de tecnología se empieza a utilizar en 1983 cuando en los Estados Unidos identifican la necesidad de implementar una estrategia de tecnología con el fin de establecer competitividad en el país. Para ello, se formula el Proyecto Sócrates, "un programa de la Agencia de Inteligencia de Defensa de EE.UU"[8], fundada y dirigida por el físico Michael C. Sekora, la cual tenía una doble misión: "determinar la verdadera causa de la disminución de la capacidad de Estados Unidos para competir".

---

[4] HENRY MINTZBERG, James Brian y QUINN, John Voyer. El proceso estratégico, conceptos, contexto y casos [Libro en línea]. Prentice-Hall Hispanoamérica, S.A. Pag, 653., 1995. Colección de e-book. < https://books.google.com.co/books?id=YephqTRD71IC&pg=PA2&lpg=PA2&dq=von+neumann+y+morgenstern+la+estrategia+%E2%80%9CEs+una+serie+de+actos+que+ejecuta+una+empresa,+los+cuales+son+seleccionados+de+acuerdo+con+una+situaci%C3%B3n+concreta&source=bl&ots=FaJDQ4ZUln&sig=W1v6Sm6O3lPiBrvxJ4u2XYOC9R4&hl=en&sa=X&ei=gttHVaiWHcGNNrOkgbgO&ved=0CCoQ6AEwAg#v=onepage&q=von%20neumann%20y%20morgenstern%20la%20estrategia%20%E2%80%9CEs%20una%20serie%20de%20actos%20que%20ejecuta%20una%20empresa%2C%20los%20cuales%20son%20seleccionados%20de%20acuerdo%20con%20una%20situaci%C3%B3n%20concreta&f=false

[5] Ibid., p.7.

[6] Ibid., p.7.

[7] Ibid., p.7.

[8] SANDERS, Joshua. Spurring America's Economic Renaissance. 2013

2.1.1 Antecedentes implementación del Plan estratégico de TI a nivel mundial.

El plan estratégico de tecnologías de la información es aplicable en cualquier empresa sin importar su razón social u objetivos, ya que esta se encarga del manejo adecuado de las TI que son herramientas aplicables a diferentes objetivos y razones sociales. Esta afirmación se encuentra registrada en trabajos como: Maquera Atencio, René Nelson realiza un trabajo monográfico para la facultad de Ciencias Matemáticas EAP de Computación de la Universidad Nacional Mayor de San Marcos (Perú), titulado Planeamiento estratégico de la tecnología de la información aplicada al Instituto Superior Tecnológico Público de Chancay, propone la tendencia de las TI en las empresas "como las encargadas de automatizar el "desorden", centrándose en solo atacar los problemas a corto plazo o inmediato dando soluciones poco duraderas, costosas y sin un plan estratégico en pro del beneficio de la empresa"[9].

La Contraloría General de la República de Costa Rica en Julio de 2007 formula el Plan Estratégico de Tecnologías de Información y Comunicación 2007-20124[10], donde realiza una descripción del proceso seguido para elaborar este plan, un análisis de la situación actual de la CGR en materia tecnológica, una estrategia de alineamiento del PETIC con la estrategia institucional, los factores críticos de éxito que considera el desarrollo y ejecución de este plan así como la descripción de los principales riesgos del PETIC.

El 17 de mayo de 2011 por medio de la resolución ministerial N. 0191-2011-ED la oficina de informática de la Secretaría de planificación estratégica, propone para aprobación, el Plan Estratégico de Tecnologías de Información y Comunicaciones – PETI[11] del Ministerio de Educación de Perú, donde se exponen las definiciones estratégicas a nivel de TIC para el Ministerio (Rol, Misión y Visión TIC) y los factores claves de éxito para alcanzar la visión TIC.

2.1.2 Antecedentes implementación del Plan estratégico de TI a nivel nacional.

Por medio de revisiones documentales de fuentes digitales, se constató que a nivel nacional existen diferentes organizaciones donde se ha formulado e implementado el Plan Estratégico de TI, dentro de las que se pueden citar:

Orozco Murillo Nelson Eduin, Rodríguez Cruz César Orlando y Serrano Zambrano Walter, realizaron el trabajo de investigación de la Especialización de gerencia informática de la Universidad EAN en Bogotá, titulado Planeación Estratégica de TIC para la empresa diez y

[9] Disponible en Internet:http://sisbib.unmsm.edu.pe/bibvirtualdata/Tesis/Basic/maquera_ar/T_completo.PDF
[10] Disponible en Internet:
http://documentos.cgr.go.cr/content/dav/jaguar/documentos/cgr/estrategia/documentos/PETIC.pdf
[11] Disponible en Internet:http://www.minedu.gob.pe/normatividad/resoluciones/rm_0316-2011-ed.pdf

medios Ltda.[12], donde se afronta abarca el plan estratégico TIC para la empresa Diez y Medios Ltda., compañía pujante del sector de las TIC en Colombia, siguiendo la metodología PETI (Planeación estratégica de las Tecnologías de la Información), la cual es ampliamente reconocida y consiste en un proceso de planeación dinámico, que nos lleva a realizar en primer lugar una radiografía completa de la empresa para identificar oportunidades de mejora, luego a establecer los objetivos principales a lograr con una planeación estratégica y finalmente se hace el diseño de las estrategias a aplicar en el mediano y largo plazo en la compañía.

En el año 2011 fue presentado en la Facultad de Minas, Escuela de Sistemas de la Universidad Nacional de Colombia, Seccional Medellín el trabajo de investigación Metodología para la elaboración del mapa estratégico de tecnologías de información y comunicaciones para instituciones de educación superior en Colombia usando el Balanced Scorecard para TI realizado por Andrés Esteban Cardona Usuga como requisito para optar al título Magister en Ingeniería – Sistema, donde se aborda el problema de la planeación estratégica de TIC y su mapa estratégico al interior de las instituciones de educación superior en Colombia y se replantea la posición frente a las TIC por parte de estas organizaciones[13].

2.1.3 Antecedentes sobre la implementación del Plan estratégico de TI a nivel local.

Mediante diferentes tipos de revisiones digitales e impresas se observa que a nivel local son pocos los trabajos que se han realizado asociados a un Plan estratégico de TI.

Dentro de los cuales se puede citar:

En el año 2013, los Ingenieros de sistemas Jiménez Ovallos, Wilson Fabián y Gaona Cáceres, Jessica Lorena[14], realizan como trabajo de grado para obtener el título de Especialista en Auditoría de Sistemas en la Universidad Francisco de Paula Santander Seccional Ocaña, una Guía Metodológica para el diseño de un Plan Estratégico de TI en empresas de telecomunicaciones, a través de la cual se podrán identificar las necesidades de información organizacionales que permite el diseño de un plan estratégico de TI en empresas de telecomunicaciones, que contribuya dar soporte a los diferentes niveles de la organización.

En el año 2013, Los estudiantes Bohórquez Conde Lorena Astrid, Gallardo Quintero Jazmín, Arévalo Solano Linda Carolina y Bayona Ibáñez Eduard[15], realizan como trabajo

[12] Disponible en Internet: http://repository.ean.edu.co/bitstream/10882/1789/15/OrozcoNelson2012.pdf
[13] Disponible en Internet: http://www.bdigital.unal.edu.co/5475/
[14] JIMÉNEZ OVALLOS, Wilson Fabián y GAONA CÁCERES, Jessica Lorena. Guía Metodológica para el diseño de un Plan Estratégico de TI en empresas de telecomunicaciones, 2013.
[15] BOHÓRQUEZ CONDE, Lorena Astrid, et al. Plan estratégico para el proyecto Génesis SIA de la Universidad Francisco de Paula Santander Ocaña, 2013.

de grado para obtener el título de Especialista en Auditoría de Sistemas en la Universidad Francisco de Paula Santander Seccional Ocaña, un Plan estratégico para el proyecto Génesis SIA. La presente investigación propone la elaboración de un plan estratégico para el Proyecto de Interconectividad Génesis SIA desarrollado por el departamento de Sistemas e Informática de la Universidad Francisco de Paula Santander Ocaña.

En el año 2013, Los estudiantes Flórez Picón Ivette Carolina, Estévez Pacheco Yefferson y Velásquez Carrascal Jesús Emiro[16] realizan como trabajo de grado para obtener el título de Especialista en Auditoría de Sistemas en la Universidad Francisco de Paula Santander Seccional Ocaña, plan estratégico de tecnología de la información (PETI) aplicado a la cooperativa de transporte Cootranshacaritama Ltda. La presente investigación propone el desarrollo de un plan estratégico de TI basado en la metodología PETI, teniendo como resultado el diagnostico situacional de la organización producto del desarrollo de una auditoria informática, el modelado del negocio, la formulación de un modelo de TI siguiendo el ciclo PHVA y por último el modelo de planeación.

2.2 MARCO TEÓRICO

2.2.1 Plan estratégico de Tecnología de la Información. El estudio teórico del Plan Estratégico de Tecnologías de Información - PETI, se subdivide en dos marcos generales, la planeación estratégica la cual tiene un amplio recorrido histórico que los líderes y en general la sociedad, ha querido planear para lograr objetivos y para organizar recursos y personal, y en segunda posición por ser más joven las Tecnologías de la Información – TI, las cuales están moviendo en su totalidad todos los procesos de una empresa.

La planeación estratégica establece procedimientos de planificación de recursos, personal, actividades y proyectos para alcanzar objetivos organizacionales a un plazo previamente fijado, teniendo una visión futura y anticipándose a los cambios del mercado y del entorno. Obedeciendo los principios de planificación: cuantificable, factible, objetiva, unidad, flexible y del cambio de estrategia.

La necesidad de una respuesta inmediata y globalizada en los procesos de cualquier organización, obligó al hombre a desarrollar herramientas capaces de suplirlas, es así como se introduce al campo de juego las TI o Tecnologías de la Información. Para Castells, "El informalismo es la sociedad construida alrededor de las tecnologías de la información basadas en la microelectrónica y que opera mediante software, siendo relevante el nuevo paradigma tecnológico que constituye la base material de la nueva sociedad del siglo XXI, entendiendo por paradigma el modelo conceptual que estable los principios de actuación.

[16] FLÓREZ PICÓN, Ivette Carolina, et al. Plan estratégico de tecnología de la información (PETI) aplicado a la Cooperativa de transporte Cootranshacaritama Ltda, 2013.

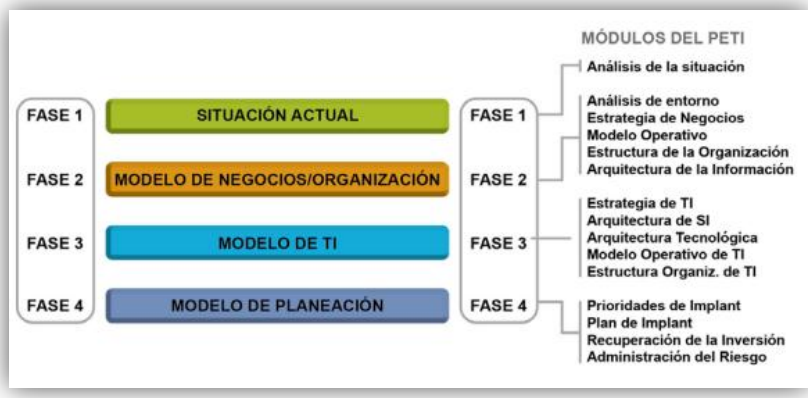
Nos encontramos por tanto ante un nuevo modelo conceptual y no solo la aplicación de las nuevas fuentes de información o conocimiento al anterior paradigma de la era industrial"[17].

Existe una herramienta ampliamente reconocida para ordenar los esfuerzos de incorporación de TI, la cual es la Planeación estratégica de tecnologías de la información PETI, dicha herramienta establece las políticas requeridas para controlar la adquisición, el uso y la administración de los recursos de TI en las organizaciones. Una Planeación de TI se estructurada a través del siguiente proceso:

- Entendimiento de la situación actual de la unidad responsable de TI (análisis, diagnóstico y documentación de la estructura organizacional y funcional de TI).
- Entendimiento de la situación actual de los dominios tecnológicos y exploración de tendencias tecnológicas.
- Definición de la estrategia de la unidad responsable de TI (estrategias de TI).
- Diseño de arquitecturas por dominio.
- Conformación de la cartera de proyectos de TI.

2.2.2 Metodología PETI. La metodología PETI se compone de 4 fases y 15 módulos agrupados por fases como se puede ver en la figura 1. Este paradigma está concebido, en concordancia con el modelo conceptual a través de una visión estratégica de negocios y organización y una visión estratégica de TI. La metodología integra ambas visiones en una única finalidad.

Figura 1. Metodología de Planeación Estratégica de Tecnología de Información.



Fuente. NAJARRO BELLIDO, Julio Ernesto y FIGUEROA ORBEGOSO, Carlos Ernesto. Planeamiento Estratégico de Tecnología de Información de la Escuela Superior Privada de Tecnología – SENATI.

[17] CASTELLS, Manuel. La Sociedad Red: Una visión global. 2006. ISBN 84-206-4784-5 Alianza Editorial.

1. Fase I: Situación actual.

Para esta fase, se formula el siguiente interrogante: ¿Dónde estamos hoy?. Comienza con un análisis de la situación actual de la organización, para tener como resultado la generación del modelo funcional de la empresa. Para ello, se evalúa de manera general la estrategia de negocios utilizada, la eficiencia de los procesos operativos y la aceptación de TI en la organización. En esta fase se responden los siguientes cuestionamientos:

- ¿Qué tan bien responde nuestra capacidad de TI a las necesidades de la organización?
- ¿Cómo se compara nuestra capacidad de TI con la de nuestros competidores?
- ¿Cuáles son las tendencias en TI y cuáles debemos adoptar?

2. Fase II: Modelo del Negocio/Organización.

Se formula la pregunta ¿A dónde queremos llegar? Está relacionada con la creación de un modelo de la organización, inicia con un análisis del entorno y el establecimiento de la estrategia de negocios. Continua con el diseño en detalle de los modelos operativos, que van a producir en parte los requerimiento de TI necesarios para mejorar la eficiencia y productividad de la empresa. Posteriormente se construye la estructura de la organización, que especifica puestos, perfiles, habilidades, entre otros necesarios para administrar la empresa. La fase termina con la construcción de una arquitectura de información, que identifica las necesidades globales de información de la empresa. El modelo es descrito con la utilización de términos y conceptos de negocio/organización, independientemente del soporte computacional y jerga informática.

En este modelo se concibe dar respuesta a los siguientes interrogantes:

- ¿Hacia dónde se dirige nuestro negocio?
- ¿Cuáles son nuestras oportunidades para tomar ventaja de la tecnología?
- ¿Cuál debería ser nuestra estrategia general de TI?
- ¿Qué arquitecturas se requieren? ¿Qué estructura administrativa necesitamos entre TI y el resto del negocio?

3. Fase III: Modelo de TI.

Cabe la pregunta ¿Cómo llegamos allí? Es el cuestionamiento que se formula en esta fase. Para dar respuesta a ello, es necesario solucionar los siguientes interrogantes:

- ¿Cuál es la brecha entre dónde estamos y a donde queremos llegar?
- ¿Cuáles son las iniciativas y proyectos requeridos para cerrar la brecha?
- ¿Qué cambios debemos introducir en nuestra capacidad de TI y en la organización para cerrar la brecha?

Se trata del desarrollo de un modelo de TI. En su primer módulo, tiene como objetivo la transformación de las estrategias de negocios en una estrategia de TI. Sigue con la construcción de la arquitectura de sistemas, que establece un marco para la especificación de las aplicaciones y la integración de la información. Luego se definen los elementos claves y las características esenciales de la arquitectura tecnológica (hardware y comunicaciones), que establece la plataforma en la que los sistemas van a funcionar. Continúa con el diseño en detalle de los modelos operativos de TI, que describen el funcionamiento del área informática. Finaliza con la definición sobre la estructura de la organización de TI, necesaria para administrar los requerimientos informáticos.

4. Fase IV: Modelo de planeación.

En este modelo se centra en la elaboración de un modelo de planeación. Primero se establecen las prioridades par a la implantación de TI y los procesos operativos. Luego se define un plan de implantación, que determina el orden de desarrollo de los proyectos de negocios/organización y de TI. Continúa con un estudio de la recuperación de la inversión, a través de un análisis costo/beneficio. Todo el proceso finaliza con un estudio de administración del riesgo, que se encarga de reconocer la existencia de amenazas que puedan poner en peligro el éxito del PETI.[18]

2.3 MARCO CONCEPTUAL

2.3.1 Planeación. "Implica una visión del futuro, ya que de una situación actual se espera llegar a un resultado final, para lo cual existen varios caminos y, por lo tanto, hay que elegir las opciones y los medios idóneos que nos permita alcanzar el objetivo esperado"[19].

"Es un término que define un conjunto de acciones orientadas al logro de un resultado claramente definido, siempre y cuando se posea un alto nivel de certidumbre sobre la situación en que éstas van a llevarse a cabo, y un elevado control de los factores permitirán que se alcance el resultado perseguido."[20]

La planeación incrementa significativamente la posibilidad de que gran parte de las actividades y recursos de la organización sean transformadas en utilidades para el negocio, disminuyendo también con ella el nivel de vulnerabilidad. La no planeación conduce al desorden y al desperdicio organizacional. Se planea para: Preparar estrategias, prevenir amenazas, obtener resultados finales, actuar con mayor efectividad, ser líderes en el mercado, minimizar la incertidumbre y saber qué hacer.

---

[18] Disponible en Internet: < http://sisbib.unmsm.edu.pe/bibvirtualdata/Tesis/Basic/najarro_bj/cap03.pdf>
[19] RODRÍGUEZ VALENCIA, J. Cómo aplicar la planeación estratégica a las pequeñas y medianas empresas.
[20] MATILLA, Katia. Los modelos de planeación estratégica en la teoría de las relaciones públicas. 1 ed.: Editorial UOC, 2008. 269 p.

2.3.2 Estrategia. Debe considerarse en un concepto multidimensional que abarca a toda la Organización, otorgándole un sentido de sistema abierto perfectamente delimitada con su entorno, con el que interacciona, en el que diferentes tipos de procesos, operaciones, información y decisiones son reconocibles y orientados. Desde el punto de vista sistémico la estrategia es un marco de referencia para la organización, pues facilita su adaptación a un entorno cambiante y permite sustentar su continuidad. Definir una estrategia(s) implica: Un plan de acción, conocimiento de lo que se va a hacer y adaptación al medio.[21]

2.3.3 Planeación estratégica. Ramanantsoa lo define como "El proceso organizativo que intenta mostrar con antelación los cambios estructurales estratégicos, que permite el acoplamiento entre las distintas áreas de la compañía y también intenta adaptar al personal según su especialización par el mejor cumplimiento de los objetivos".[22]

Como resultado de realizar un análisis de la información relevante, pasada y presente, con previsión del futuro, desde el pensamiento estratégico, permite definir un curso de acción que guie a la organización a su visión de éxito por los logros alcanzados y definidos en la planeación. Parte de su éxito está centrado en la visión sistémica y en el ciclo auto-controlado que se le imprima para que el plan no pierda vigencia. Esta posibilidad se detalla mejor en el planteamiento metodológico.

2.3.4 Plan Estratégico de Tecnologías de la Información – PETI. La Planeación Estratégica de Tecnologías de Información es ampliamente reconocida como una herramienta para ordenar los esfuerzos de incorporación de TI. Dicha herramienta establece las políticas requeridas para controlar la adquisición, el uso y la administración de los recursos de TI. Integra la perspectiva de negocios y organizacional con el enfoque de TI.23

2.3.5 COBIT. Es una herramienta desarrollada por Information System Audit and Control Association ISACA) y por IT Governance Institute (ITGI), cuyo propósito fundamental es ayudar al entendimiento y a la administración de riesgos asociados con TI. El principio del cual parte, es que las empresas exitosas no solo aprovechan los beneficios de una gestión exitosa, sino también gestionan el riesgo y COBIT coadyuva a la identificación y adopción de mejores prácticas de control y auditoría en la gestión de TI, a partir de tres requerimientos del negocio como la calidad, los fiduciarios y los de seguridad.

2.3.6 Norma ISO/IEC 27001:2013. La norma/estándar UNE ISO/IEC 27001: 2013 del "Sistema de Gestión de la Seguridad de la Información" es la solución de mejora continua

---

[21] CORREA OSPINA, J. I. y LÓPEZ TRUJILLO, M. Planeación estratégica de tecnologías informáticas y sistemas de información. Manizales: Universidad de Caldas, 2007.

[22] RAMANANTSOA, T. Planificación estratégica en empresas diversificadas. En: ABASCAL ROJAS, Francisco. Como se hace un plan estratégico: la teoría del marketing estratégico. 4ed. España: ESIC Editorial, 2004.

[23] BAILEY, Cristian. PETI Planeación Estratégica de Tecnologías de Información, Metodología. [En línea]. Disponible en: http://es.scribd.com/doc/27526056/Peti-planeacion-Estrategica-Ti-Itcp.

más adecuada para evaluar los riesgos físicos (incendios, inundaciones, sabotajes, vandalismos, accesos indebidos e indeseados) y lógicos (virus informáticos, ataques de intrusión o denegación de servicios) y establecer las estrategias y controles adecuados que aseguren una permanente protección y salvaguarda de la información.

El Sistema de Gestión de la Seguridad de la Información (SGSI) se fundamenta en la norma UNE-ISO/IEC 27001:20132, que sigue un enfoque basado en procesos que utilizan el ciclo de mejora continua o de Deming, que consiste en Panificar- Hacer-Verificar-Actuar, más conocido con el acrónimo en inglés PDCA (Plan-Do-Check-Act) (similar a la más extendida y reconocida norma ISO 9001).

2.4 MARCO LEGAL

DOCUMENTO CONPES 3072 AGENDA DE CONECTIVIDAD 9 DE FEBRERO DE 2000. A través del cual se presenta a consideración del CONPES la "Agenda de Conectividad", que busca masificar el uso de las Tecnologías de la Información y con ello aumentar la competitividad del sector productivo, modernizar las instituciones públicas y de gobierno, y socializar el acceso a la información, siguiendo los lineamientos establecidos en el Plan Nacional de Desarrollo 1998 – 2002 "Cambio para Construir la Paz".

PLAN NACIONAL DE TIC 2008- 2019. Busca que, al final de este período, todos los colombianos se informen y se comuniquen haciendo uso eficiente y productivo de las Tecnologías de Información y Comunicación TIC, para mejorar la inclusión social y aumentar la competitividad. Para lograr este objetivo se proponen una serie de políticas, acciones y proyectos en ocho ejes principales, cuatro transversales y cuatro verticales. Los ejes transversales cubren aspectos y programas que tienen impacto sobre los distintos sectores y grupos de la sociedad. Los ejes verticales se refieren a programas que harán que se logre una mejor apropiación y uso de las TIC en sectores considerados prioritarios para este Plan.

Los ejes transversales son:

- Comunidad.
- Marco regulatorio.
- Investigación, Desarrollo e Innovación.
- Gobierno en Línea.

Los cuatro ejes verticales son:

- Educación.
- Salud.
- Justicia.
- Competitividad Empresarial.

LEY 72 DEL 20 DE DICIEMBRE DE 1989. El Gobierno Nacional, por medio del Ministerio de Comunicaciones, adoptará la política general del sector de comunicaciones y ejercerá las funciones de planeación, regulación y control de todos los servicios de dicho sector, que comprende, entre otros:

- Los servicios de telecomunicaciones.
- Los servicios informáticos y de telemática.
- Los servicios especializados de telecomunicaciones o servicios de valor agregado.
- Los servicios postales.

LEY 555 DEL 2 DE FEBRERO DE 2000 EN LA LEY NO. 1341 DEL 30 DE JULIO DE 2009. "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.", muestra el esfuerzo que ha tenido el gobierno colombiano por brindar un marco normativo para el desarrollo de tecnologías de la información y la comunicación.

Artículo 2o. Principios orientadores. Las Tecnologías de la Información y las Comunicaciones deben servir al interés general y es deber del Estado promover su acceso eficiente y en igualdad de oportunidades, a todos los habitantes del territorio nacional.

Son principios orientadores de la presente ley:

Prioridad al acceso y uso de las Tecnologías de la Información y las Comunicaciones. El Estado y en general todos los agentes del sector de las Tecnologías de la Información y las Comunicaciones deberán colaborar, dentro del marco de sus obligaciones, para priorizar el acceso y uso a las Tecnologías de la Información y las Comunicaciones en la producción de bienes y servicios, en condiciones no discriminatorias en la conectividad, la educación, los contenidos y la competitividad.

Artículo 3o. Sociedad de la Información y del Conocimiento.

El Estado reconoce que el acceso y uso de las Tecnologías de la Información y las Comunicaciones, el despliegue y uso eficiente de la infraestructura, el desarrollo de contenidos y aplicaciones, la protección a los usuarios, la formación de talento humano en estas tecnologías y su carácter transversal, son pilares para la consolidación de las sociedades de la información y del conocimiento.

3. DISEÑO METODOLÓGICO

3.1 TIPO DE INVESTIGACIÓN

Dado el propósito del presente proyecto, de diseñar un Plan Estratégico de Tecnologías de Información para la Universidad Francisco de Paula Santander Ocaña, se llevó a cabo una investigación cualitativa, ya que de acuerdo con una de sus definiciones, "es aquella donde se estudia la calidad de las actividades, relaciones, asuntos, medios, materiales o instrumentos en una determinada situación o problema. La misma procura por lograr una descripción holística, esto es, que intenta analizar exhaustivamente, con sumo detalle, un asunto o actividad en particular"[24].

Partiendo de esta definición, la investigación cualitativa, permitió comprender y explorar los elementos que intervienen en el diseño del plan estratégico en mención, logrando determinar que ésta pudo ser la mejor opción para optimizar los procesos de la Universidad a través del uso eficiente de las tecnologías de información y comunicación.

3.2 POBLACIÓN Y MUESTRA

Para el presente proyecto, se tomó como población a los responsables de los siguientes procesos, delegando autoridad a los jefes de algunas unidades, relacionadas con la gestión de la seguridad de la información en la Universidad:

RESPONSABLE	PROCESO
Jefe División de Sistemas	*Sistema de Inform. Telecomunicaciones y Tecnología*
Jefe de Personal	*Gestión Humana*
Jefe de Almacén	*Gestión Administrativa y Financiera*
Jefe de Calidad	*Control Interno*

La muestra estuvo representada por el 100% de la población.

3.3 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

En el diseño del Plan Estratégico de Tecnologías de Información para la Universidad Francisco de Paula Santander Ocaña, en primera instancia se utilizó, como técnica de recolección de información la entrevista y como instrumento un cuestionario para la misma, que fue aplicado a los responsables de las dependencias relacionadas anteriormente, con el fin de realizar un diagnóstico de la manera como se han gestionado las tecnologías de información TI a cada uno de los procesos administrativos y académicos de la Universidad

[24] VERA VÉLEZ, Lamberto. La investigación cualitativa. Disponible en Internet en: <http://www.ponce.inter.edu/cai/Comite-investigacion/investigacion-cualitativa.html>

(Ver Anexos A, B, C, y D). Y en segunda instancia, los instrumentos propios de la auditoría (papeles de trabajo.)

4. RESULTADOS

4.1 ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA EN LOS PROCESOS DE ADOPCIÓN DE TECNOLOGÍAS DE INFORMACIÓN

Con el fin de realizar un análisis de la situación actual del proceso de adopción de tecnologías de la información en la Universidad y de la manera como se vienen gestionando, se llevó a cabo una auditoría de cumplimiento bajo el estándar ISO 27002:2013, incluyendo sus catorce (14) dominios, e involucrando los siguientes procesos:

Sistema de Información. Telecomunicaciones y Tecnología, Gestión Humana, Gestión Administrativa y Financiera y Control Interno.

El informe de la auditoría realizada se presenta a continuación:

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

Auditoría de Cumplimiento 2015

ISO/IEC 27002:2013

ÍNDICE

1. ASPECTOS GENERALES DEL ÁREA AUDITADA

1.1 DESCRIPCIÓN DEL ÁREA

La División de Sistemas de la Universidad Francisco de Paula Santander Ocaña, es una dependencia administrativa, encargada de la logística tecnológica de los procesos Académicos y Administrativos, suministrando soporte técnico, asistencia y asesoría en la adquisición y mantenimiento del software y hardware de la Universidad y entes externos, proponiendo y fijando pautas competitivas para el desarrollo e implementación de software, con el fin de fortalecer los sistemas tecnológicos institucionales.

Dentro de su estructura se encuentran las siguientes funciones:

- Analizar las necesidades relacionas con las tecnologías de la información en las áreas institucionales (docencia, investigación y servicios administrativos). Contribuyendo con los objetivos, procesos y procedimientos de la Universidad.

- Elaborar planes estratégicos que contemplen las necesidades básicas, para alcanzar objetivos comunes, en beneficio de la Institución.

- Asignar objetivos a las distintas divisiones, seguir el desarrollo de proyecto y actividades, controlar los resultados en materia informática y de telecomunicaciones.

- Gestionar y mantener aplicaciones orientadas a proporcionar información a la comunidad universitaria.

- Llevar a cabo la función gerencial para el desarrollo de los sistemas de información y telecomunicaciones en la Universidad.

- Adecuar los procedimientos en el uso de los sistemas informáticos y las normas de seguridad vigentes e implantar los medios y las medidas necesarias para ello.

- Asesorar, estudiar e implementar soluciones de equipamiento e infraestructura para la red de voz y la red de datos de la Universidad.

- Responder consultas técnicas, de seguridad y documentar la configuración del sistema.

- Prestar asesoramiento a la comunidad universitaria en la adquisición de equipos y programas informáticos de uso común.

- Velar porque las operaciones efectuadas se apliquen correctamente en los sistemas diseñados para cumplir con las necesidades de la Institución.

- Ofrecer soporte a la institución en la adquisición y uso de tecnologías de informática y de telecomunicaciones como apoyo a la administración, la docencia y la investigación.

- Analizar, evaluar, planear y ejecutar los proyectos que favorecen el desarrollo de la informática y las telecomunicaciones en la universidad de acuerdo con las políticas institucionales establecidas.

- Crear y mantener un sistema de información institucional integral y consistente de apoyo a la toma de decisiones de la dirección Universitaria.

- Asesorar en la utilización de sistemas de información a los diferentes procesos de la Institución.

- Brindar soporte y contratar el mantenimiento de la infraestructura de redes y servidores, equipo de cómputo, servicios de Internet, sistemas de información y sistemas de comunicaciones.

- Fomentar y velar por el buen funcionamiento de los recursos de servicios de información.

- Velar por el cumplimiento de estándares, normas y leyes de uso de servidores de información.

- Efectuar ajustes sobre los sistemas que están operando de acuerdo a las nuevas necesidades.

- Asesorar a la Universidad sobre aspectos de informática cuando así lo requiere.

- Responder ante el director por el cumplimiento de las actividades del personal de la división de sistemas de la Universidad.

- Responder por el inventario de todos los equipos existentes en la división de sistemas.

La División de Sistemas cuenta con las siguientes áreas específicas para el cumplimiento de sus actividades:

Área de soporte y mantenimiento

- Mantenimiento preventivo y correctivo de equipos.
- Activación de puntos de red y/o teléfono.
- Administración de cuentas de correo.
- Controles de seguridad.
- Capacitación al usuario.
- Atención al Usuario.

Área de Sistemas de Información y Desarrollo

- Análisis y Desarrollo de aplicaciones de software que para solucionar necesidades detectadas.
- Mantenimientos y Actualización en los sistemas de información existentes.
- Apoyar las funciones Académico - administrativas desarrollando soluciones integradas de Sistemas de información, que agilicen los procesos de toma de decisiones institucionales, facilitando los procesos internos y externos que aseguren la confiabilidad de la información en la Universidad.

Área de Redes y Telecomunicaciones

- Proveer la infraestructura tecnológica para el funcionamiento de Internet, redes alámbricas e inalámbricas.
- Administración de servidores.
- Administración de la infraestructura de red.
- Backup's, protección y recuperación de la información.
- Administración de salas de cómputo.
- Administración de la base de datos.
- Administración de cámaras de vigilancia y monitoreo.

2. ASPECTOS DE LA AUDITORIA

2.1 OBJETIVOS

2.1.1 Objetivo General

Realizar una auditoría de cumplimiento bajo el estándar ISO 27002:2013

2.1.2 Objetivos Específicos

- Evaluar el cumplimiento de las actividades relacionadas con la seguridad de la información.

- Verificar la eficiencia de los controles implementados para preservar la seguridad de la información.

2.2 ALCANCES

Teniendo en cuenta la importancia de la seguridad de la información, se hizo necesario evaluar la existencia y eficiencia de los controles implementados para gestionar adecuadamente la seguridad de la información en la Universidad Francisco de Paula Santander Ocaña. La auditoría realizada incluyó la evaluación de dichos controles, involucrando los siguientes procesos: ***Sistema de Información, Telecomunicaciones y Tecnología, Gestión Humana, Gestión Administrativa y Financiera y Control Interno.***

2.3 RECURSOS NECESARIOS

Para la ejecución de la auditoría realizada a la División de Sistemas, se hizo necesaria la utilización de los siguientes recursos:

2.3.1 Recursos de Hardware. Se utilizaron elementos como: equipo de cómputo, impresora, medios de almacenamiento.

2.3.2 Recursos de Software. Se hizo necesario un editor de texto como Microsoft Word 2010.

2.3.3 Recurso Humano. El equipo auditor estuvo conformado de la siguiente manera:

MAGRETH ROSSIO SANGUINO REYES - Auditora Líder
MARÍA ALEJANDRA ARRIETA SANCHEZ- Auditora Junior 1
CINDY LORENA LOBO SANCHEZ - Auditora Junior 2

2.4 CRITERIOS DE AUDITORÍA

La auditoría realizada se llevó a cabo bajo el estándar ISO/IEC 27002:2013, teniendo en cuenta sus 14 dominios, 35 objetivos de control y 114 controles.

3. METODOLOGÍA

Para llevar a cabo la auditoría de cumplimiento bajo el estándar ISO/IEC 27002:2013 a las áreas que tienen que ver con los procesos de gestión de seguridad de la información en la Universidad Francisco de Paula Santander Ocaña, se organizaron las siguientes actividades:

3.1 PLAN DE AUDITORÍA

Contiene el conjunto de actividades que como equipo auditor, se establecieron para llevar a cabo los acuerdos para la organización del trabajo, así como el lugar y fecha de encuentro con los auditados.

R/PT PLA01

Empresa: **Universidad Francisco de Paula Santander Ocaña**
Área o Proceso**: División de Sistemas**

Fecha Inicio: 09/02/2015
Fecha Final: 17/02/2015

Objetivo General
Realizar una auditoría de cumplimiento bajo el estándar ISO 27002:2013

No.	ACTIVIDAD	FECHA	LUGAR	RESPONSABLE
1	Definición del objeto y los alcances de la auditoría.	30/01/2015	DIVISIS UFPSO	EQUIPO AUDITOR
2	Reunión del equipo de trabajo para definir responsabilidades y tareas	30/01/2015	UFPSO	
3	Solicitud de documentación de los procesos relacionados con la gestión de la seguridad de la información de la Universidad	04/02/2015	DIVISIS UFPSO	
4	Reunión del equipo de trabajo para el análisis de la documentación	06/02/2015	UFPSO	
5	Diseño de instrumentos de recolección de información	07/02/2015	UFPSO	
6	Aplicación de instrumentos para la realización de la auditoría de cumplimiento bajo el estándar ISO 27002:2013	09/02/2015	UFPSO	
7	Realización de entrevistas adicionales	11/02/2015	UFPSO	
8	Análisis de la información recolectada	18/02/2015	UFPSO	
9	Recolección de información adicional	03/03/2015	DIVISIS UFPSO	
11	Reunión Pre - Informe	11/03/2015	DIVISIS UFPSO	
12	Elaboración Informe de Auditoría	16/03/2015	UFPSO	

3.2 PROGRAMA DE AUDITORÍA

Comprende las actividades propias de la auditoría para evaluar el grado de cumplimiento de los controles del estándar ISO/IEC 27002:2013, relacionados con la gestión de la seguridad de la información en la Universidad. En la presente tabla se relaciona el objetivo general y dos objetivos específicos que van a permitir su cumplimiento. Asociada a cada objetivo, se establece una actividad con sus correspondientes instrumentos de recolección de información que van a permitir materializar su realización (columna RPT).

			R/PT PRA01
Empresa: **Universidad Francisco de Paula Santander Ocaña** Proceso**: Gestión de la Seguridad de los Sistemas de Información**			Fecha Inicio: 09/02/2015 Fecha Final: 17/02/2015
Auditora Líder**: Magreth Rossio Sanguino Reyes -** M.R.S.R. Auditora Junior 1: **María Alejandra Arrieta Sánchez -** M.A.A.S. Auditora Junior 2: **Cindy Lorena Lobo Sánchez -** C.L.L.S**.**			
Objetivo General Realizar una auditoría de cumplimiento bajo el estándar ISO 27002:2013			
Objetivos Específicos 1. Evaluar el cumplimiento de las actividades relacionadas con la seguridad de la información. 2. Verificar la eficiencia de los controles implementados para preservar la seguridad de la información.			
Alcances La auditoría se llevará a cabo a la Seguridad Física y Ambiental en la División de Sistemas de la Universidad Francisco de Paula Santander, involucrando las áreas de la División de Sistemas, Oficina de Calidad, Almacén y Personal. Esta evaluación estará comprendida desde el 09 al 17 de febrero de 2015			
ÍTEM	**ACTIVIDAD**	**RPT**	**AUDITADO**
1.1	Medir el grado de cumplimiento de los controles presentes en el estándar ISO/IEC 27002:2013, dentro del Sistema de Gestión de la Seguridad de la Información, mediante la realización de entrevistas.	ENT01 ENT02 ENT03 ENT04	J.D.S. J.D.P. J.U.A J.C.
2.2	Verificar la eficiencia en la implementación de los controles de la norma antes citada, mediante pruebas de cumplimiento.	PRC01 PRC02 PRC03-1 PRC03-2 PRC04	
MARCAS O TILDES UTILIZADAS **PLA01:** Programa de Auditoría **J.D.S.:** Jefe de la División de Sistemas **J.D.P.:** Jefe División de Personal **J.O.C.:** Jefe de Calidad **J.U.A.:** Jefe Unidad de Almacén			

4. HALLAZGOS DE LA AUDITORÍA

Para presentar los hallazgos, se tuvo en cuenta los 14 dominios del estándar ISO/IEC 27002:2013

Los dominios que se evaluaron se relacionan a continuación:

- Políticas de Seguridad
- Aspectos organizativos de la seguridad de la información
- Seguridad ligada a los recursos humanos
- Gestión de activos
- Control de accesos
- Cifrado
- Seguridad física y ambiental
- Seguridad en la operativa
- Seguridad en las telecomunicaciones
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Relaciones con suministradores
- Gestión de incidentes en la seguridad de la información
- Aspectos de seguridad de la información en la gestión de la continuidad del negocio
- Cumplimiento

A continuación se presentan los hallazgos y las recomendaciones respectivas por cada dominio:

DOMINIO 5: POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

HALLAZGOS:

Existe un documento de Políticas de Seguridad de la Información (versión No. 2), aprobado por el Comité de Apoyo Académico bajo Acta No. 0011 de 21 de Abril de 2015, que contiene los lineamientos para la protección y uso correcto de los activos de información.

La revisión de la Política de Seguridad está a cargo del responsable del proceso Sistemas de Información, Telecomunicaciones y Tecnología **SITT**, que se encarga de evaluar cada dos años este documento y realizar las modificaciones necesarias. Actualmente, dicha política no es del conocimiento de todos los miembros de la comunidad universitaria, puesto que no se ha publicado oficialmente, ni a través de la plataforma Web, ni por medios impresos. Cabe destacar que aunque no se han realizado capacitaciones formales, algunos aspectos de seguridad que se consideran relevantes, se vienen divulgando a través del correo institucional.

RECOMENDACIONES:

La revisión de las políticas de seguridad de la información debería tener en cuenta los resultados de las revisiones por parte de la dirección de la Universidad. Así mismo, establecer criterios y procedimientos formales para la revisión que pudieran sugerir modificaciones al documento,

como cambios en el entorno institucional, nuevas tendencias tecnológicas, reportes de amenazas y/o vulnerabilidades, recomendaciones de autoridades relevantes, entre otros.

De igual forma, se sugiere socializar y/o comunicar a los diferentes estamentos de la Universidad, los lineamientos contemplados en el documento de Políticas de Seguridad de la Información, para que se adopte una cultura de la protección de la información y de los demás activos de información de la institución.

DOMINIO 6: ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

HALLAZGOS:

Actualmente la Universidad Francisco de Paula Santander Ocaña, no cuenta con un marco regulatorio para iniciar y controlar los procesos de implementación de la seguridad de la información dentro de la Institución. Existen procedimientos establecidos, aprobados, controlados e implementados en cada uno de los procesos estratégicos, misionales y de apoyo de la Universidad (https://ufpso.edu.co/sig/), que permiten soportar algunas de las actividades relacionadas con la gestión de la seguridad de la información; sin embargo, no son suficientes para alcanzar el objetivo.

No existen responsabilidades claramente definidas para la protección de los activos individuales, ni se conocen procesos de seguridad específicos para cada uno de ellos. La responsabilidad de los activos, recae sobre el jefe del área.

De la misma manera, la Universidad, no cuenta con procedimientos formales para establecer contacto con autoridades relevantes para los casos en los que se presente un incidente de seguridad que pueda poner en riesgo la continuidad de las operaciones. Por su parte, la División de Sistemas se encuentra inscrita a un servicio de bases de datos de vulnerabilidades, a través de las cuales se reciben alertas de seguridad para evitar o corregir fallas en los sistemas de información o aplicaciones. Así mismo, se recibe asesoría de una empresa de seguridad contratada para tal fin y para realizar auditorías de penetración, que se llevan a cabo anualmente.

RECOMENDACIONES:

Definir un marco regulatorio que garantice el cumplimiento de los controles de seguridad contemplados en la política de seguridad de la información. Igualmente, se deben definir claramente las responsabilidades para la protección de los activos individuales y llevar a cabo los procesos de seguridad específicos, definiendo y documentando claramente los niveles de autorización.

DOMINIO 7: SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

HALLAZGOS:

En la etapa de reclutamiento de personal, una vez se hace todo el proceso de convocar a nuevos empleos, se hace la recepción de las hojas de vida de los aspirantes y se realiza el estudio y revisión de los perfiles y competencias laborales solicitadas, así como el estudio de antecedentes.

Con respecto a la etapa de contratación del personal, se realizan los diligenciamientos de ley y el empleado firma el contrato. Cabe destacar que aunque el contrato no estipula una cláusula de confidencialidad específica, existe un ítem que se refiere a la reserva total de la información a la cual tendrá acceso. De igual forma, la Universidad, en cumplimiento de la Ley 734 de Febrero 05 de 2002 por la cual se expide el código disciplinario único, realiza las debidas sanciones o llamados de atención a los empleados que cometan alguna falta contra la institución o contra la información que se le ha asignado respectivamente. Estos procedimientos se llevan a cabo a través de la oficina de la División de Personal y la Dirección de la Institución.

Por su parte, los empleados no reciben capacitación específica en cuanto a procedimientos de seguridad de la información que tienen bajo su responsabilidad. Solo reciben a su correo institucional, tips de seguridad enviados por el Administrador Web.

El contrato de trabajo tampoco contempla reglas claras para el uso aceptable de algunos activos como correo electrónico, dispositivos, datos, equipos, entre otros.

En el momento de terminación del contrato, existe un formato denominado FORMATO ENTREGA DEL PUESTO DE TRABAJO, que contiene las actividades necesarias para hacer entrega oficial de su puesto de trabajo y la conformidad de las distintas dependencias de la Universidad con las cuales se establece relación directa.

RECOMENDACIONES:

Establecer un acuerdo de confidencialidad para cada uno de los empleados de la Universidad en el momento de su contratación o cuando haya algún cambio de puesto de trabajo, que contemple los requerimientos para proteger la información, utilizando términos legalmente ejecutables y especificando entre otros aspectos, el tipo de información que debe protegerse, la duración esperada del acuerdo, las responsabilidades para usar información confidencial, así como para evitar su divulgación, condiciones específicas de terminación del contrato laboral y las sanciones impuestas para los casos de incumplimiento de dicho acuerdo.

DOMINIO 8: GESTIÓN DE ACTIVOS

HALLAZGOS:

La Universidad cuenta con un inventario de todos sus activos, debidamente clasificados y mantenidos. Todos los activos se encuentran etiquetados de tal manera que sean de fácil acceso. Los responsables de dichos activos son los jefes de área, que a su vez pueden delegar en otros empleados dichas responsabilidades. Cabe resaltar que aunque estas funciones son delegadas, no existen documentos formales que establezcan dicha responsabilidad.

Existen formatos para entrega de activos, así como reportes de baja de elementos. En relación con las licencias de software como activo de información, están bajo la responsabilidad y custodia del jefe de la División de Sistemas.

En cuanto al proceso de baja de equipos, el responsable del manejo de los inventarios, solicita al jefe de la División de Sistemas, un dictamen sobre el estado del equipo para proceder a retirarlo de la dependencia que haya solicitado tal procedimiento.

Con respecto a los equipos de cómputo, una vez son retirados, se almacenan en bodega, sin aplicar ningún procedimiento específico de destrucción de la información contenida en ellos.

Finalmente, cabe destacar, que aunque el documento de Políticas de Seguridad de la Información (versión No. 2), contempla las reglas para el uso aceptable de algunos activos como correo electrónico, dispositivos, datos, equipos, entre otros, éstas no se han dado a conocer a la comunidad universitaria.

RECOMENDACIONES:

Acordar y documentar la propiedad para cada uno de los activos de información. De igual manera, establecer una clasificación específica para la División de Sistemas, que indique los niveles de protección de acuerdo con la importancia de los mismos y el valor comercial que representan para la Universidad.

Documentar e implementar reglas para el uso aceptable y seguro de los activos de información.

DOMINIO 9: CONTROL DE ACCESOS

HALLAZGOS:

El documento de Políticas de Seguridad de la Información, contempla las reglas de control de acceso y los derechos para cada usuario o grupos de usuarios de los sistemas de información. Así mismo, establece la responsabilidad de los usuarios en el tratamiento de la información, actualización de hardware y software, uso del correo electrónico, almacenamiento y respaldo de los datos, uso adecuado de la red interna, entre otros.

Además de lo anterior, dentro del proceso de Sistemas de Información, Telecomunicaciones y Tecnología **SITT** del Sistema Integrado de Gestión, existen procedimientos documentados, aprobados, controlados e implementados, que detallan la manera como se deben llevar a cabo las actividades propias del procedimiento. Para el caso particular, existe uno, denominado ADMINISTRACIÓN DE RECURSOS INFORMÁTICOS, cuyo objeto es el de "definir las actividades que se realizan para garantizar el uso eficiente de los recursos tecnológicos disponibles en la UFPSO, a través de actividades de monitoreo y supervisión de uso de equipos informáticos, de comunicación, de almacenamiento y demás infraestructura tecnológica activa"25.

RECOMENDACIONES:

Establecer un procedimiento formal para la gestión de los derechos de acceso de los usuarios de los sistemas de información, donde se entregue un documento a cada usuario indicando la información relacionada con el acceso (usuario y contraseña) y los requerimientos de protección de la información que tendrá bajo su responsabilidad.

DOMINIO 10: CIFRADO

HALLAZGOS:

Aunque existe un control para la asignación de privilegios de acceso a los sistemas de información, los mismos no se revisan periódicamente, ni existe procedimiento formal para realizarlo. El sistema automáticamente solicita cambio de contraseña de usuario cada seis (6) meses.

El proceso de gestión de claves de usuario se lleva a cabo por el administrador del sistema, quien autoriza o deniega los derechos de acceso a los diferentes servicios informáticos.

RECOMENDACIONES:

Establecer protocolos y documentar los procedimientos para la gestión de los derechos y niveles de acceso a los sistemas de información.

DOMINIO 11: SEGURIDAD FÍSICA Y AMBIENTAL

HALLAZGOS:

[25]UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. División de Sistemas. Procedimiento administración de los recursos informáticos. 23 de enero de 2015.

En el ítem de Áreas Seguras, se pudo determinar que no existen medidas efectivas para controlar el acceso a las áreas críticas en la División de Sistemas (Sala de servidores). Este cuarto de servidores es un área muy reducida de la dependencia que sólo la protege una puerta con llave. Esta situación pone en riesgo la seguridad de los activos que se encuentran en el área y la integridad, confidencialidad y disponibilidad de la información que allí se maneja.

Así mismo, se encontró que las copias de respaldo que se hacen diariamente por una parte, quedan almacenadas en el mismo servidor y una copia se guarda en el servidor de backup interno. Este último, se encuentra también en el cuarto de servidores, presentándose la misma situación de ineficiencia en los controles de acceso. Por otra parte, las copias que se hacen en formato DVD, se guardan en una caja con llave, y esta caja queda también en el mismo cuarto de servidores.

Cabe anotar que ni en el área de recepción, ni en el área administrativa de la División de Sistemas, existe cámara de vigilancia que pueda registrar los accesos a la misma. Sólo existe una cámara en el cuarto de servidores.

En cuanto al equipo de seguridad para la protección física de los activos, la Universidad cuenta con una subestación eléctrica que ha permitido regular las cargas de tensión, evitando la interrupción del servicio eléctrico y por ende, de las operaciones académicas y administrativas. Sin embargo, carece de un generador de emergencia (planta eléctrica) que permita darle continuidad a los servicios que ofrece la Universidad y por ende, evitar o reducir el riesgo de daño en los equipos de cómputo y la pérdida parcial o total de la información que allí se procesa, cuando el corte en el fluido eléctrico es prolongado.

Cabe destacar que la Universidad cuenta con pararrayos que ayuda a disminuir la posibilidad de daños en los equipos en los casos en los que se presenten descargas eléctricas.

De igual manera, la Universidad cuenta con extintores para casos de incendios. Sin embargo, aunque el personal de mantenimiento recibió adiestramiento en el manejo de los mismos en una oportunidad, este tipo de capacitaciones no se ha vuelto a realizar, teniendo en cuenta que una parte del personal del área ha sido cambiada. Así mismo, no existen alarmas contra incendios ni detectores de humo, que puedan poner en alerta al personal de la Universidad sobre la presencia de fuego.

Por otra parte, los equipos que manejan información sensible como los servidores y equipos principales de procesamiento, cuentan con un sistema de refrigeración adecuada (18^{o}C). Sin embargo, los niveles de humedad y la impermeabilidad en el cuarto de servidores no se controla a través de ningún mecanismo; situación que puede poner en riesgo la integridad de las copias de respaldo que se almacenan en este lugar.
Es importante resaltar, que a nivel de cableado, estas instalaciones se encuentran bien dotadas, utilizando las normas para cableado estructurado e independizando las conexiones eléctricas y de datos.

RECOMENDACIONES:

La Universidad Francisco de Paula Santander Ocaña, debe implementar las acciones contempladas en el Plan de Contingencias y en las Políticas de Seguridad, en cuanto a riesgos de seguridad física se refiere. Para esto, se sugiere:

- Implantar sistemas biométricos que permitan controlar de forma más eficiente el acceso a las áreas críticas de la División de Sistemas (cuarto de servidores).

- Instalar alarmas contra incendios, detectores de humo y salidas de emergencia, para minimizar el impacto que puede provocar la presencia de una catástrofe ambiental.

- Construir o adecuar un espacio fuera de las instalaciones de la Universidad, con las medidas de seguridad física necesarias para almacenar las copias de respaldo que se realizan diariamente en la División de Sistemas.

- Adquirir e implementar un sistema alterno de suministro eléctrico (planta eléctrica) para garantizar la continuidad de los servicios de información en los procesos críticos de la Universidad.

- Realizar campañas de sensibilización sobre la protección tanto de los equipos como de la información que cada funcionario, específicamente los que manejan sistemas de información, tiene bajo su responsabilidad.

- Implementar todas las acciones contemplados en el Documento PROCEDIMIENTO ADMINISTRACION DE LOS RECURSOS INFORMATICOS R-TT-DSS-002

DOMINIO 12: SEGURIDAD EN LA OPERATIVA

HALLAZGOS:

Actualmente el SITT cuenta con procedimientos documentados para diferentes actividades del sistema tales como ADMINISTRACIÓN DE RECURSOS INFORMÁTICOS, GESTIÓN DE LOS SISTEMAS DE TI, SOPORTE Y ATENCIÓN AL USUARIO, entre otros. Dichos procedimientos son controlados por la Oficina de Calidad que autoriza las modificaciones a los mismos a través del diligenciamiento de un formato de control de novedades. Dichas actualizaciones son comunicadas a través de la plataforma Web a toda la comunidad universitaria.

En el entorno de desarrollo de aplicaciones, las funciones propias de cada etapa (análisis, diseño, implementación, instalación, entre otras), no se encuentran segregadas. Solo existe un responsable de todo el proceso, que generalmente es realizado por pasantes o estudiantes de últimos semestres. Así mismo, la verificación del cumplimiento de cada una de las etapas anteriores, se realiza de manera interna, por el responsable del área, pero dicho procedimiento no se documenta.

En cuanto al proceso de respaldo de la información, cada servidor realiza de manera automática la copia de seguridad relacionada con el tipo de información que almacena (archivos de configuración, bases de datos, archivos de sistema, entre otros), y una vez terminado el proceso, esta información es enviada al servidor de backup interno. Posteriormente estos respaldos son almacenados en un datacenter externo contratado por la Universidad. Sin embargo, aunque se han ejecutado pruebas de restauración de los datos respaldados, éstas no se encuentran formalmente establecidas como procedimiento y por lo tanto, no se tiene registro de los resultados arrojados por el mismo.

RECOMENDACIONES:

Se recomienda definir y documentar las reglas para la transferencia de software del estado de desarrollo al de producción, incluyendo entre otros aspectos, el uso de perfiles de usuario diferentes en las fases de desarrollo, prueba y operación del sistema y los controles necesarios para evitar la introducción de rutinas fraudulentas que puedan poner en riesgo la integridad, disponibilidad y confidencialidad de los datos.

En cuanto a las copias de seguridad, se debe diseñar e implementar una política de respaldo que contenga los procedimientos para la realización de backup y su restauración. Así mismo, que contemple las acciones para definir el nivel necesario de respaldo de la información y la extensión y frecuencia de dicho procedimiento, de acuerdo con los requerimientos propios de la Universidad.

DOMINIO 13: SEGURIDAD EN LAS TELECOMUNICACIONES

HALLAZGOS:

En cuanto a la seguridad de las redes de datos que soportan todos los procesos de la Universidad, se tiene instalado un firewall o cortafuegos en cada red, para impedir el tráfico no autorizado desde Internet hacia la red interna y entre los equipos de la misma red, con el fin de evitar accesos no autorizados para modificar o sustraer información confidencial. Sin embargo, la red inalámbrica, no tiene este tipo de restricción.

La Política de Seguridad de la Información de la Universidad, contempla entre otros aspectos, las reglas de acceso a los servicios de red para los cuales han sido específicamente autorizados los usuarios. De igual forma, reglas para uso de la red interna e Internet, control de conexión a las redes, seguridad en comunicaciones, acceso lógico, entre otros.

De igual forma, se utiliza información de usuario y contraseña, como medida de protección para compartir recursos o información, a través de la red de datos.

RECOMENDACIONES:

Implementar controles para garantizar la protección de la información que transita a través de la red de datos; estos controles incluyen, segregación de responsabilidades, asignación de privilegios a los operarios de las redes, procedimientos documentados para mantener la disponibilidad de los servicios de la red.

DOMINIO 14: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

HALLAZGOS:

En el entorno de desarrollo aplicaciones, actualmente no existen tareas por cada etapa del proceso (análisis, diseño, implementación, instalación, entre otras) que se encuentren segregadas ni asignadas a diferentes usuarios. Quien diseña, codifica, implementa, instala, capacita, configura, etc.

A pesar que existe un procedimiento de gestión de los sistemas de información, cuyo fin es el de "solucionar las necesidades a nivel de desarrollo y actualización de software para cumplir con los requerimientos y dar soporte funcional para el mejoramiento continuo de los procesos"[26], las actividades de cada etapa del proceso de desarrollo de aplicaciones, no se documenta.

En lo relacionado con la realización de pruebas de los requerimientos operacionales de los nuevos sistemas (o actualizaciones) antes de su aceptación y uso, no existe un documento formal que establezca tal procedimiento. Solo se realizan pruebas internas.

En cuanto al proceso de adquisición de tecnología de hardware y/o software, se realizan proyecciones de los requerimientos en la ampliación de la capacidad tecnológica de acuerdo con lo establecido en el plan de acción de la División de Sistemas y evaluado por la Subdirección Administrativa que realiza el estudio de la necesidad.

RECOMENDACIONES:

Segregar las tareas propias en cada una de las fases del proceso de desarrollo de software. Así mismo, documentar las actividades en cada fase y definir los controles necesarios para especificar los requerimientos de seguridad antes y después del desarrollo de aplicaciones.

DOMINIO 15: RELACIONES CON SUMINISTRADORES

HALLAZGOS:

[26] UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. División de Sistemas. Procedimiento gestión de los sistemas de TI. 20 de septiembre de 2010.

Cuando se establecen acuerdos con terceros (contratistas, proveedores, entre otros), la verificación del cumplimiento de los servicios ofrecidos por éstos, es llevada a cabo por un supervisor del servicio, que pertenece a la Universidad.

Con respecto a las condiciones de protección y confidencialidad de la información que se intercambia con terceros, se establecen acuerdos de no divulgación para garantizar el uso adecuado y necesario de los datos. Sin embargo, no existen procedimientos formales para administrar los cambios en los servicios ofrecidos por los mismos.

RECOMENDACIONES:

Establecer formalmente protocolos para la prestación de servicios ofrecidos por terceros, que contemple entre otras cosas, el tratamiento del riesgo al proporcionar información confidencial, controles para garantizar el cumplimiento de los acuerdos y procedimientos para la gestión del cambio en dichos servicios.

DOMINIO 16: GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

HALLAZGOS:

La Universidad Francisco de Paula Santander Ocaña, no cuenta con procedimientos formales de reporte de eventos o debilidades que puedan tener un impacto en la seguridad de los activos institucionales.

Para los casos en los que se presentan fallas en los sistemas o que se detecte la presencia de alguna vulnerabilidad, existe un formato de bitácoras, que permite hacer el registro de las respectivas anomalías y es de manejo interno de la División de Sistemas.

A pesar de que se han presentado algunos casos de fallas en el sistema por ataques externos, el tratamiento que se le ha dado a estas situaciones, tampoco se encuentra documentado y, por lo tanto, no existe un procedimiento aprobado para el manejo efectivo de tales eventos una vez han sido reportados. Tampoco existe procedimiento alguno, para el monitoreo o revisión periódica de la bitácora de los sistemas; solo se lleva a cabo, cuando se presentan errores.

En cuanto a las evidencias de los eventos de seguridad, se hace revisión de los logs o archivos utilizados para registrar datos sobre quién, qué, cuándo, dónde y por qué ocurrió el evento para el caso particular de los administradores de los distintos sistemas de información. Para los usuarios de las aplicaciones, se encuentra habilitada en el motor de bases de datos, una función de auditoría interna, que permite registrar las actividades realizadas por los mismos.

RECOMENDACIONES:

Se recomienda establecer un procedimiento formal para el reporte de eventos de seguridad, así como el establecimiento de canales seguros para el reporte de los mismos. Junto con éste,

procedimientos para dar respuesta oportuna a dichos incidentes, asignando responsables o un punto de contacto, que atienda tales solicitudes.

Por otra parte, se sugiere entrenar a los usuarios de los sistemas de información y de aquellos que tengan activos de información a su cargo, sobre las diversas actividades de identificación y reporte de eventos de seguridad.

DOMINIO 17: ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

HALLAZGOS:

En la actualidad, la Universidad Francisco de Paula Santander Ocaña, no cuenta con un Plan de Continuidad del Negocio (PCN), que contemple las actividades necesarias para minimizar el impacto sobre la Institución y recuperarse de la pérdida de activos de información hasta un nivel aceptable.

Por su parte, existe un Plan de Contingencia (versión No. 1), elaborado con el fin de orientar los procedimientos relevantes con relación a protocolos y políticas de seguridad, backup, lineamientos para el desarrollo y actualización de los sistemas de información que son vitales para orientar las acciones ante una contingencia a la infraestructura informática en la Universidad Francisco de Paula Santander Ocaña. Se entenderá como infraestructura informática al hardware, software y elementos complementarios que soportan la información o datos críticos para la función de los procesos misionales y de apoyo[27].

RECOMENDACIONES:

Implementar un proceso de gestión de la continuidad del negocio, en adelante PCN, bajo estándares internacionales reconocidos y probados, para minimizar el impacto sobre la Universidad en caso de pérdida parcial o total de sus funciones de operación, provocada por eventos no intencionados como desastres naturales, accidentes, fallas en los equipos o cualquier otro incidente cometido de forma deliberada.

El proceso de gestión del PCN debe incluir la intervención de la dirección de la Universidad y de los estamentos que a nivel directivo puedan tomar decisiones para proveer soluciones al respecto. Dicho proceso requiere entre otras cosas, la realización permanente de análisis y evaluación de riesgos, que permitan identificar amenazas y vulnerabilidades en los elementos de información y calcular el impacto que la materialización de las mismas pueda generar en el desarrollo de las operaciones de la Universidad.

[27] UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. División de Sistemas. Plan de Contingencia de TI, 2010. Disponible en Internet: <https://ufpso.edu.co/ftp/doc/otrospro/sitt/L-TT-DSS-002A.pdf>

Por otra parte, el PCN debe contemplar la adquisición de pólizas que garanticen en gran medida el aseguramiento de los activos de información; considerar la implementación de controles preventivos; identificar los recursos financieros y organizacionales para tratar los requerimientos de seguridad y capacitar al personal para enfrentar situaciones adversas y poder responder oportuna y eficientemente a los mismos.

DOMINIO 18: CUMPLIMIENTO

HALLAZGOS:

La Política de Seguridad de la Información (versión No. 2), contempla las sanciones pertinentes y necesarias de aplicar en los casos en los que se incurra en algún delito informático de los que trata la Ley 1273 de 2009. Sin embargo, existen procedimientos que aunque se realizan, no se encuentran documentados, lo que evidencia una falta de organización y de estandarización en las actividades propias de la administración de la información y de los demás recursos informáticos.

RECOMENDACIONES:

Definir, documentar y actualizar todos los requerimientos legales, reguladores y contractuales y el enfoque de la Universidad para satisfacer esos requerimientos, para cada sistema de información. De igual forma se recomienda, que para efecto de revisión y publicación de procedimientos relacionados con sistemas de información, arquitecturas de hardware y software, telecomunicaciones, entre otros, en el equipo de Calidad, se cite a un experto en el tema, para que el resultado de dicha evaluación pueda ser lo más objetivo posible.

4.2 IDENTIFICACIÓN DEL ESTÁNDAR/METODOLOGÍA PARA EL DISEÑO DEL PLAN ESTRATÉGICO DE TECNOLOGÍAS DE INFORMACIÓN PETI

La creciente adopción de mejores prácticas de TI explica porque la industria de TI requiere mejorar la administración de la calidad y la confiabilidad de TI en los negocios y para responder a un creciente número de requerimientos regulatorios y contractuales. Sin embargo, existe el peligro de que las implementaciones de estas mejores prácticas, potencialmente útiles, puedan ser costosas y desenfocadas si son tratadas como guías puramente técnicas.

Para ser más efectivos, las mejores prácticas deberían ser aplicadas en el contexto del negocio, haciendo mayor énfasis donde su utilización proporcione el mayor beneficio a la organización. La alta dirección, los gerentes, auditores, oficiales de cumplimiento y directores de TI, deberían trabajar en armonía para estar seguros que las mejores prácticas conduzcan a servicios de TI económicos y bien controlados.

Cada empresa necesita ajustar la utilización de estándares y prácticas a sus requerimientos individuales. En este sentido, los tres estándares de los cuales se hablará a continuación, pueden desempeñar un papel muy útil: COBIT® e ISO/IEC 27002 para ayudar a definir lo que debería hacerse, e ITIL proporciona el cómo para los aspectos de la gestión de servicios.

Para efectos del presente proyecto, se definió un estándar con el cual trabajar para el diseño del PETI para la Universidad Francisco de Paula Santander Ocaña. A continuación se presenta un cuadro comparativo, entre diferentes estándares que suelen enmarcarse en el ámbito denominado **Gobierno de tecnologías de la información** (IT Governance): ITIL v3, ISO 27002:20103 y COBIT 4.1 (Ver Cuadro 1).

Cuadro 1. Análisis comparativo ITIL v3, ISO 270022:2013 y COBIT 4.1

DOMINIOS DE COBIT 4.1			
PLANEAR Y ORGANIZAR			
OBJ. DE CONTROL COBIT 4.1 PO1. DEFINIR UN PLAN ESTRATÉGICO DE TI	**ÁREAS CLAVE DE COBIT 4.1**	**ÁREAS CLAVE DE ITIL V3**	**ÁREAS CLAVE DE ISO/IEC 27002:2013**
PO1.1 Gestión del valor de TI	▪ Caso de negocio ▪ Asignación presupuestal ▪ Obtención de beneficios ▪ Evaluación de caso de negocio	▪ ¿Qué son los servicios? ▪ Creación de valor ▪ Estructuras del servicio ▪ Preparar la ejecución ▪ Gestión financiera	
PO1.2 Alineación de TI con el negocio	▪ Alineación de TI con la estrategia del negocio ▪ Involucramiento direccional y recíproco en el plan estratégico	▪ ¿Qué es gestión del servicio? ▪ El proceso de negocio ▪ Principios de la gestión del servicio	
PO1.3 Evaluación del desempeño y la capacidad actual	▪ Línea base del desempeño actual ▪ Evaluación de la contribución del negocio, funcionalidad, estabilidad, complejidad, costos, fortalezas y debilidades	▪ Preparar la ejecución ▪ Evaluaciones	
PO1.4 Plan estratégico de TI	▪ Definición de objetivos de TI ▪ Contribución a los objetivos de la empresa, presupuestos, financiación, compras y estrategia de adquisición	▪ Tipos de proveedor de servicio ▪ Fundamentos de la estrategia del servicio ▪ Desarrollar las ofertas ▪ Desarrollar activos estratégicos ▪ Estrategia de outsourcing	
PO1.5 Planes tácticos de TI	▪ Iniciativas de TI ▪ Requerimientos de recursos ▪ Monitoreo y gestión del logro de beneficios	▪ Preparar la ejecución ▪ Implementación a través del ciclo de vida ▪ Estrategia y diseño	
PO1.6 Gestión del portafolio de TI	▪ Definiendo, priorizando y gestionando programas ▪ Clarificando el alcance y los resultados del esfuerzo ▪ Asignando el rol de la rendición de	▪ El ciclo de vida del servicio ▪ Estructuras del servicio ▪ Gestión del portafolio de servicios ▪ Gestión de la demanda ▪ Diseño de soluciones de servicios	

	cuentas ▪ Asignando recursos y financiamiento		
OBJ. DE CONTROL COBIT 4.1 PO2 DEFINIR LA ARQUITECTURA DE INFORMACIÓN	**ÁREAS CLAVE DE COBIT 4.1**	**ÁREAS CLAVE DE ITIL V3**	**ÁREAS CLAVE DE ISO/IEC 27002:2013**
PO2.1 Modelo de arquitectura de información empresarial	▪ Análisis de soporte a las decisiones ▪ Mantenimiento del modelo de arquitectura de información ▪ Modelo corporativo de datos	▪ Aspectos de diseño ▪ Diseño de la arquitectura tecnológica ▪ Arquitectura orientada al servicio del negocio	
PO2.2 Diccionario de datos empresarial y reglas de sintaxis de datos	▪ Diccionario corporativo de datos ▪ Comprensión general de los datos	▪ Gestión de los datos y la información	▪ Inventario de activos ▪ Políticas de control de acceso
PO2.3 Esquema de clasificación de datos	▪ Clases de información ▪ Propietarios ▪ Retención ▪ Reglas de acceso ▪ Niveles de seguridad para cada clase de información	▪ Gestión de los datos y la información	▪ Directrices de clasificación ▪ Acuerdos de intercambio ▪ Políticas de control de acceso
PO2.4 Gestión de integridad	▪ Integridad y consistencia de los datos	▪ Gestión de los datos y la información	
OBJ. DE CONTROL COBIT 4.1 PO3. DETERMINAR LA ORIENTACIÓN TECNOLÓGICA	**ÁREAS CLAVE DE COBIT 4.1**	**ÁREAS CLAVE DE ITIL V3**	**ÁREAS CLAVE DE ISO/IEC 27002:2013**
PO3.1 Planeamiento de la orientación tecnológica	▪ Tecnologías disponibles ▪ Habilitación de la estrategia de TI ▪ Arquitectura de sistemas ▪ Dirección tecnológica ▪ Estrategias de migración	▪ Estrategia y tecnología	▪ Revisión de la política para la seguridad de la información ▪ Planificación de la continuidad de la seguridad de la información
PO3.2 Plan de infraestructura	▪ Plan de infraestructura tecnológica	▪ Diseño de la arquitectura tecnológica	

tecnológica	▪ Orientación sobre adquisiciones ▪ Economías de escala ▪ Interoperabilidad de plataformas		
PO3.3 **Monitoreo de tendencias y regulaciones futuras**	▪ Sector del negocio, industria, tecnología, infraestructura, las tendencias legales y reglamentarias		
PO3.4 **Estándares tecnológicos**	▪ Fórum tecnológico ▪ Estándares y directrices de productos		▪ Pruebas de aceptación
PO3.5 **Consejo de arquitectura de TI**	▪ Estándares y directrices de arquitectura tecnológica		
OBJ. DE CONTROL COBIT 4.1 **PO4.** **DEFINIR LOS PROCESOS, ORGANIZACIÓN Y RELACIONES DE TI**	**ÁREAS CLAVE DE COBIT 4.1**	**ÁREAS CLAVE DE ITIL V3**	**ÁREAS CLAVE DE ISO/IEC 27002:2013**
PO4.1 **Marco de trabajo de procesos de TI**	▪ Estructura y relaciones del proceso de TI ▪ Propiedad de los procesos ▪ Integración con los procesos del negocio, la gestión del portafolio de la empresa y los procesos de cambio	▪ Preservando valor ▪ Efectividad en mediciones ▪ Diseño de la arquitectura tecnológica ▪ Análisis de roles funcionales ▪ Roles y responsabilidades ▪ Marcos, modelos ▪ estándares y sistemas de calidad	▪ Asignación de responsabilidades para la seguridad de la información ▪ Segregación de tareas
PO4.2 Comité estratégico de TI	▪ Comité de dirección ▪ Gobierno de TI ▪ Dirección estratégica ▪ Revisión de las inversiones	▪ Alcance	
PO4.3 **Comité directivo de TI**	▪ Priorización del programa de inversiones y el seguimiento de estado de proyectos ▪ Resolución de recursos ▪ Servicios de monitoreo		
PO4.5 **Estructura organizacional de TI**	▪ Alineamiento organizacional con ▪ las necesidades del negocio	▪ Funciones y procesos a través del ciclo de vida	

		▪ Desarrollo organizacional ▪ Diseño organizacional ▪ Estrategia de outsourcing	
PO4.6 **Establecer roles y responsabilidades**	▪ Roles y responsabilidades explícitos. ▪ Clara rendición de cuentas y autorizaciones de usuario final	▪ Funciones y procesos a través del ciclo de vida ▪ Organización para la mejora continua del servicio	▪ Asignación de las responsabilidades para la seguridad de la información
PO4.7 **Responsabilidades para el aseguramiento de la calidad de TI**	▪ Responsabilidad, experiencia e implementación de control de calidad según los requisitos de la organización	▪ Organización para la mejora continua del servicio	
PO4.10 **Supervisión**	▪ Ejecución apropiada de roles y responsabilidades ▪ Evitar el compromiso de procesos críticos	▪ Gestión de seguridad de la información y la operación del servicio	▪ Segregación de tareas ▪ Separación de los entornos de desarrollo, prueba y producción
PO4.12 **Personal de TI**	▪ Número y competencia; evaluación de requerimientos ▪	▪ Mesa de servicios	
PO4.13 **Personal clave de TI**	▪ Roles clave definidos ▪ Minimizar dependencia del staff		
PO4.14 **Políticas y procedimientos para el personal contratado**	▪ Conocimiento y cumplimiento de políticas ▪ Activos de información protegidos		▪ Acuerdos de confidencialidad y secreto ▪ Tratamiento del riesgo dentro de acuerdos de suministradores ▪ Política de seguridad de la información para suministradores ▪ El trabajo en áreas seguras
OBJ. DE CONTROL COBIT 4.1 **PO5.** **GESTIONAR LA INVERSIÓN EN TI**	**ÁREAS CLAVE DE COBIT 4.1**	**ÁREAS CLAVE DE ITIL V3**	**ÁREAS CLAVE DE ISO/IEC 27002:2013**

PO5.2 **Priorización dentro del presupuesto de TI**	▪ Asignación de recursos de TI ▪ Optimización del ROI	▪ Retorno sobre la inversión ▪ Gestión del portafolio de servicios	
PO5.5 **Gestión de beneficios**	▪ Monitoreo y análisis de beneficios ▪ Mejora de la contribución de TI ▪ Mantenimiento de los casos de negocio	▪ ¿Qué son los servicios? ▪ Gestión financiera ▪ Retorno sobre la inversión	
OBJ. DE CONTROL COBIT 4.1 **PO6.** **COMUNICAR LAS ASPIRACIONES Y LA DIRECCIÓN DE LA GERENCIA**	**ÁREAS CLAVE DE COBIT 4.1**	**ÁREAS CLAVE DE ITIL V3**	**ÁREAS CLAVE DE ISO/IEC 27002:20132**
PO6.1 **Política y entorno de control de TI**	▪ Filosofía de gestión y estilo de operación ▪ Integridad, ética, competencias, rendir cuentas y responsabilidad ▪ Cultura de entrega de valor y gestión de riesgos		▪ Conjunto de políticas para la seguridad de la información
PO6.3 **Gestión de políticas de TI**	▪ Creación de políticas ▪ Política propuesta, roles y responsabilidades		▪ Conjunto de políticas para la seguridad de la información ▪ Revisión de las políticas para la seguridad de la información
PO6.4 **Implantación de políticas, estándares y procedimientos**	▪ Distribución y aplicación de las políticas al staff		
PO6.5 **Comunicación de los objetivos y de la dirección de TI**	▪ Conciencia y comprensión de los objetivos de TI y del negocio	▪ Gestión de las comunicaciones y el compromiso ▪ Comunicaciones	▪ Conjunto de políticas para la seguridad de la información
OBJ. DE CONTROL COBIT 4.1 **PO7.** **GESTIÓN DE LOS RECURSOS HUMANOS DE TI**	**ÁREAS CLAVE DE COBIT 4.1**	**ÁREAS CLAVE DE ITIL V3**	**ÁREAS CLAVE DE ISO/IEC 27002:2013**
PO7.2	▪ Definición de las competencias		

Competencias personal	básicas ▪ Verificación de competencias		
PO7.4 **Entrenamiento del personal de TI**	▪ Inducción organizacional y entrenamiento continuo para elevar los niveles de habilidad técnica y gerencial	▪ Habilidades y atributos	▪ Concienciación, educación y capacitación en seguridad de la información
PO7.6 **Verificación de antecedentes de personal**	▪ Acreditaciones de seguridad según la criticidad de la posición		▪ Investigación de antecedentes
PO7.8 **Cambios y ceses en los puestos de trabajo**	▪ Transferencia y reasignación del conocimiento a fin de minimizar riesgos		▪ Cese o cambio de puesto de trabajo ▪ Devolución de activos ▪ Retirada o adaptación de los derechos de acceso
ADQUIRIR E IMPLEMENTAR			
OBJ. DE CONTROL COBIT 4.1 **AI3.** **ADQUIRIR Y MANTENER LA INFRAESTRUCTURA TECNOLÓGICA**	**ÁREAS CLAVE DE COBIT 4.1**	**ÁREAS CLAVE DE ITIL V3**	**ÁREAS CLAVE DE ISO/IEC 27002:2013**
AI3.3 **Mantenimiento de la infraestructura**	▪ Control de cambios, gestión de parches, estrategias de actualización y requerimientos de seguridad	▪ Gestión y soporte de servidores ▪ Gestión de redes ▪ Administración de bases de datos	▪ El trabajo en áreas seguras ▪ Mantenimiento de los equipos ▪ Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
AI5.1 **Control de adquisiciones**	▪ Estándares y procedimientos alineados con el proceso de adquisiciones de la empresa	▪ Adquisición de la solución elegida	▪ Acuerdos de confidencialidad y secreto
AI5.3 **Selección de proveedores**	▪ Proceso de selección justo y formal ▪ Mejor ajuste viable de los requerimientos	▪ Evaluación de soluciones alternativas ▪ Nuevos proveedores y contratos	
ENTREGAR Y DAR SOPORTE			

OBJ. DE CONTROL COBIT 4.1 DS4. GARANTIZAR LA CONTINUIDAD DEL SERVICIO	ÁREAS CLAVE DE COBIT 4.1	ÁREAS CLAVES DE ITIL V3	ÁREAS CLAVES DE ISO/IEC 27002
DS4.1 Marco de trabajo de continuidad de TI	▪ Enfoque consistente y corporativo a la gestión de continuidad	▪ Gestión de continuidad de servicios de TI ▪ Gestión de continuidad de servicios de TI	▪ Planificación de la continuidad de la seguridad de la información
DS4.2 Planes de continuidad de TI	▪ Planes individuales de continuidad ▪ Análisis de impacto en el negocio ▪ Resiliencia, procesamiento alternativo y recuperación		▪ Contacto con las autoridades ▪ Contacto con grupos de interés especial
DS4.4 Mantenimiento del plan de continuidad de TI	▪ Control de cambios para reflejar los requerimientos cambiantes del negocio	▪ Etapa 4 – Operación continua	▪ Verificación, revisión y evaluación de la continuidad de la seguridad de la información
DS4.9 Almacenamiento externo de respaldos	▪ Almacenamiento externo de los medios críticos; documentación y recursos necesarios, en colaboración con los dueños de los procesos de negocio	▪ Etapa2-Requisitos y estrategia ▪ Respaldo y restauración	▪ Copias de seguridad de la información
DS2.2 Gestión de relaciones con Proveedores	▪ Enlace respecto a temas del cliente y el proveedor ▪ Confianza y transparencia	▪ Gestión y desempeño de proveedores y contratos ▪ Renovación de términos	▪ Política de seguridad de la información para suministradores ▪ Gestión de cambios a los servicios prestados por terceros
DS2.4 Monitoreo del desempeño Proveedores	▪ Satisfacer los requerimientos del negocio, adhesión a los contratos y desempeño competitivo		▪ Política de seguridad de la información para suministradores ▪ Supervisión y revisión de los servicios prestados por terceros
DS3.4 Disponibilidad de	▪ Provisión de recursos, contingencias, tolerancia a fallas y	▪ Gestión de la capacidad de los componentes	

recursos de TI	priorización de recursos	▪ Actividades de soporte de la gestión de capacidad ▪ Gestión de la disponibilidad	
DS4.1 Marco de trabajo de continuidad de TI	▪ Enfoque consistente y corporativo a la gestión de continuidad	▪ Gestión de continuidad de servicios de TI ▪ Gestión de continuidad de servicios de TI	▪ Contacto con las autoridades ▪ Contacto con grupos de interés especial ▪ Implantación de la continuidad de la seguridad de la información
DS4.2 Planes de continuidad de TI	▪ Planes individuales de continuidad ▪ Análisis de impacto en el negocio ▪ Resiliencia, procesamiento alternativo y recuperación	▪ Etapa 2 – Requisitos y estrategia ▪ Etapa 3 – Implementación	▪ Contacto con las autoridades ▪ Contacto con grupos de interés especial
DS4.4 Mantenimiento del plan de continuidad de TI	▪ Control de cambios para reflejar los requerimientos cambiantes del negocio	▪ Etapa 4 – Operación continua	▪ Verificación, revisión y evaluación de la continuidad de la seguridad de la información
DS4.5 Pruebas del plan de continuidad de TI	▪ Pruebas regulares ▪ Implementación del plan de acción	▪ Etapa 3 –Implementación ▪ Etapa 4 – Operación continua	▪ Verificación, revisión y evaluación de la continuidad de la seguridad de la información
DS4.8 Recuperación y reanudación de los servicios de TI	▪ Planificación del período cuando TI se esté recuperando y reanudando servicios ▪ Entendimiento del negocio y soporte a la inversión	▪ Actividades proactivas de la gestión de la disponibilidad ▪ Etapa 4 – Operación continua	▪ Planificación de la continuidad de la seguridad de la información
DS4.9 Almacenamiento externo de respaldos	▪ Almacenamiento externo de los medios críticos; documentación y recursos necesarios, en colaboración con los dueños de los procesos de negocio	▪ Etapa 2 – Requisitos y estrategia ▪ Respaldo y restauración	▪ Copias de seguridad de la información
DS5.1 Gestión de la seguridad de TI	▪ Ubicar la gestión de seguridad a	▪ Gestión de seguridad de la información ▪ Gestión de seguridad de la	▪ Conjunto de políticas para la seguridad de la información

	alto nivel para cumplir con las necesidades del negocio	información y la operación del servicio	
OBJ. DE CONTROL COBIT 4.1 DS4. GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS	**ÁREAS CLAVE DE COBIT 4.1**	**ÁREAS CLAVE DE ITIL V3**	**ÁREAS CLAVES DE ISO/IEC 27002**
DS5.2 Plan de Seguridad de TI	▪ Traducción de requerimientos de negocio, riesgo y cumplimiento en un plan de seguridad	▪ Políticas, principios y conceptos básicos ▪ Controles de seguridad (cobertura a alto nivel, sin detalle)	▪ Conjunto de políticas para la seguridad de la información ▪ Revisión de la política para la seguridad de la información
DS5.3 Gestión de identidad	▪ Identificación de todos los usuarios (internos, externos y temporales) y su actividad	▪ Gestión de acceso	▪ Conjunto de políticas para la seguridad de la información ▪ Revisión de la política para la seguridad de la información ▪ Acuerdos de confidencialidad y secreto
DS5.4 Gestión de cuentas de usuario	▪ Gestión del ciclo de vida de las cuentas de usuario y privilegios de acceso	▪ Gestión de acceso ▪ Peticiones de acceso ▪ Verificación ▪ Habilitar privilegios ▪ Monitorear el estado de la identidad ▪ Registro y seguimiento	▪ Acuerdos de confidencialidad y secreto ▪ Tratamiento del riesgo dentro de acuerdos de suministradores ▪ Cese o cambio de puesto de trabajo ▪ Retirada o adaptación de los derechos de acceso
DS5.6 Definición de incidente de seguridad	▪ Definición y clasificación de las características de los incidentes de seguridad	▪ Controles de seguridad(cobertura de alto nivel, sin detalle) ▪ Gestión de brechas de seguridad e incidentes	▪ Proceso disciplinario ▪ Notificación de los eventos de seguridad de la información ▪ Notificación de puntos débiles de la seguridad

DS5.7 Protección de la tecnología de seguridad	▪ Resistencia a la manipulación	▪ Gestión y soporte de servidores	▪ Áreas de acceso público, carga y descarga ▪ Emplazamiento y protección de equipos
DS5.9 Prevención, detección y corrección de software malicioso	▪ •Parches de actualización, control de virus y protección de malware		▪ Controles contra el código malicioso
OBJ. DE CONTROL COBIT 4.1 DS4. GESTIONAR AMBIENTE FÍSICO	**ÁREAS CLAVE DE COBIT 4.1**	**ÁREAS CLAVE DE ITIL V3**	**ÁREAS CLAVE DE ISO/IEC 27002**
DS12.3 Acceso físico	▪ Acceso controlado a los locales	▪ Descripción detallada de la gestión de las instalaciones ▪ Controles de acceso físico	▪ Tratamiento del riesgo dentro de acuerdos de suministradores ▪ Controles físicos de entrada ▪ El trabajo en áreas seguras ▪ Áreas de acceso público, carga y descarga ▪ Seguridad de los equipos y activos fuera de las instalaciones
DS12.4 Protección contra factores ambientales	▪ Monitoreo y control de factores ambientales	▪ Descripción detallada de la gestión de las instalaciones	▪ Protección contra las amenazas externas y ambientales ▪ Emplazamiento y protección de equipos ▪ Seguridad del cableado
DS13.5 Mantenimiento preventivo del hardware	▪ Mantenimiento para reducir el impacto de fallas	▪ Gestión de mainframe ▪ Gestión y soporte de servidores	▪ Mantenimiento de los equipos
Fuente: ARRIETA SÁNCHEZ, María Alejandra, et al.			

Entre los tres estándares que se enfocan al Gobierno de las Tecnologías de la Información, en primera instancia, "**ITIL v3** (Information Technology Infraestructure Library o Biblioteca de Infraestructura de Tecnologías de la Información) se define como un compendio de publicaciones, o librería, que describe de manera sistemática un conjunto de "buenas prácticas" para la gestión de los servicios de Tecnología Informática (en adelante TI)"[28].

Uno de sus volúmenes, denominado Estrategia de Servicios, plantea que el "objetivo de la Estrategia de Servicio es la de incluir las TI en la Estrategia Empresarial de manera que se pueda calibrar los objetivos según la infraestructura TI y adaptar cada uno a las necesidades del otro. Las modificaciones de estructura que ha sufrido la biblioteca ITIL han situado finalmente a la estrategia empresarial relacionada con el servicio de las TI como parte principal y como eje en el Ciclo de Vida ITIL".

Por su parte, el estándar internacional **ISO/IEC 27002:2013**, tiene como objetivo "brindar información a los responsables de la implementación de seguridad de la información de una organización. Puede ser visto como una buena práctica para desarrollar y mantener normas de seguridad y prácticas de gestión en una organización para mejorar la fiabilidad en la seguridad de la información en las relaciones interorganizacionales"[29]. En él se definen las estrategias de 114 controles de seguridad organizados bajo 14 dominios y 35 objetivos de control. La norma resalta la importancia de la gestión del riesgo y hace énfasis en que no es necesario aplicar todos los controles, sino sólo aquellos que sean necesarios. Los dominios de la norma, son los puntos de partida para la implementación de la seguridad de la información

Por su parte, **"COBIT,** es un marco de referencia globalmente aceptado para el gobierno de TI basado en estándares de la industria y las mejores prácticas. Una vez implementado, los ejecutivos pueden asegurarse de que se ajusta de manera eficaz con los objetivos del negocio y dirige mejor el uso de TI para obtener ventajas comerciales"[30].

[28] RÍOS HUÉRCANO, Sergio. Manual ITIL v3 Íntegro. Disponible en Internet: <http://es.slideshare.net/Biable/manual-itil-integro>

[29] IT GOVERNANCE INSTITUTE. Alineando COBIT 4.1, ITIL v3 e ISO 27002 en beneficio de la empresa. 2008. p. 17. Disponible en Internet: <http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-COBIT-4-1-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa_res_Spa_0108.pdf>

[30] Ibid., p. 13

Se ha optado para diseñar el **Plan Estratégico de Tecnologías de la Información PETI** 2016 – 2018 para la Universidad Francisco de Paula Santander Ocaña, el estándar internacional COBIT 4.1, ya que brinda las mejores prácticas para la gestión de las actividades de TI, proporcionado métodos para evaluar si los servicios de TI satisfacen los requisitos de la organización y si se logran los objetivos propuestos. Así mismo, este marco describe específicamente, cómo los procesos de TI entregan la información que el negocio necesita para alcanzar sus objetivos.

COBIT 4.1, establece cuatro dominios así: Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar. El primero, y en el que está basada la presente propuesta, cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir eficientemente al logro de los objetivos del negocio. Este dominio cubre los siguientes aspectos:

- Alineación de las estrategias de TI y del negocio
- Optimización en el uso de sus recursos
- Entendimiento de los objetivos de TI por parte del personal de la organización
- Administración de riesgos de TI
- Soporte de TI para las necesidades del negocio

4.3 DOCUMENTO PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

A continuación se presenta el documento que contiene todas las actividades relacionadas con el diseño del Plan Estratégico de Tecnologías de la Información PETI para la Universidad Francisco de Paula Santander Ocaña, para la vigencia 2016 – 2018:

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

Plan Estratégico de Tecnologías de la Información

2016 – 2018

Hacia la Excelencia Institucional

ÍNDICE

INTRODUCCIÓN

La Dirección de la Universidad Francisco de Paula Santander Ocaña, ha priorizado el componente tecnológico como un aspecto clave para el logro de los objetivos estratégicos de la Institución, los cuales se orientan al diseño, administración y mantenimiento de los sistemas de información, las telecomunicaciones y la infraestructura tecnológica, utilizados para el desarrollo de los procesos de la Universidad de manera eficaz, efectiva y oportuna.

La incorporación de tecnología en los procesos de la Universidad, debe realizarse con base en una planificación con visión y objetivos claros, alineada a los objetivos institucionales y con un enfoque de soporte efectivo a sus procesos.

De acuerdo con lo anterior, se dio inicio al proceso de diseño y formulación del Plan Estratégico de Tecnologías de la Información PETI, el cual pretende definir el enfoque tecnológico para la Universidad y la forma como este enfoque se aplica en sus procesos para la prestación eficiente de sus servicios académicos y administrativos.

Para la elaboración de dicho plan, ha sido necesario:

- La revisión y análisis de la situación actual de la Universidad desde el punto de vista tecnológico; este diagnóstico se realizó a partir de una auditoría de cumplimiento bajo el estándar ISO 27002:2013, evaluando sus 14 Dominios, 35 Objetivos de Control y 114 Controles.

- La definición de componentes estratégicos de Tecnología de Información TI, a partir del estándar internacional COBIT 4.1.

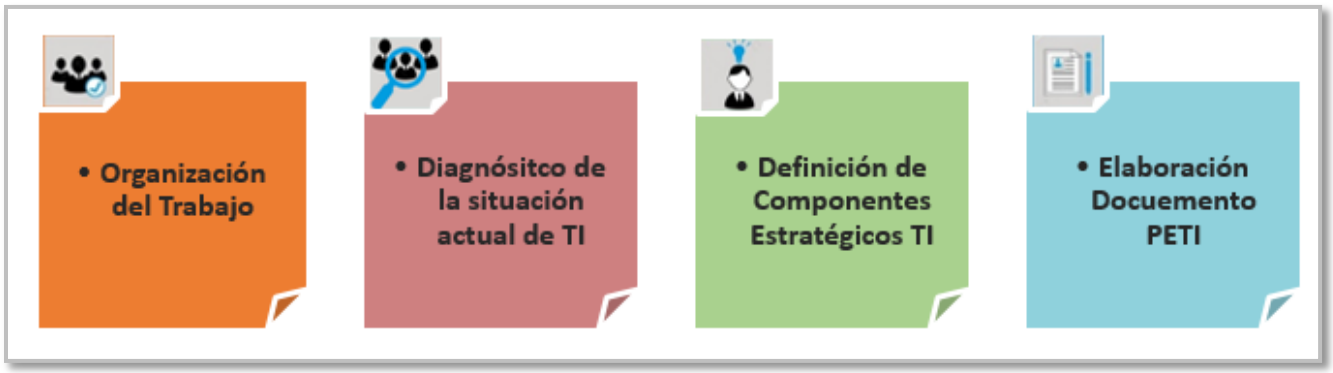
- La conformación de la estructura del PETI con base en la definición de metas asociadas a cada una de las líneas estratégicas identificadas y los programas y proyectos que deben ejecutarse para el cumplimiento de las mismas. El contenido de este documento muestra el desarrollo de cada una de las etapas necesarias para la formulación del Plan Estratégico de Tecnologías de la Información PETI, con sus respectivos anexos.

1. DESARROLLO DEL PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN – PETI

El desarrollo del Plan Estratégico de Tecnologías de Información se realizó según una metodología probada en diversos estudios y en el Plan de Trabajo aprobado por la Universidad en cabeza del Jefe de la División de Sistemas.

En cuanto al enfoque metodológico para la Formulación del Plan Estratégico de Tecnologías de Información, a continuación se mencionan y describen las siguientes etapas:

Figura 2. Etapas formulación Plan Estratégico de Tecnologías de la Información



Fuente: ARRIETA SÁNCHEZ, María Alejandra, et al.

Etapa Uno.

Organización del Trabajo. Comprende la definición de las actividades relacionadas con el diseño del PETI, y la asignación de responsables para la ejecución de cada una de las fases del proceso.

Etapa Dos

Diagnóstico de la Situación Actual TI. Contempla la revisión de la situación actual de TI en la Universidad, en cuanto a operatividad, infraestructura, seguridad y eficiencia de su plataforma tecnológica, tomando como referencia los 14 dominios, 35 objetivos de control y 114 controles del estándar ISO 27002:2013. El producto de esta etapa, se muestra en un capítulo posterior del presente documento.

Etapa Tres

Definición de Componentes Estratégicos TI. Comprende la definición de lineamientos estratégicos TI, a partir del análisis DOFA y de la identificación de los Factores claves de Éxito, de acuerdo con el estándar internacional COBIT 4.1.

Etapa Cuatro

Elaboración del Documento PETI. Contiene las metas asociadas a cada una de las líneas estratégicas identificadas y los programas y proyectos que deben ejecutarse para el cumplimiento de las mismas.

2. ETAPA UNO: ORGANIZACIÓN DEL TRABAJO

La organización, diseño y ejecución de las actividades relacionadas con la elaboración del Plan Estratégico de Tecnologías de la Información PETI para la Universidad Francisco de Paula Santander Ocaña, se muestran en el Anexo J.

3. ETAPA DOS: DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

3.1 Aspectos Generales

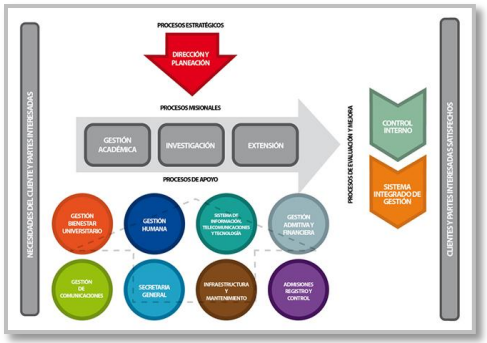
3.1.1 La Universidad Francisco de Paula Santander Ocaña. La Universidad Francisco de Paula Santander Ocaña, como institución pública de educación superior en esta zona del país tiene la responsabilidad social de ser actor protagónico del desarrollo académico, científico, cultural y socioeconómico en los escenarios locales, regionales e internacionales con calidad y eficiencia.

3.1.2 Organización. Con miras a la excelencia institucional, la Universidad ha adoptado el Sistema Integrado de Gestión como una filosofía para dirigir y evaluar el desempeño institucional orientado al mejoramiento de los productos y/o servicios que se ofrecen al estudiante y a la sociedad.

De conformidad con lo establecido en el decreto 1599 de 2005 por el cual se adopta el Modelo Estándar de Control Interno para el Estado Colombiano, la ley 872 de 2003 por el cual se crea el Sistema de Gestión de la Calidad y el decreto 4110 de 2004 por medio de la cual se adopta la NTCGP 1000, la Institución ha logrado consolidar un modelo de operación por procesos, que articula los estándares y requisitos de estas normas para la gestión sistemática y transparente a través de la evaluación del desempeño institucional en términos de calidad y satisfacción social en la prestación de servicios.

El enfoque por procesos permite mejorar la satisfacción de los clientes y el desempeño de la gestión de la Universidad en su misión de formar profesionales idóneos; la implementación de la NTCGP 1000:2009 permite el cumplimiento de la norma internacional ISO 9001:2008 que brinda como beneficios herramientas para el uso eficiente de los recursos, la toma de decisiones basada en evidencias objetivas y hacia el logro del plan de desarrollo y el cumplimiento de los requisitos y las necesidades en materia de formación profesional. El mapa de procesos se muestra a continuación:

Figura 3. Mapa de Procesos Universidad Francisco de Paula Santander Ocaña

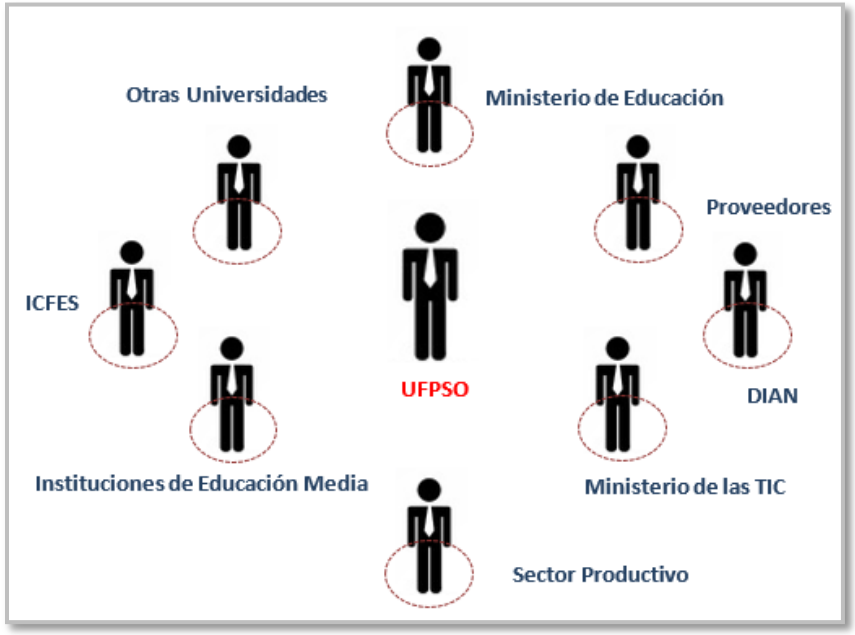


Fuente: www.ufpso.edu.co/sig/procedimientos_sig.html#arbol_procesos

El alcance del Plan Estratégico de Tecnologías de Información PETI, comprende la revisión y análisis del componente tecnológico presente en cada uno de los Ejes Estratégicos contemplados en el Plan de Desarrollo Institucional 2014 – 2019 y en los Planes de Acción para el año 2015.

3.1.3 Grupos de Interés. La Universidad Francisco de Paula Santander interactúa con otras instituciones de educación superior, así como con otros grupos de interés (públicos y privados) cuyos actores en muchos casos solicitan, brindan y/o intercambian información (física o virtual). Entre los principales grupos de interés de la Universidad se tienen los mostrados en la siguiente imagen:

Figura 4. Grupos de Interés UFPSO



Fuente: ARRIETA SANCHEZ, María A, et al.

3.2 Orientación Estratégica de la Universidad y la contribución de las Tecnologías de la Información

La Universidad Francisco de Paula Santander, cuenta actualmente con un Plan de Desarrollo Institucional "Hacia la Excelencia Institucional" formulado para la vigencia 2014 – 2019, con el cual reafirma su voluntad y compromiso de hacer de la educación superior, un factor dinamizador del desarrollo regional y nacional. Así mismo plantea, que el posicionamiento de la Universidad en el siglo XXI, implica incorporar las Tecnologías de Información y Comunicación a todos los procesos institucionales, administrativos y académicos, además de fortalecer los procesos de conectividad que le permitan ser un referente para las demás instituciones educativas y administraciones municipales de la región.

3.2.1 Misión y Visión institucionales

El Plan de Desarrollo Institucional, como todo documento estratégico, cuenta con una misión y visión claramente definidas, las cuales son consideradas como el núcleo de la orientación estratégica institucional.

Misión

- La Universidad Francisco de Paula Santander Ocaña, institución pública de educación superior, es una comunidad de aprendizaje y autoevaluación en mejoramiento continuo, comprometida con la formación de profesionales idóneos en las áreas del conocimiento, a través de estrategias pedagógicas innovadoras y el uso de las tecnologías; contribuyendo al desarrollo nacional e internacional con pertinencia y responsabilidad social.

Visión

- La Universidad Francisco de Paula Santander Ocaña para el **2019**, será reconocida por su excelencia académica, cobertura y calidad, a través de la investigación como eje transversal de la formación y el uso permanente de plataformas de aprendizaje; soportada mediante su capacidad de gestión, la sostenibilidad institucional, el bienestar de su comunidad académica, el desarrollo físico y tecnológico, la innovación y la generación de conocimiento, bajo un marco de responsabilidad social y ambiental hacia la proyección nacional e internacional.

Para el logro de la misión y la visión, se hace necesario que las Tecnologías de la Información, brinden el soporte para consolidar sus factores clave de éxito y facilitar el logro de sus objetivos estratégicos a mediano y largo plazo.

3.2.2 Factores clave de éxito. Según Rockart (1986), los Factores Clave de Éxito - FCE se definen como el número limitado de áreas, en las cuales los resultados, si son satisfactorios, asegurarán un funcionamiento competitivo y exitoso para la organización. Para el caso de la Universidad Francisco de Paula Santander Ocaña por ser una institución pública, los FCE se constituyen en las variables que pueden afectar su posición comparativa y de cumplimiento de su orientación estratégica.

A continuación se muestra en color verde aquellos FCE que son más sensibles o en los que podría existir una mayor contribución potencial de las Tecnologías de Información TI, en color amarillo los medianamente sensibles, y finalmente en color rojo los que de manera comparativa con los anteriores serían los menos sensibles y/o sólo con impacto indirecto de las TI en los FCE. Los FCE son tomados de los ejes estratégicos del Plan de Desarrollo Institucional vigencia 2014 – 2019.

Cuadro 2. Factores Clave de Éxito Universidad Francisco de Paula Santander Ocaña

FACTORES CLAVE DE ÉXITO – FCE		DESCRIPCIÓN DEL FCE	OBJETIVO GENERAL	POTENCIAL CONTRIBUCIÓN DE LAS TI
FCE 1	**Investigación y Formación Académica**	Implica la necesidad de considerar a la investigación como eje transversal de la formación académica.	Incorporar e implementar las TIC en los procesos académicos, la cualificación docente, la calidad y pertinencia de la oferta, la cobertura y el desarrollo estudiantil.	Mejorar los procesos académicos a través de la apropiación de las TI.
FCE 2	**Desarrollo físico y tecnológico**	Comprende la modernización de la infraestructura tecnológica y la adecuación de los espacios para el	Fortalecer la gestión tecnológica, modernizar los recursos y adecuación de espacios físicos	Mejorar la infraestructura física y tecnológica.

		desarrollo de las actividades académicas y administrativas.	suficientes para el desarrollo de las funciones institucionales.	
FCE 3	**Sostenibilidad administrativa y financiera**	Comprende el mejoramiento de los procesos de planeación, ejecución y evaluación administrativa y financiera.	Implementar y mantener procesos eficientes en la planeación, ejecución y evaluación administrativa y financiera.	Optimizar los servicios institucionales para lograr la satisfacción de sus clientes y terceros.
FCE 4	**Bienestar Institucional**	Tiene en cuenta la creación de programas para la formación integral y el desarrollo de los miembros de la comunidad universitaria.	Generar programas para la formación integral, el desarrollo humano y el acompañamiento institucional que permitan el mejoramiento de las condiciones de vida de la comunidad universitaria.	Brindar soporte para el mejoramiento de los servicios de seguimiento a egresados y acompañamiento a estudiantes.
FCE 5	**Visibilidad nacional e internacional**	Comprende las acciones necesarias para fortalecer la investigación, docencia y extensión en el ámbito internacional.	Integrar, transformar y fortalecer las funciones de investigación, docencia y extensión para su articulación en un ambiente globalizado de excelencia y competitividad.	Brindar soporte para la creación de espacios para trabajo colaborativo con grupos de investigación a nivel internacional.
FCE 6	**Impacto y proyección social**	Tiene en cuenta la proyección social de la Universidad en la región.	Desarrollar las capacidades institucionales promoviendo impactos positivos en la región, el medio ambiente y la comunidad.	Brindar soporte para las diferentes actividades de extensión, a través de la implementación de TI.
Fuente: ARRIETA SANCHEZ, María A., et al.				

3.3 Diagnóstico

El Diagnóstico incluye la revisión y análisis de la situación actual de la Universidad, tomando como referencia aspectos internos desde el punto de vista operativo y tecnológico así como aspectos de tipo administrativo y académico.

3.3.1 Evaluación de la Capacidad de Gestión TI según ISO 27002:2013. La Universidad Francisco de Paula Santander Ocaña dentro de sus procesos de apoyo en el Sistema Integrado de Gestión, cuenta con el Sistema de Información, Telecomunicaciones y Tecnología SITT, cuyo fin es el de administrar y mantener la infraestructura tecnológica necesaria para el desarrollo de sus procesos de una manera eficaz, efectiva y oportuna, buscando siempre, la satisfacción de sus clientes. Su campo de acción, va "desde la identificación de las necesidades de actualización, modernización y mantenimiento, hasta el aseguramiento en la prestación del servicio de tecnología y telecomunicaciones"[31.]

Además de lo anterior, el SITT debe garantizar que la información que se administra, pueda cumplir con los requerimientos mínimos necesarios para dar el soporte a la toma de decisiones a nivel institucional y se pueda llevar a cabo el cumplimiento de su misión. Pero para lograr esto, se necesita el esfuerzo de todos y cada uno de los entes que componen la Universidad, en la implementación de herramientas que permitan la eficiencia y la mejora continua de sus procesos institucionales.

En aras de lograr este cometido, la seguridad de la información juega un papel predominante, ya que permite que se pueda garantizar la integridad, confidencialidad y disponibilidad de la información, así como minimizar el impacto que una situación irregular pueda provocar, garantizando la continuidad de sus procesos y el logro de sus objetivos.

La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesita establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos[32.]

[31] UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. División de Sistemas. Caracterización proceso Sistemas de Información, Telecomunicaciones y Tecnología. 6 de Noviembre de 2013.
[32] ISO/IEC 27002:2013. Tecnología de la información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información. Disponible en Internet: <http://www.iso27000.es/download/ControlesISO27002-2013.pdf>

Con el fin de realizar un análisis de la situación actual del proceso de adopción y gestión de la capacidad tecnológica de la Universidad, se llevó a cabo una auditoría de cumplimiento bajo el estándar ISO 27002:2013, incluyendo sus dieciocho (18) dominios, e involucrando los siguientes procesos: ***Sistema de Información, Telecomunicaciones y Tecnología, Gestión Humana, Gestión Administrativa y Financiera y Control Interno,*** por estar relacionadas con la gestión de la seguridad de la información:

Los dominios que se evaluaron se relacionan a continuación:

- *Políticas de Seguridad*
- *Aspectos organizativos de la seguridad de la información*
- *Seguridad ligada a los recursos humanos*
- *Gestión de activos*
- *Control de accesos*
- *Cifrado*
- *Seguridad física y ambiental*
- *Seguridad en la operativa*
- *Seguridad en las telecomunicaciones*
- *Adquisición, desarrollo y mantenimiento de los sistemas de información*
- *Relaciones con suministradores*
- *Gestión de incidentes en la seguridad de la información*
- *Aspectos de seguridad de la información en la gestión de la continuidad del negocio*
- *Cumplimiento*

El siguiente diagnóstico se obtuvo a partir de la realización de entrevistas aplicadas a los responsables de los procesos mencionados anteriormente, (ver Anexos), que arrojó los siguientes resultados, categorizados por dominios:

Dominio 5: Políticas de seguridad de la información

Existe un documento de Políticas de Seguridad de la Información (versión No. 2), aprobado por el Comité administrativo de la Universidad, que contiene los lineamientos para la protección y uso correcto de los activos de información.

La revisión de la Política de Seguridad está a cargo del responsable del proceso Sistemas de Información, Telecomunicaciones y Tecnología SITT, quien evalúa anualmente este documento y realiza las modificaciones necesarias.

Actualmente, dicha política no es del conocimiento de todos los miembros de la comunidad universitaria, puesto que no se ha publicado oficialmente, ni a través de la plataforma Web, ni por medios impresos. Cabe destacar que aunque no se han realizado capacitaciones formales, algunos aspectos de seguridad que se consideran relevantes, se vienen divulgando a través del correo institucional.

Dominio 6: Aspectos organizativos de la seguridad de la información

Actualmente la Universidad Francisco de Paula Santander Ocaña, no cuenta con un marco referencial para iniciar y controlar los procesos de implementación de la seguridad de la información dentro de la Institución. Existen procedimientos establecidos, aprobados, controlados e implementados, que permiten soportar algunas de las actividades relacionadas con la gestión de la seguridad de la información; sin embargo, no son suficientes para alcanzar el objetivo.
No existen responsabilidades claramente definidas para la protección de los activos individuales, ni se conocen procesos de seguridad específicos para cada uno de ellos. La responsabilidad de los activos, recae sobre el responsable del área.

De la misma manera, la Universidad, no cuenta con procedimientos formales para establecer contacto con autoridades relevantes para los casos en los que se presente un incidente de seguridad que pueda poner en riesgo la continuidad de las operaciones. Por su parte, la División de Sistemas se encuentra inscrita a un servicio de bases de datos de vulnerabilidades, a través de las cuales se reciben alertas de seguridad para evitar o corregir fallas en los sistemas de información o aplicaciones. Así mismo, se recibe asesoría de una empresa de seguridad contratada para tal fin y para realizar auditorías de penetración, que se llevan a cabo anualmente.

Dominio 7: Seguridad ligada a los recursos humanos

En la etapa de reclutamiento de personal, una vez se hace todo el proceso de convocar a nuevos empleos, se hace la recepción de las hojas de vida de los aspirantes y se realiza el estudio y revisión de los perfiles y competencias laborales solicitadas, así como el estudio de antecedentes.

Con respecto a la etapa de contratación del personal, se realizan los diligenciamientos de ley y el empleado firma el contrato. Cabe destacar que aunque el contrato no estipula una cláusula de confidencialidad específica, existe un ítem que se refiere a la reserva total de la información a la cual tendrá acceso. De igual forma, La Universidad, en cumplimiento de la Ley 734 de Febrero 05 de 2002 por la cual se expide el código disciplinario único, realiza las debidas sanciones o llamados de atención a los empleados que cometan alguna falta contra la institución o contra la información que se le ha asignado respectivamente. Estos procedimientos se llevan a cabo a través de la oficina de la División de Personal y la Dirección de la Institución.
Por su parte, los empleados no reciben capacitación específica en cuanto a procedimientos de seguridad de la información que tienen bajo su responsabilidad. Solo reciben a su correo institucional, tips de seguridad, enviados por el Administrador Web.

El contrato de trabajo tampoco contempla reglas claras para el uso aceptable de algunos activos como correo electrónico, dispositivos, datos, equipos, entre otros.

En el momento de terminación del contrato, existe un formato denominado FORMATO ENTREGA DEL PUESTO DE TRABAJO, que contiene las actividades necesarias para hacer entrega oficial de su puesto de trabajo y la conformidad de las distintas dependencias de la Universidad con las cuales se establece relación directa.

Dominio 8: Gestión de activos

La Universidad cuenta con un inventario de todos sus activos, debidamente clasificados y mantenidos. Todos los activos se encuentran etiquetados de tal manera que sean de fácil acceso. Los responsables de dichos activos son los jefes de área, que a su vez pueden delegar en otros empleados dichas responsabilidades.

Existen formatos para entrega de activos, así como reportes de baja de elementos. En relación con las licencias de software como activo de información, están bajo la responsabilidad y custodia del jefe de la División de Sistemas.

En cuanto al proceso de baja de equipos, el responsable del manejo de los inventarios, solicita al jefe de la División de Sistemas, un dictamen sobre el estado del equipo para proceder a retirarlo del lugar en el que se encuentra instalado.

Con respecto a los equipos de cómputo, una vez son retirados, se almacenan en bodega, sin aplicar ningún procedimiento específico de destrucción de la información contenida en ellos.

Finalmente, cabe destacar, que aunque el documento de Políticas de Seguridad de la Información (versión No. 2), contempla las reglas para el uso aceptable de algunos activos como correo electrónico, dispositivos, datos, equipos, entre otros, éstas no se han dado a conocer a la comunidad universitaria.

Dominio 9: Control de accesos

El documento de Políticas de Seguridad de la Información, contempla las reglas de control de acceso y los derechos para cada usuario o grupos de usuarios de los sistemas de información. Así mismo, establece la responsabilidad de los usuarios en el tratamiento de la información, actualización de hardware y software, uso del correo electrónico, almacenamiento y respaldo de los datos, uso adecuado de la red interna, entre otros.

Además de lo anterior, dentro del proceso de Sistemas de Información, Telecomunicaciones y Tecnología SITT del Sistema Integrado de Gestión, existen procedimientos documentados, aprobados, controlados e implementados, que detallan la manera como se deben llevar a cabo las actividades propias del procedimiento. Para el caso particular, existe uno, denominado ADMINISTRACIÓN DE RECURSOS INFORMÁTICOS, cuyo objeto es el de “definir las actividades que se realizan para garantizar el

uso eficiente de los recursos tecnológicos disponibles en la UFPSO, a través de actividades de monitoreo y supervisión de uso de equipos informáticos, de comunicación, de almacenamiento y demás infraestructura tecnológica activa"[33].

Dominio 10: Cifrado

Aunque existe un control para la asignación de privilegios de acceso a los sistemas de información, los mismos no se revisan periódicamente, ni existe procedimiento formal para realizarlo. El sistema automáticamente solicita cambio de contraseña de usuario cada seis (6) meses.

El proceso de gestión de claves de usuario se lleva a cabo por el administrador del sistema, quien autoriza o deniega los derechos de acceso a los diferentes servicios informáticos.

Dominio 11: Seguridad física y ambiental

En el ítem de Áreas Seguras, se pudo determinar que no existen medidas efectivas para controlar el acceso a las áreas críticas en la División de Sistemas (Sala de servidores). Este cuarto de servidores es un área muy reducida de la dependencia que sólo la protege una puerta con llave. Esta situación pone en riesgo la seguridad de los activos que se encuentran en el área y la integridad, confidencialidad y disponibilidad de la información que allí se maneja.

Así mismo, se encontró que las copias de respaldo que se hacen diariamente por una parte, quedan almacenadas en el mismo servidor y una copia se guarda en el servidor de backup interno. Este último, se encuentra también en el cuarto de servidores, presentándose la misma situación de ineficiencia en los controles de acceso. Por otra parte, las copias que se hacen en formato DVD, se guardan en una caja con llave, y esta caja queda también en el mismo cuarto de servidores.

[33] UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. División de Sistemas. Procedimiento administración de los recursos informáticos, 2015. Disponible en Internet: <https://ufpso.edu.co/ftp/pdf/procedimientos/sitt/R-TT-DSS-002D.pdf>

Cabe anotar que ni en el área de recepción, ni en el área administrativa de la División de Sistemas, existe cámara de vigilancia que pueda registrar los accesos a dicha dependencia. Sólo existe una cámara en el cuarto de servidores.

En cuanto al equipo de seguridad para la protección física de los activos, la Universidad cuenta con una subestación eléctrica que ha permitido regular las cargas de tensión, evitando la interrupción del servicio eléctrico y por ende, de las operaciones académicas y administrativas. Sin embargo, carece de un generador de emergencia (planta eléctrica) que permita darle continuidad a los servicios que ofrece la Universidad y por ende, evitar o reducir el riesgo de daño en los equipos de cómputo y la pérdida parcial o total de la información que allí se procesa, cuando el corte en el fluido eléctrico es prolongado.

Cabe destacar que la Universidad cuenta con pararrayos que ayuda a disminuir la posibilidad de daños en los equipos en los casos en los que se presenten descargas eléctricas.

De igual manera, la Universidad cuenta con extintores para casos de incendios. Sin embargo, aunque el personal de mantenimiento recibió adiestramiento en el manejo de los mismos en una oportunidad, este tipo de capacitaciones no se ha vuelto a realizar, teniendo en cuenta que una parte del personal del área ha sido cambiada. Así mismo, no existen alarmas contra incendios ni detectores de humo, que puedan poner en alerta al personal de la Universidad sobre la presencia de fuego.

Por otra parte, los equipos que manejan información sensible como los servidores y equipos principales de procesamiento, cuentan con un sistema de refrigeración adecuada (18^{o}C). Sin embargo, los niveles de humedad y la impermeabilidad en el cuarto de servidores no se controla a través de ningún mecanismo; situación que puede poner en riesgo la integridad de las copias de respaldo que se almacenan en este lugar.

Es importante resaltar, que a nivel de cableado, estas instalaciones se encuentran bien dotadas, utilizando las normas para cableado estructurado e independizando las conexiones eléctricas y de datos.

Dominio 12: Seguridad en la operativa

Actualmente el SITT cuenta con procedimientos documentados para diferentes actividades del sistema tales como ADMINISTRACIÓN DE RECURSOS INFORMÁTICOS, GESTIÓN DE LOS SISTEMAS DE TI, SOPORTE Y ATENCIÓN AL USUARIO, entre otros. Dichos procedimientos son controlados por la Oficina de Calidad que autoriza las modificaciones a los mismos a través del diligenciamiento de un formato de control de novedades. Dichas actualizaciones son comunicadas a través de la plataforma Web a toda la comunidad universitaria.
En el entorno de desarrollo de aplicaciones, las funciones propias de cada etapa (análisis, diseño, implementación, instalación, entre otras), no se encuentran segregadas. Solo existe un responsable de todo el proceso, que generalmente es realizado por pasantes o estudiantes de últimos semestres. Así mismo, la verificación del cumplimiento de cada una de las etapas anteriores, se realiza de manera interna, por el responsable del área, pero dicho procedimiento no se documenta.

En cuanto al proceso de respaldo de la información, cada servidor realiza de manera automática la copia de seguridad relacionada con el tipo de información que almacena (archivos de configuración, bases de datos, archivos de sistema, entre otros), y una vez terminado el proceso, esta información es enviada al servidor de backup interno. Posteriormente estos respaldos son almacenados en un Data Center externo contratado por la Universidad. Sin embargo, aunque se han ejecutado pruebas de restauración de los datos respaldados, éstas no se encuentran formalmente establecidas como procedimiento y por lo tanto, no se tiene registro de los resultados arrojados por el mismo.

Dominio 13: Seguridad en las telecomunicaciones

En cuanto a la seguridad de las redes de datos que soportan todos los procesos de la Universidad, se tiene instalado un firewall o cortafuegos en cada red, para impedir el tráfico no autorizado desde Internet hacia la red interna y entre los equipos de la misma red, con el fin de evitar accesos no autorizados para modificar o sustraer información confidencial.

La Política de Seguridad de la Información de la Universidad, contempla entre otros aspectos, las reglas de acceso a los servicios de red para los cuales han sido específicamente autorizados los usuarios. De igual forma, reglas para *Uso de la red interna e Internet*, *Control de conexión a las redes, Seguridad en comunicaciones, Acceso lógico,* entre otros.

De igual forma, se utiliza información de *Usuario* y *Contraseña*, como medida de protección para compartir recursos o información, a través de la red de datos.

Dominio 14: Adquisición, desarrollo y mantenimiento de los sistemas de información

En el entorno de desarrollo aplicaciones, actualmente no existen tareas por cada etapa del proceso (análisis, diseño, implementación, instalación, entre otras) que se encuentren segregadas ni asignadas a diferentes usuarios. Quien diseña, codifica, implementa, instala, capacita, configura, etc.

A pesar que existe un procedimiento de gestión de los sistemas de información, cuyo fin es el de "solucionar las necesidades a nivel de desarrollo y actualización de software para cumplir con los requerimientos y dar soporte funcional para el mejoramiento continuo de los procesos"[34], las actividades de cada etapa del proceso de desarrollo de aplicaciones, no se documenta.

En lo relacionado con la realización de pruebas de los requerimientos operacionales de los nuevos sistemas (o actualizaciones) antes de su aceptación y uso, no existe un documento formal que establezca tal procedimiento. Solo se realizan pruebas internas.

En cuanto al proceso de adquisición de tecnología de hardware y/o software, se realizan proyecciones de los requerimientos en la ampliación de la capacidad tecnológica de acuerdo con lo establecido en el plan de acción de la División de Sistemas y evaluado por la Subdirección Administrativa que realiza el estudio de la necesidad.

Dominio 15: Relaciones con suministradores

[34] UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. División de Sistemas. Procedimiento gestión de los sistemas de TI, 2010. Disponible en Internet: <https://ufpso.edu.co/ftp/pdf/procedimientos/sitt/R-TT-DSS-003A.pdf>

Cuando se establecen acuerdos con terceros (contratistas, proveedores, entre otros), la verificación del cumplimiento de los servicios ofrecidos por éstos, es llevada a cabo por un *supervisor del servicio*, que pertenece a la Universidad.
Con respecto a las condiciones de protección y confidencialidad de la información que se intercambia con terceros, se establecen acuerdos de no divulgación para garantizar el uso adecuado y necesario de los datos. Sin embargo, no existen procedimientos formales para administrar los cambios en los servicios ofrecidos por los mismos.

Dominio 16: Gestión de incidentes en la seguridad de la información

La Universidad Francisco de Paula Santander Ocaña, no cuenta con procedimientos formales de reporte de eventos o debilidades que puedan tener un impacto en la seguridad de los activos institucionales. Para los casos en los que se presentan fallas en los sistemas o que se detecte la presencia de alguna vulnerabilidad, existe un formato de bitácoras, que permite hacer el registro de las respectivas anomalías y es de manejo interno de la División de Sistemas.

A pesar de que se han presentado algunos casos de fallas en el sistema por ataques externos, el tratamiento que se le ha dado a estas situaciones, tampoco se encuentra documentado y, por lo tanto, no existe un procedimiento aprobado para el manejo efectivo de tales eventos una vez han sido reportados. Tampoco existe procedimiento alguno, para el monitoreo o revisión periódica de la bitácora de los sistemas; solo se lleva a cabo, cuando se presentan errores.

En cuanto a las evidencias de los eventos de seguridad, se hace revisión de los logs o archivos utilizados para registrar datos sobre quién, qué, cuándo, dónde y por qué ocurrió el evento para el caso particular de los administradores de los distintos sistemas de información. Para los usuarios de las aplicaciones, se encuentra habilitada en el motor de bases de datos, una función de auditoría interna, que permite registrar las actividades realizadas por los mismos.

Dominio 17: Aspectos de seguridad de la información en la gestión de la continuidad del negocio

En la actualidad, la Universidad Francisco de Paula Santander Ocaña, no cuenta con un Plan de Continuidad del Negocio (PCN), que contemple las actividades necesarias para minimizar el impacto sobre la Institución y recuperarse de la pérdida de activos de información hasta un nivel aceptable.

Por su parte, existe un Plan de Contingencia (versión No. 1), elaborado con el fin de orientar los procedimientos relevantes con relación a protocolos y políticas de seguridad, backup, lineamientos para el desarrollo y actualización de los sistemas de información que son vitales para orientar las acciones ante una contingencia a la infraestructura informática en la Universidad Francisco de Paula Santander Ocaña. Se entenderá como infraestructura informática al hardware, software y elementos complementarios que soportan la información o datos críticos para la función de los procesos misionales y de apoyo[35].

Dominio 18: Cumplimiento

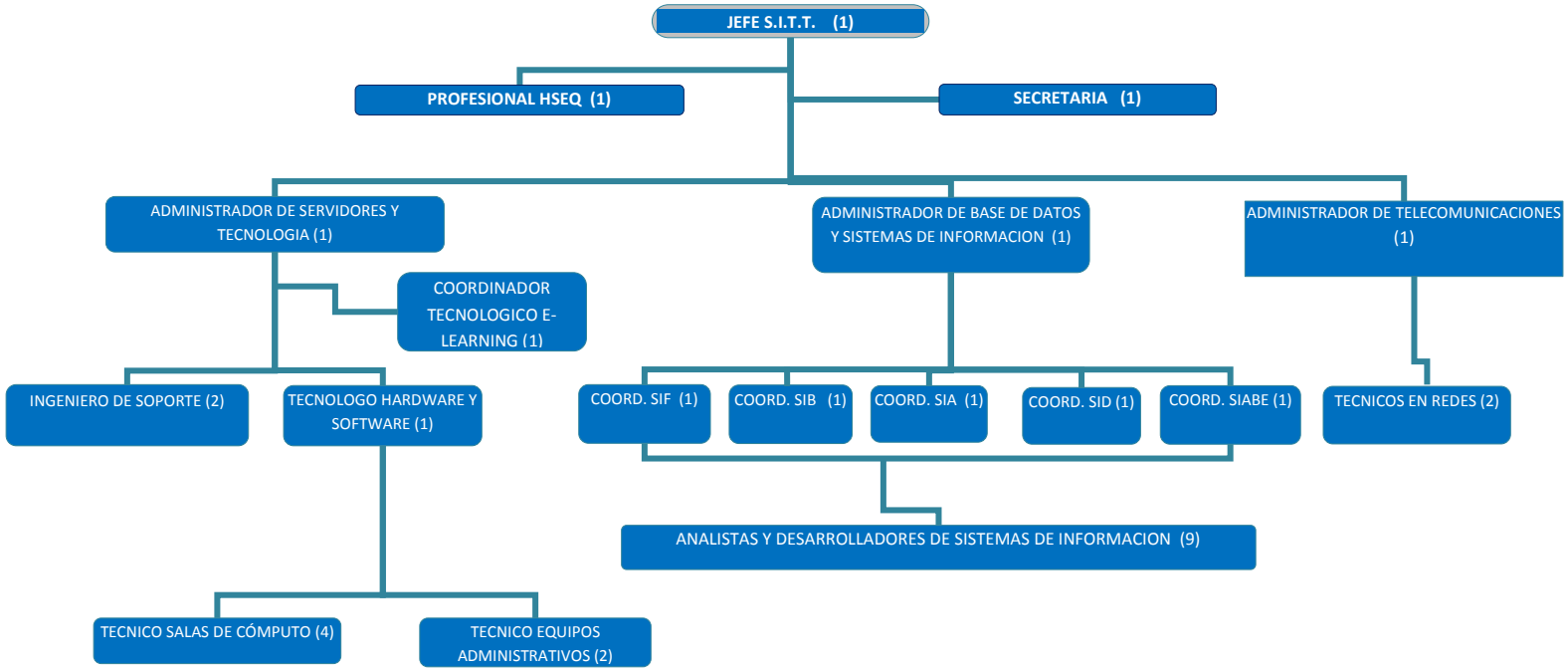
Existe un documento denominado **Política de Seguridad de la Información** (versión No. 2), que contempla las sanciones pertinentes y necesarias de aplicar en los casos en los que se incurra en algún delito informático de los que trata la Ley 1273 de 2009.

3.3.2 Organización de las TI en la Universidad Francisco de Paula Santander Ocaña. En el mapa de procesos de acuerdo como lo establece el Sistema Integrado de Gestión, la organización de las TI se encuentra como un proceso denominado **SISTEMAS DE INFORMACION, TELECOMUNICACIONES Y TECNOLOGIA**. De acuerdo con ello, su función es diseñar, administrar y mantener los sistemas de información, las telecomunicaciones y la infraestructura tecnológica utilizados para el desarrollo de

[35] UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. División de Sistemas. Plan de Contingencia de TI versión 1.0, 2010. Disponible en Internet: <https://ufpso.edu.co/ftp/doc/otrospro/sitt/L-TT-DSS-002A.pdf>

los procesos de la Universidad de manera eficaz, efectiva y oportuna[36]. De acuerdo con información proporcionada por el Jefe de la División de Sistemas, la siguiente es la estructura organizacional del área de TI:

Figura 5. Estructura orgánica de la División de Sistemas



Fuente: UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. División de Sistemas, 2015.

[36] UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. Caracterización proceso sistemas de información, telecomunicaciones y tecnología, 2013. Disponible en Internet: <https://ufpso.edu.co/ftp/pdf/caracterizacion/sitt/Z-TT-DSS-001E1.pdf>

Del anterior esquema, se puede inferir en términos de organización, lo siguiente:

- El área de TI (División de Sistemas), no cuenta con una sección o subdivisión que se encargue de desarrollar políticas internas tanto de calidad como de seguridad de información, así como de formular los estándares y metodologías para las diferentes actividades que se llevan a cabo; por ejemplo: gestión de proyectos, desarrollo de software, estándares de documentación, estándares de infraestructura tecnológica, entre otros.

- No se evidencia la existencia de un área que se encargue del monitoreo, evaluación y control de la gestión interna y del resultado de los proyectos de TI.

- No existe un Comité Directivo de TI que se encargue de determinar las prioridades de los programas o proyectos de inversión tecnológica, acorde con las necesidades de la institución.

Actualmente, esta estructura organizacional no se encuentra formalmente aprobada; por lo tanto, las actividades del área de TI, se ajustan sólo, a las necesidades y exigencias de los servicios informáticos que surgen.

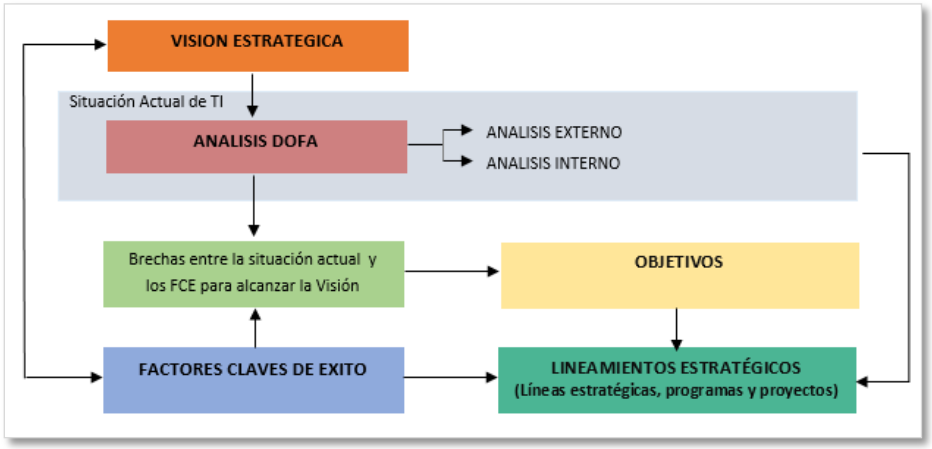
4. ETAPA TRES: DEFINICION DE COMPONENTES ESTRATEGICOS DE LAS TI EN LA UFPSO

La definición de los componentes estratégicos de las TI para la Universidad Francisco de Paula Santander Ocaña, se divide en 5:

- **Componente 1 - Visión Estratégica de las TI**
- **Componente 2 - Matriz DOFA**
- **Componente 3 - FCE – Factores Clave de Éxito de TI**
- **Componente 4 - Objetivos Estratégicos**
- **Componente 5 - Lineamientos Estratégicos**
- **Componente 6 – Alineación Plan Estratégico Institucional y Plan Estratégico de TI**

A continuación se muestra un gráfico que muestra el panorama completo de la definición estratégica de TI para la UFPSO.

Figura 6. Definición estratégica de las Tecnologías de Información para la UFPSO



Fuente: ARRIETA SANCHEZ, María A., et al.

4.1 Componente 1: Visión estratégica de las TI para la Universidad Francisco de Paula Santander

De manera consensuada con el Jefe de la División de Sistemas, se decidió formular la siguiente visión estratégica para el área de TI de la Universidad:

Para el año 2019, la Universidad Francisco de Paula Santander Ocaña habrá integrado y apropiado las Tecnologías de la Información y la Comunicación TIC en sus procesos estratégicos, misionales y de apoyo, con miras a la excelencia institucional.

4.2 Componente 2: Matriz DOFA

A partir de la información recolectada y como producto de la auditoría de cumplimiento bajo el estándar ISO/IEC 27002:2013, se formula la siguiente matriz DOFA:

Cuadro 3. Matriz DOFA

DEBILIDADES	OPORTUNIDADES
1. Inexistencia de un Comité de TI que determine las iniciativas de inversión en tecnología y priorice los proyectos de desarrollo a nivel de hardware y software. 2. Falta de socialización de las políticas de seguridad de la información a todos los estamentos de la Universidad. 3. Inexistencia de estándares para documentar los procedimientos de las diversas actividades que se llevan a cabo por parte del área de TI. 4. Inexistencia de un manual de funciones del área de TI con sus respectivos perfiles establecidos y aprobados.	1. Apertura al trabajo colaborativo con otras entidades para participar conjuntamente en iniciativas de TI. 2. Desarrollo de nuevas tecnologías en el mercado; tendencias tecnológicas y buenas prácticas de gestión. 3. Apertura para el intercambio de conocimiento y experiencias con otras instituciones similares a nivel nacional e internacional. 4. Alineación de la estrategia de Gobierno en Línea con los procesos administrativos de la Universidad. 5. Certificación internacional en gestión de la seguridad de la información.
AMENAZAS	**FORTALEZAS**
1. Insatisfacción por parte de terceros con los que se establecen contratos, por incumplimiento de los acuerdos de niveles de servicio SLA's.	1. Competencias técnicas del personal administrativo de la Universidad en el uso de nuevas tecnologías de la información y las comunicaciones.

2. Instituciones de Educación Superior a nivel regional certificadas en gestión de la seguridad de la información. 3. Aumento del ciberterrorismo.	2. Segregación de funciones a nivel de servicios de TI. 3. Infraestructura tecnológica actualizada y en continuo mejoramiento. 4. Capacidad del área de TI para gestionar las necesidades de infraestructura tecnológica con la alta Dirección. 5. Personal de la División de Sistemas con capacidad técnica y experiencia profesional.
Fuente: ARRIETA SANCHEZ, María A., et al.	

4.3 Componente 3: Factores clave de éxito a nivel tecnológico según COBIT 4.1

Se han identificado cinco Factores Claves de Éxito FCE, a partir del estándar COBIT 4.1, para que la Universidad Francisco de Paula Santander Ocaña, en manos de la División de Sistemas, logre alcanzar su Visión Estratégica:

Cuadro 4. Factores Clave de Éxito para el área de TI

FCE – FACTOR CLAVE DE EXITO		DESCRIPCION
FCE 01	**Desarrollar el rol administrador de TI de la División de Sistemas**	Este FCE tiene como propósito, desarrollar un rol normativo de TI en la División de Sistemas de la UFPSO; de acuerdo con ello, se deben establecer estructuras organizacionales de TI transparentes, flexibles y responsables hacia los procesos de negocio y de decisión; ello incluye la definición de políticas de TI, planificación estratégica de TI y el control para asegurar el cumplimiento de las normas a nivel tecnológico por parte de los funcionarios informáticos asignados en la Universidad. El aspecto normativo de las TI es un componente clave de la gestión informática, a efectos de que la UFPSO no corra el riesgo de perder el control a

		nivel de estándares tecnológicos y de gestión de las TI.
FCE 02	**Contar con un modelo de planeación tecnológica que permita integrarse a la estrategia institucional**	Su objetivo fundamental es crear y hacer uso de una herramienta de gestión de TI que se alinee a los requerimientos y necesidades de las distintas dependencias de la UFPSO. La implementación de un PETI contribuirá a fortalecer los objetivos estratégicos de la UFPSO (metas), así como la transparencia sobre los beneficios, costos y riesgos relacionados, incluyendo cómo TI dará soporte a los programas de inversión y a la entrega de los servicios operativos.
FCE 03	**Crear un modelo de gestión de TI consistente con los objetivos estratégicos de la UFPSO, basado en la aplicación de buenas prácticas internacionales.**	Este FCE tiene como fin, diseñar e implementar procesos de gestión de TI que aseguren la provisión de servicios tecnológicos de calidad, y que incorporen buenas prácticas de gestión probadas y comprobadas a nivel internacional. Respecto a la UFPSO, se requiere formalizar la estructura orgánica del área de TI, con perfiles, funciones, y responsabilidades del personal para desarrollar las estrategias definidas y orientadas al cumplimiento de los objetivos tecnológicos. Respecto a los procesos de gestión, se requiere incorporar modelos o normas, que permitan disminuir los riesgos de una mala administración de TI, como los que define COBIT, ITIL, ISO, entre otros.
FCE 04	**Disponer de una plataforma tecnológica integrada a nivel de aplicaciones, bases de datos, infraestructura y comunicaciones.**	Este FCE se refiere a la implementación de soluciones tecnológicas integradas, que satisfagan las necesidades internas de la comunidad universitaria, agilizando la respuesta a los requerimientos, proporcionando información confiable y consistente, para integrar de forma transparente las aplicaciones dentro de los procesos institucionales. Se considera también que la plataforma tecnológica sea homogénea, estandarizada y flexible, con capacidad de evolución para dar soporte al crecimiento continuo de las necesidades institucionales incorporando innovación, interoperabilidad u otros aplicativos orientados ofrecer servicios de

		manera más eficiente.
FCE 05	**Gestionar eficientemente los servicios de TI**	Su propósito es crear un portafolio de servicios TI hacia afuera de la institución; servicios acorde con las necesidades y demandas de la UFPSO, facilitando la realización de trámites, búsqueda de información, pago de matrículas, cancelaciones de materias, entre otros utilizando las tecnologías de información. Tanto en éste como en el anterior FCE, se requiere por parte de la Dirección de la UFPSO y de la División de Sistemas, la exigencia oportuna a los proveedores externos que proporcionan los servicios de TI al interior de la institución educativa.
Fuente: ARRIETA SANCHEZ, María A., et al.		

4.4 Componente 4: Objetivos estratégicos

A continuación se muestran los objetivos estratégicos de TI derivados de la matriz de contrastación de los Factores Clave de Éxito FCE con la situación actual (DOFA). Los objetivos se orientan a cubrir las brechas para lograr los FCE, y por consiguiente alcanzar la visión estratégica. La matriz de contrastación, da como origen los controles de COBIT 4.1 que serán implementados y materializados en programas y proyectos concretos:

Cuadro 5. Matriz de contrastación DOFA – Factores Claves de Éxito

FACTOR CLAVE DE ÉXITO	ELEMENTOS DOFA	DOMINIO SEGÚN COBIT 4.1	CONTROL COBIT 4.1
FCE01	**D1 - O1 - F4**	**PLANEAR Y ORGANIZAR**	PO4.3 Establecer un Comité Directivo de TI
			PO6.3 y PO6.4 Elaborar, implantar y comunicar un conjunto de políticas que apoyen la estrategia de TI
			PO9.1 Establecer un marco de trabajo de administración de riesgos de TI PO9.6 Priorizar y planear las actividades de control a todos los niveles para implementar la respuesta a los riesgos
			PO4.15 Establecer y mantener una estructura óptima de enlace, comunicación y coordinación entre la función de TI y otros interesados
			PO8.3 Adoptar y mantener estándares para todo desarrollo y adquisición de tecnología
FCE02	**O5**	**PLANEAR Y ORGANIZAR**	PO1.4 Crear un Plan Estratégico que defina cómo TI contribuirá a los objetivos estratégicos de la empresa
FCE03	**D4 – F5**	**PLANEAR Y ORGANIZAR**	PO8.2 Identificar y mantener estándares, procedimientos y prácticas para los procesos claves de TI
		ENTREGAR Y DAR SOPORTE	DS4.1 Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio
		PLANEAR Y ORGANIZAR	PO4.5 Establecer una estructura organizacional de TI interna y externa que refleje las necesidades del negocio

			PO4.6 Definir y comunicar los roles y las responsabilidades para el personal de TI
			PO4.7 Asignar la responsabilidad para el desempeño de la función de aseguramiento de calidad
FCE04	**O3 – F3**	**ENTREGAR Y DAR SOPORTE**	DS12.2 Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio
			DS4.9 Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos
			DS3.1 Establecer un proceso de planeación para la revisión del desempeño y la capacidad de los recursos de TI
			DS3.4 Brindar la capacidad y desempeño requeridos tomando en cuenta aspectos como cargas de trabajo normales, contingencias, requerimientos de almacenamiento, entre otros
		ADQUIRIR E IMPLEMENTAR	AI7.5 Implementar un plan de conversión de datos y migración de infraestructuras como parte de los métodos de desarrollo de la organización
			AI4.3 Transferir conocimientos y habilidades para permitir que los usuarios finales utilicen con efectividad y eficiencia los sistemas de aplicación
FCE04	**A2 – O5**	**PLANEAR Y ORGANIZAR**	PO4.8 Establecer la responsabilidad de los riesgos relacionados con TI a un nivel superior apropiado, incluyendo la responsabilidad específica de la seguridad de la información, la seguridad física y el cumplimiento.
		ADQUIRIR E IMPLEMENTAR	AI2.4 Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados.

FCE05	**A1 – F1**	**ENTREGAR Y DAR SOPORTE**	DS1.1 Definir un marco de trabajo que brinde un proceso formal de administración de niveles de servicio
			DS1.3 Definir y acordar convenios de niveles de servicio para todos los procesos críticos de TI
			DS2.2 Formalizar el proceso de gestión de relaciones con proveedores
Fuente: ARRIETA SANCHEZ, María A., et al.			

4.5 Componente 5: Lineamientos del Plan Estratégico de Tecnologías de la Información

El Plan Estratégico de Tecnologías de la Información PETI 2016 – 2018 para la Universidad Francisco de Paula Santander Ocaña, se ha formulado, con base en los controles que propone COBIT 4.1 y que se relacionaron en la anterior tabla. Dichos controles se asocian a las actividades contempladas en el Plan de Desarrollo Institucional y a los diferentes Planes de Acción para el año 2015. Dicho plan se estructura con base en programas asociados a cada una de las líneas estratégicas que deben ser desarrolladas durante su implementación. A su vez, los programas se materializan en proyectos que deben ejecutarse a través de diferentes actividades.

En cada uno de los Proyectos, se define el (los) responsable(s) de los mismos, así como el tiempo durante el cual se desarrollará. Para cada una de los doce (12) programas que componen el PETI, existe una numeración secuencial, así como los proyectos asociados. Esta numeración tiene por objetivo relacionar los proyectos de Tecnologías de Información con las actividades estratégicas del Plan de Desarrollo Institucional 2014-2019.

Cuadro 6. Estructura Plan Estratégico de Tecnologías de la Información UFPSO

LÍNEA ESTRATÉGICA	**P1**	**PROGRAMA**	**PR1**	**PROYECTO**
			PR2	**PROYECTO**
	P2	**PROGRAMA**	**PR3**	**PROYECTO**
			PR4	**PROYECTO**

Fuente: ARRIETA SANCHEZ, María A., et al.

LÍNEA ESTRATÉGICA	PROGRAMA		PROYECTO		RESPONSABLE	2016	2017	2018
Establecer las bases institucionales para el uso y soporte de las TI Se busca generar una visión estratégica, en donde la Dirección de TI sea considerada un referente en la introducción y uso de las tecnologías en la Universidad Francisco de Paula Santander Ocaña. Para cumplir con este cometido, será necesario desarrollar las políticas que normen el uso, la adquisición y la seguridad de las TI en la Institución.	**1**	**Ser el referente y responsable en la UFPSO para la introducción y uso de TI a nivel institucional.**	**1.1**	Creación y aprobación del Comité Directivo de TI.	Jefe División de Sistemas			
			1.2	Establecimiento de la estructura orgánica de la Dirección de TI.	Director UFPSO			
			1.3	Definición de roles y responsabilidades.	Jefe División de Sistemas			
	2	**Contar con un marco regulatorio que garantice el crecimiento estandarizado y el uso eficiente de los recursos de TI.**	**2.1**	Implementación del Plan Estratégico de Tecnologías de la Información PETI.	Jefe División de Sistemas			
			2.2	Actualización y socialización de las políticas de seguridad de la Información.	Jefe División de Sistemas			
			2.3	Creación e implementación de una política estandarizada de adquisición de tecnología.	Jefe División de Sistemas			
			2.4	Diseño, aprobación y socialización del manual de políticas de tratamiento de datos personales.	Jefe División de Sistemas			
			2.5	Implementación de buenas prácticas de TI basadas en ISO 27002:2013.	Jefe División de Sistemas			
			2.6	Construcción del Plan de Continuidad del Negocio.	Jefe División de Sistemas			
	3	**Disponer de redes de apoyo para la incorporación, aplicación y soporte de TI.**	**3.1**	Establecimiento de convenios con grupos de interés para asesorías y servicios de seguridad informática.	Jefe División de Sistemas			

LÍNEA ESTRATÉGICA	PROGRAMA		PROYECTO		RESPONSABLE	2016	2017	2018
Impulsar el mejoramiento de los procesos administrativos, académico-administrativo y de gestión a través del fortalecimiento de las Tecnologías de Información Se busca mejorar la eficiencia en los procesos administrativos y de gestión de la Universidad, a través de la incorporación de nuevas tecnologías de la información y la comunicación.	**4**	**Apoyar la fidelización y seguimiento de egresados.**	**4.1**	Proyecto seguimiento a egresados	Jefe División de Sistemas – Jefe Bienestar Universitario			
	5	**Modernizar los procesos administrativos para incrementar su eficiencia y la satisfacción de clientes internos y externos.**	**5.1**	Sistema de Información para la consulta de normas a nivel interno y externo	Jefe División de Sistemas – Secretario General			
			5.2	Apoyo al proceso de liquidación para estudiantes antiguos	Jefe División de Sistemas – Jefe Admisiones, Registro y Control			
			5.3	Gobierno en Línea	Jefe División de Sistemas – Jefe Planeación			
			5.4	Sistema de Información para Bienestar Universitario	Jefe División de Sistemas – Jefe Bienestar Universitario			
			5.5	Desarrollo portal Web para la escuela de Bellas Artes	Jefe División de Sistemas – Escuela Bellas Artes			
			5.6	Sistema de Autenticación Único	Jefe División de Sistemas			

LÍNEA ESTRATÉGICA		PROGRAMA		PROYECTO	RESPONSABLE	2016	2017	2018
Incorporar las Tecnologías de la Información a los procesos académicos de la Universidad Se busca mejorar el proceso educativo mediante el uso e integración de las Tecnologías de la Información, como apoyo a las prácticas pedagógicas de los docentes y a los procesos de aprendizaje de los estudiantes.	**6**	**Mejorar el nivel de uso y apropiación de las TI en el proceso educativo**	**6.1**	Capacitación docente en TI	Jefe División de Sistemas – Planes de Estudio			
			6.2	Implementación Sistema de Información Bibliográfico Web	Jefe División de Sistemas – Jefe Biblioteca			
			6.3	Capacitación a docentes y estudiantes en el uso de recursos bibliográficos digitales	Jefe División de Sistemas – Jefe Biblioteca			
	7	**Disponer de la tecnología adecuada para la adopción de la modalidad virtual y de apoyo a la presencialidad**	**7.1**	Unidad Virtual	Jefe División de Sistemas – U Virtual			
			7.2	Implementación mesa de ayuda	Jefe División de Sistemas			
			7.3	Implementación de cuatro nuevas salas de cómputo	Jefe División de Sistemas			
			7.4	Implementación de eduroam en las sedes Algodonal, Bellas Artes e Invías	Jefe División de Sistemas			

LÍNEA ESTRATÉGICA		PROGRAMA		PROYECTO	RESPONSABLE	2016	2017	2018
Proveer una infraestructura de TI estable, confiable y segura, que mejore la productividad en los servicios que ofrece la Universidad Su objetivo es diseñar e implementar iniciativas que permitan disponer de una infraestructura de TI que soporte el crecimiento estandarizado de la Universidad a corto y mediano plazo.	**8**	**Mantener una plataforma tecnológica actualizada para asegurar la disponibilidad y continuidad de los servicios institucionales**	**8.1**	Migración de los sistemas de información de la Intranet de la Universidad de la versión 6i a 10G	Jefe División de Sistemas			
			8.2	Mantenimiento preventivo de los portales de los sistemas de información vía Web	Jefe División de Sistemas			
	9	**Diseñar e implementar el plan de adquisición tecnológica**	**9.1**	Creación del Data Center	Jefe División de Sistemas			
			9.2	Actualización del cableado estructurado de las sedes de la Universidad	Jefe División de Sistemas			
			9.3	Ampliación de 50 puntos IP más, en la cobertura del servicio de voz IP	Jefe División de Sistemas			
			9.4	Vinculación de la Universidad al proyecto Voz IP de la red RENATA	Jefe División de Sistemas			
			9.5	Actualización del servicio para la consola del Antivirus	Jefe División de Sistemas			
			9.6	Implementación red de área de almacenamiento SAN	Jefe División de Sistemas			
			9.7	Implementación enlaces inalámbricos de respaldo	Jefe División de Sistemas			
			9.8	Implantación de dispositivos para el control de acceso al área de servidores	Jefe División de Sistemas			
			9.9	Adquisición planta de emergencia para la subestación eléctrica	Jefe División de Sistemas			

LÍNEA ESTRATÉGICA	PROGRAMA		PROYECTO		RESPONSABLE	2016	2017	2018
Impulsar una cultura de la excelencia en la entrega de servicios, a través del fortalecimiento de las competencias del personal de TI Se busca desarrollar actividades que permitan al personal de TI, mejorar sus competencias profesionales de acuerdo con su perfil laboral y las responsabilidades que le han sido encomendadas	**10**	**Implementar una estructura organizacional para la División de Sistemas, que permita satisfacer los requerimientos institucionales**	**10.1**	Levantamiento estructura organizacional actual	Jefe División de Sistemas			
			10.2	Nueva estructura organizacional	Jefe División de Sistemas			
	11	**Mejorar las capacidades técnicas del personal de la División de Sistemas**	**11.1**	Levantamiento del perfil profesional del personal de TI	Jefe División de Sistemas			
			11.2	Plan de capacitación del personal acorde con su perfil profesional y laboral	Jefe División de Sistemas			
	12	**Fortalecer el desempeño de los servicios entregados a clientes internos y externos**	**12.1**	Revisión de las nuevas tendencias en TI para las instituciones de educación superior	Jefe División de Sistemas			

4.6 Componente 6: Plan Estratégico Institucional y Plan Estratégico de Tecnologías de la Información

El Plan Estratégico Institucional "Hacia la excelencia institucional 2014 - 2019", se ha estructurado con base en seis (6) ejes estratégicos, distribuidos en actividades y metas necesarias para su cumplimiento. Por su parte, el Plan Estratégico de Tecnologías de la Información se estructura con base en programas asociados a cada una de las líneas estratégicas definidas anteriormente; estos a su vez, se materializan en proyectos que deben ejecutarse a través de diferentes actividades. La alineación entre el Plan Estratégico Institucional y el de Tecnologías de la Información, se realiza a nivel de programas y proyectos con las actividades del Plan Estratégico Institucional. Para cada uno de los programas de tecnologías de la información que tienen relación con el Plan Estratégico Institucional, se referencia el número con el cual se ha declarado anteriormente.

Cuadro 6. Estructura alineación Plan Estratégico Institucional y Plan Estratégico de Tecnologías de la Información UFPSO

PLAN ESTRATÉGICO INSTITUCIONAL			PLAN ESTRATÉGICO DE TI			
EJE ESTRATÉGICO	ACTIVIDAD ESTRATÉGICA	META	P1	PROGRAMA	PR1	PROYECTO
					PR5	PROYECTO
	ACTIVIDAD ESTRATÉGICA	META	P2	PROGRAMA	PR4	PROYECTO
					PR8	PROYECTO

Fuente: ARRIETA SANCHEZ, María A., et al.

PLAN ESTRATEGICO INSTITUCIONAL			PLAN ESTRATEGICO DE TI			
EJE ESTRATEGICO	**ACTIVIDAD ESTRATEGICA**	**META**	**PROGRAMA**		**PROYECTO**	
Investigación y formación académica	Implementación de las TI en los procesos académicos	Implementar en los currículos el uso y aprovechamiento de las TI.	**6**	Mejorar el nivel de uso y apropiación de las TI en el proceso educativo	**6.1**	Capacitación docente en TI
	Implementación y desarrollo de la UVirtual	Implementar programas de pregrado y posgrado y continuada en la modalidad virtual.	**7**	Disponer de la tecnología adecuada para la adopción de la modalidad virtual y de apoyo a la presencialidad	**7.1**	Unidad Virtual
	Fomento de la cultura en el uso de la virtualidad y TI en los programas presenciales	Apropiación del uso de la plataforma Moodle como componente virtual de cada cátedra.	**7**	Disponer de la tecnología adecuada para la adopción de la modalidad virtual y de apoyo a la presencialidad	**7.1**	Unidad Virtual
Desarrollo físico y tecnológico	Establecimiento de políticas que garanticen la confiabilidad y seguridad de la información institucional	Aprobación de políticas de confiabilidad y seguridad de la información.	**2**	Contar con un marco regulatorio que garantice el crecimiento estandarizado y el uso eficiente de los recursos de TI.	**2.2**	Actualización y socialización de las políticas de seguridad de la Información.
	Integración de los sistemas de información institucional	Sistemas de información integrados administrativamente	**8**	Mantener una plataforma tecnológica actualizada que asegure la disponibilidad y continuidad de los servicios institucionales.	**8.1**	Migración de los sistemas de información de la Intranet de la Universidad de la versión 6i a 10G
	Ejecución del plan de adquisición y modernización de equipos, redes y telecomunicaciones	Plan de adquisición y modernización de equipos, redes y telecomunicaciones ejecutado en su totalidad	**9**	Diseñar e implementar el plan de adquisición tecnológica	**9.1**	Creación del Data Center

Desarrollo físico y tecnológico	Ejecución del plan de adquisición de equipos, redes y telecomunicaciones	Ejecución del plan de adquisición de equipos, redes y telecomunicaciones	**9**	Diseñar e implementar el plan de adquisición tecnológica	**9.2**	Actualización del cableado estructurado de las sedes de la Universidad
					9.3	Ampliación de 50 puntos IP más, en la cobertura del servicio de voz IP
					9.4	Vinculación de la Universidad al proyecto Voz IP de la red RENATA
					9.6	Implementación red de área de almacenamiento SAN
					9.7	Implementación enlaces inalámbricos de respaldo
					9.8	Implantación de dispositivos para el control de acceso al área de servidores
					9.9	Adquisición planta de emergencia para la subestación eléctrica
Impacto y proyección social	Fortalecimiento de los mecanismos de comunicación e información entre los egresados y la Universidad	Actualizar en una 100% la base de datos del consultorio laboral	**4**	Apoyar la fidelización y seguimiento de egresados.	**4.1**	Proyecto seguimiento a egresados
	Desarrollo del arte con uso de las nuevas tecnologías	Inclusión en los contenidos programáticos de las asignaturas de artes, el uso de TI	**5**	Modernizar los procesos administrativos para incrementar su eficiencia y la satisfacción de clientes internos y externos.	**5.5**	Desarrollo portal Web para la escuela de Bellas Artes

Impacto y proyección social	Desarrollo del arte con uso de las nuevas tecnologías	Realizar jornadas de capacitación en el uso y apropiación de TI a docentes y administrativos	**6**	Mejorar el nivel de uso y apropiación de las TI en el proceso educativo	**6.1**	Capacitación docente en TI
Sostenibilidad administrativa y financiera	Modernización de los medios y mecanismos de comunicación	Implementación del sistema actualizado para la consulta de la normatividad	**5**	Modernizar los procesos administrativos para incrementar su eficiencia y la satisfacción de clientes internos y externos.	**5.1**	Sistema de Información para la consulta de normas a nivel interno y externo
	Estructuración de un sistema de consulta para la normatividad interna y externa requerida para el desarrollo de los procesos de la Universidad	Implementación de nuevos mecanismos tecnológicos de información			**5.5**	Desarrollo portal Web para la escuela de Bellas Artes
	Implementación de la estrategia de Gobierno en Línea	Cumplir con el manual y los avances de Gobierno en Línea en un 100%			**5.3**	Gobierno en Línea

5. CONCLUSIONES

Una vez desarrollada la propuesta de investigación, se pudo constatar que:

- Se elaboró el diagnóstico situacional, el cual permitió determinar la situación actual del proceso de adopción e implementación de las tecnologías de información en la Universidad Francisco de Paula Santander Ocaña.

- Se identificó la metodología más apropiada para el diseño del Plan Estratégico de Tecnologías de Información PETI para la Universidad Francisco de Paula Santander Ocaña.

- Se elaboró el documento que estructura el Plan Estratégico de Tecnologías de Información PETI para la Universidad Francisco de Paula Santander Ocaña.

Además, los datos obtenidos en la investigación sobre la gestión de los recursos tecnológicos de la Universidad Francisco de Paula Santander Ocaña, permitieron dimensionar el estado actual de dicha gestión y estructurar a partir del mismo, una alternativa para mediar en la búsqueda de soluciones para dicha situación.

La situación relacionada con la gestión de los recursos tecnológicos de la Universidad Francisco de Paula Santander Ocaña, no se ve a nivel institucional como un hecho aislado, sino como un problema que requiere atención prioritaria, pues afecta los índices de calidad institucionales.

El Plan Estratégico de Tecnologías de la Información propuesto, se estructuró de forma tal que todas las iniciativas de TI, puedan soportar las actividades académicas y administrativas de la Universidad y se alineen a ellas para el logro de su misión institucional.

6. RECOMENDACIONES

Para que el Plan Estratégico de Tecnologías de la Información propuesto sea realmente útil al proceso de consolidación y búsqueda de la excelencia institucional, la Dirección de la Universidad Francisco de Paula Santander Ocaña, debe incorporar el componente tecnológico como un aspecto clave para el logro de sus objetivos estratégicos, orientados a fortalecer los procesos académicos y administrativos, mejorar la imagen institucional a través de la prestación de servicios eficientes y oportunos y garantizar la seguridad en la información que se genera y se utiliza para la adecuada toma de decisiones.

La incorporación de tecnología en la ejecución de los procesos de la Universidad debe realizarse con base en una planificación con visión y objetivos claros, alineada a los objetivos institucionales y con un enfoque de soporte efectivo a sus procesos.

De igual forma, para que el Plan Estratégico de Tecnologías de la Información 2016 – 2018 se pueda llevar a cabo, es necesario considerar que su ejecución efectiva depende de las capacidades de TI. Como estas capacidades serán desarrolladas en forma progresiva, se plantea igualmente una priorización de los programas, orientada a mejorar la gestión de su ejecución.

Así mismo, se recomienda a los órganos directivos de la Universidad, entender y reconocer las capacidades tecnológicas actuales, las oportunidades que ofrece TI y la necesidad de capitalizar esas oportunidades para el logro de la misión institucional.

Se hace necesario además, implementar estrategias de formación a los distintos estamentos de la Universidad, para que se haga un uso adecuado de los recursos tecnológicos y de esta manera se garantice su disponibilidad y la de la información que a través de éstos se genera, para ofrecer servicios de calidad a toda la comunidad universitaria.

Se debe reconocer entonces que una gestión adecuada de los recursos tecnológicos, permite que la Universidad diseñe e implemente procesos académicos, administrativos y de extensión a la comunidad, cada vez más dinámicos. Es necesario destacar que el uso adecuado de estos recursos contribuye significativamente a que los procesos de gestión académica, razón de ser de la Institución, logren sus propósitos.

REFERENCIAS BIBLIOGRÁFICAS

ARRIETA SÁNCHEZ, María Alejandra, et al. Evaluación de la Seguridad Física y Ambiental en la División de Sistemas de la Universidad Francisco de Paula Santander Ocaña. Ocaña: 2014.

BAILEY, Cristian. PETI Planeación Estratégica de Tecnologías de Información, Metodología. Disponible en Internet: <http://es.scribd.com/doc/27526056/Peti-planeacion-Estrategica-Ti-Itcp>

BOHÓRQUEZ CONDE, Lorena Astrid, et al. Plan estratégico para el proyecto Génesis SIA de la Universidad Francisco de Paula Santander Ocaña. Trabajo de grado Especialista en Auditoría de Sistemas. Ocaña: Universidad Francisco de Paula Santander Ocaña. División de Posgrados y Educación Continuada, 2013.

CASTELLS, Manuel. La Sociedad Red: Una visión global. ISBN 84-206-4784-5 Alianza Editorial, 2006.

CORREA OSPINA, J. I. y LÓPEZ TRUJILLO, M. Planeación estratégica de tecnologías informáticas y sistemas de información. Manizales: Universidad de Caldas, 2007.

FLÓREZ PICÓN, Ivette Carolina, et al. Plan estratégico de tecnología de la información (PETI) aplicado a la Cooperativa de transporte Cootranshacaritama Ltda. Trabajo de grado Especialista en Auditoría de Sistemas. Ocaña: Universidad Francisco de Paula Santander Ocaña. División de Posgrados y Educación Continuada, 2013.

ISO/IEC 27002:2013. Tecnología de la información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información. Disponible en Internet: <http://www.iso27000.es/download/ControlesISO27002-2013.pdf>

IT GOVERNANCE INSTITUTE. Alineando COBIT 4.1, ITIL v3 e ISO 27002 en beneficio de la empresa. 2008. p. 17. Disponible en Internet: <http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-COBIT-4-1-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa_res_Spa_0108.pdf>

JIMÉNEZ OVALLOS, Wilson Fabián y GAONA CÁCERES, Jessica Lorena. Guía Metodológica para el diseño de un Plan Estratégico de TI en empresas de telecomunicaciones. Trabajo de grado Especialista en Auditoría de Sistemas. Ocaña: Universidad Francisco de Paula Santander Ocaña. División de Posgrados y Educación Continuada, 2013.

MATILLA, Katia. Los modelos de planeación estratégica en la teoría de las relaciones públicas. 1 ed.: Editorial UOC, 2008. 269 p.

PODER JUDICIAL DEL PERÚ. Plan Estratégico de Tecnologías de Información del Poder Judicial 2012 – 2016. Disponible en Internet: <http://www.oas.org/juridico/pdfs/mesicic4_per_anex2.pdf>

RAMANANTSOA, T. Planificación estratégica en empresas diversificadas. En: ABASCAL ROJAS, Francisco. Como se hace un plan estratégico: la teoría del marketing estratégico. 4ed. España: ESIC Editorial, 2004.

RÍOS HUÉRCANO, Sergio. Manual ITIL v3 Íntegro. Disponible en Internet: <http://es.slideshare.net/Biable/manual-itil-integro>

RODRÍGUEZ VALENCIA, J. Cómo aplicar la planeación estratégica a las pequeñas y medianas empresas.

UNIVERSIDAD AUSTRAL DE CHILE. Plan Estratégico de Tecnologías de la Información 2012 – 2015. Disponible en Internet: <https://www.uach.cl/uach/_file/plan-estrategico-de-ti.pdf>

UNIVERSIDAD DEL VALLE. Plan de informática y telecomunicaciones de la Universidad del Valle 2005-2007. Disponible en Internet: http://oitel.univalle.edu.co/plandesarrollo/2005-2007/documentos/Plan-Estrategico-OITEL-5_impresion.pdf

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. División de Sistemas. Procedimiento administración de los recursos informáticos. Actualizado 23 de enero de 2015. Disponible en Internet: <https://ufpso.edu.co/ftp/pdf/procedimientos/sitt/R-TT-DSS-002D.pdf>

_____. Oficina de Planeación. Formato plan de acción proceso. Actualizado 1 de diciembre de 2014. Disponible en Internet: <https://ufpso.edu.co/ftp/pdf/planes_accion/2015/plan_sitt15.pdf>

_____._____. Caracterización proceso Sistemas de Información, Telecomunicaciones y Tecnología, 2010. Actualizado 6 de noviembre de 2013.Disponible en Internet: <https://ufpso.edu.co/ftp/pdf/caracterizacion/sitt/Z-TT-DSS-001E1.pdf>

_____._____. Plan de Contingencia de TI versión 1.0. Actualizado 20 de octubre de 2010. Disponible en Internet: <https://ufpso.edu.co/ftp/doc/otrospro/sitt/L-TT-DSS-002A.pdf>

_____. Plan de Desarrollo Institucional 2014 – 2019. Actualizado 2 de octubre de 2013. Disponible en Internet: < https://ufpso.edu.co/ftp/pdf/documentos/plan_desarrollo2014-2019IV.pdf>

_____._____. Procedimiento gestión de los sistemas de TI. Actualizado 20 de septiembre de 2010. Disponible en Internet: <https://ufpso.edu.co/ftp/pdf/procedimientos/sitt/R-TT-DSS-003A.pdf>

VERA VÉLEZ, Lamberto. La investigación cualitativa. Disponible en Internet en: <http://www.ponce.inter.edu/cai/Comite-investigacion/investigacion-cualitativa.html>

ANEXO A. ENTREVISTA APLICADA AL JEFE DE LA DIVISIÓN DE SISTEMAS

R/PT ENT01

Empresa: **Universidad Francisco de Paula Santander Ocaña** Área: División de Sistemas Auditado: Jefe División de Sistemas	Fecha elaboración: 05/02/2015 Fecha revisión: 07/02/2015 Fecha aplicación: 09/02/2015

Objetivo

Evaluar el cumplimiento de las actividades relacionadas con la seguridad de la información de acuerdo con el estándar ISO 27002:2013

ÍTEM	PREGUNTA	RPT	AUDITOR
1	¿Existe formalmente una política de seguridad que establezca los lineamientos para la protección adecuada de los activos de información?		M.R.S.R
RTA	*Sí. El documento fue aprobado por el Comité Administrativo de la Universidad. Ya se encuentra la versión 2.0*	AP01	
2	¿Cómo se ha dado el proceso de comunicación/socialización de estas políticas a cada uno de los estamentos de la Universidad?		
RTA	*Actualmente se conoce la versión 1.0. La segunda versión fue enviada a la Oficina de Calidad para su respectiva revisión.*		
3	¿Cada cuánto se la hace revisión a estas políticas?		
RTA	*Cada dos años*		
4	¿Existen responsables de la protección de los activos de información con sus funciones claramente definidas?		
RTA	*Los responsables son los jefes de las distintas dependencias y posteriormente se delega las funciones internas.*		
5	¿Las responsabilidades en cuanto a la seguridad de los activos de información, se encuentran segregadas para reducir la posibilidad de fraude o pérdida de dichos activos?		
RTA	*Sí. Especialmente el Sistema de Información Financiero y de la Oficina de Admisiones, Registro y Control.*		
6	¿La Universidad cuenta con procedimientos claramente definidos que especifiquen cuándo y cuáles autoridades contactar en el caso en los que se presente un incidente de seguridad que pueda poner en riesgo la continuidad de las operaciones?		
RTA	*Desde la División de Sistemas, sí.*		
7	¿La Universidad o específicamente la División de Sistemas, mantiene contacto con grupos de interés especial, para establecer acuerdos de intercambio de información en temas de seguridad? (*alertas relacionadas con ataques y vulnerabilidades, asesorías, consultorías,…)*		
RTA	*Nos encontramos inscritos a una base de datos de vulnerabilidades. Recibimos asesoría de una empresa de seguridad, que se encarga de realizar auditorías anuales, específicamente lo relacionado con pentesting.*		

8	¿Existen procedimientos documentados para las diferentes actividades del sistema? (*realización de backup, desarrollo de software, capacitación, mantenimiento de hardware y software, adquisición de tecnología, seguridad, reporte de incidentes, recuperación del sistema,…*)		
RTA	*Algunos procedimientos están documentados. Lo relacionado con adquisiciones está contemplado en el Plan de Acción (anual)*	AP02	
9	¿Los cambios o modificaciones a estos procedimientos son controlados? ¿Cómo?		
RTA	*Cuando los cambios son de fondo, sí. Se hace un seguimiento de acuerdo como lo establece el estándar ISO 9001.*		
10	¿Quién autoriza estos procedimientos?		
RTA	*La Oficina de Calidad*		
11	¿Existe un procedimiento formal de aprobación de dichos cambios?		
RTA	*Sí. Esto se hace en un formato emitido por la Oficina de Calidad llamado Control de Novedades*		
12	En el entorno de desarrollo de aplicaciones, ¿las tareas propias del proceso, se encuentran segregadas?		
RTA	*No. Una persona hace todo: análisis, diseño, codificación, pruebas, etc.*		
13	Cuando se establecen acuerdos con terceros, ¿existe una persona o equipo responsable de la verificación del cumplimiento de los servicios ofrecidos por ellos?		
RTA	*Sí. Un supervisor del servicio.*		
14	¿Se realiza monitoreo y/o revisión de los servicios de terceros, en lo relacionado con las condiciones de protección y confidencialidad de la información que se maneja?		
RTA	*Sí, a través de los acuerdos de confidencialidad.*	AP01	
15	Existen procedimientos formales para administrar los cambios en los servicios ofrecidos por terceros como: *ampliación de los servicios, desarrollo de sistemas, modificación de las políticas y procedimientos establecidos por la Universidad, implementación de nuevos controles, uso de tecnologías nuevas, entre otros.*		
RTA	*No.*		
16	¿Se realizan proyecciones de los requerimientos en la ampliación de la capacidad tecnológica de hardware o software?		
RTA	Sí, de acuerdo con el Plan de Acción. Existe un plan de ejecución que evalúa las actividades.	AP02	
17	¿Existen procedimientos para probar los requerimientos operacionales de los nuevos sistemas (o actualizaciones) antes de su aceptación y uso? *Desempeño equipo de cómputo, recuperación de errores, planes de contingencia, compatibilidad con otros sistemas,…*		
RTA	*No, solo pruebas internas*		
18	¿Se realiza verificación del cumplimiento de cada una de las etapas del proceso de desarrollo de nuevos sistemas para asegurar la eficiencia operacional del diseño del sistema propuesto?		

RTA	*Sí, internamente; pero no se documenta.*		
19	¿Qué controles se tienen implementados para la detección, prevención y recuperación contra código malicioso?		
RTA	*Revisión de logs y verificaciones cuando los equipos fallan.*		
20	¿Existen procedimientos para comunicar a las distintas dependencias de la Universidad que manejan información confidencial, sobre la presencia de código malicioso o cualquier amenaza que pueda poner en riesgo la seguridad de los datos?		
RTA	No. No ha ocurrido un incidente de ese tipo. Los errores que se presentan se registran en un formato de bitácora de errores.		
21	¿Cómo se lleva a cabo la realización de Backup's?		
RTA	*Se realiza de forma automática. Cada servidor envía las copias de respaldo al servidor de backup interno (12:00 p.m.) y de allí al DATACENTER.*	AP05	
22	¿Qué tipo de información se respalda?		
RTA	Se respalda la información de la configuración, de la base de datos y del sistema.		
23	¿Se ha probado la restauración de la data?		
RTA	*Sí, pero no hay formatos. Este procedimiento no se documenta.*		
24	¿Qué resultados ha arrojado dicho procedimiento?		
RTA	*Algunos fallaron*		
25	¿Estas pruebas se documentan?		
RTA	*No.*		
26	¿Se utilizan bitácoras para registrar las fallas o problemas en los sistemas de información?		
RTA	*Sí. Hay un formato llamado bitácora manejo de errores.*	AP04	
27	¿Cómo es el procedimiento para el reporte de los eventos de seguridad de la información?		
RTA	No existe tal procedimiento. Para los eventos de seguridad se le da un manejo interno, se registra en la bitácora de errores y dependiendo del caso, se envía un correo masivo a todas las dependencias de la Universidad.	AP04	
28	¿Cómo se da respuesta a los incidentes de seguridad? ¿Está documentado el procedimiento?		
RTA	*No existe procedimiento documentado para tal situación*.		
29	¿Se realiza monitoreo en los diferentes sistemas de información para verificar la efectividad de los controles adoptados?		
RTA	*No. Se espera a que haya un requerimiento y se registra en la bitácora de errores.*		
30	¿Este procedimiento se encuentra contemplado en la política de seguridad de la información?		
RTA	Los requerimientos se hacen a través de un formato de soporte y atención al usuario.	AP06	
31	¿Se lleva registro de las operaciones realizadas por el administrador y los operadores en los sistemas de		

	información?		
RTA	*Se realiza a través de una función de auditoría interna habilitada en el motor de la base de datos.*		
32	¿Se revisa periódicamente la bitácora de los sistemas?		
RTA	*Cuando sucede algo.*		
33	¿Existen reglas claras para manejar las fallas reportadas? Indique		
RTA	*No.*		
34	¿Existe inventario de todos los activos de información de la Universidad?		
RTA	*Sí.*		
35	¿Se realiza alguna clasificación de los activos? ¿Qué criterios de clasificación se utilizan?		
RTA	*Sí, la realiza la Oficina de Almacén.*		
36	¿Existe un responsable de la protección de estos activos?		
RTA	*Sí*		
37	¿Existen reglas claramente definidas documentadas e implementadas para el uso aceptable de los activos de información? (*datos, correo electrónico, Internet, aplicaciones, dispositivos, documentación*)		
RTA	*Eso es manejado en la Oficina de Personal, pero el contrato no dice nada al respecto.*		
38	¿Se realiza verificación a los inventarios con el propósito de actualizarlos?		
RTA	*Sí. Lo realiza Almacén.*		
39	¿Existen procedimientos para el etiquetado de los activos, que sea acorde con el esquema de clasificación?		
RTA	Sí. Almacén utiliza una codificación para ello. Las licencias de software las maneja la División de Sistemas, suministradas del inventario.		
40	¿Existen procedimientos para el manejo, procesamiento, de-clasificación y destrucción de activos, por cada nivel de clasificación?		
RTA	*Para dar de baja un equipo, la oficina de Almacén solicita un dictamen sobre el estado del mismo a la División de Sistemas.*	AP07	
41	Los acuerdos con otras organizaciones que incluyen intercambio de información, ¿establecen procedimientos para identificar o interpretar las etiquetas de clasificación?		
RTA	*Eso lo maneja Inventario*		
42	¿Qué tratamiento se le da a los medios extraíbles reusables?		
RTA	*Son guardados; así mismo las licencias de software.*		
43	¿Quién se encarga de tal procedimiento?		
RTA	*La División de Sistemas*		
44	¿Qué procedimiento se utiliza para la eliminación de los medios de almacenamiento de información que hayan		

	cumplido su ciclo de vida?		
RTA	*Se almacenan*		
45	¿Existen procedimientos para proteger la información durante el transporte por fuera de los límites físicos de la Universidad? (*servicio de mensajería, empaquetado, identificación del personal de la empresa de mensajería,…*)		
RTA	No conozco la existencia de dicho procedimiento		
46	El documento de políticas de seguridad ¿contempla procedimientos de control para el registro y des-registro de usuarios para el acceso a los sistemas de información?		
RTA	De manera específica, no.		
47	¿Se controla la asignación de privilegios de acceso a los sistemas de información?		
RTA	Sí, a través de un formato de administración de usuarios	AP03	
48	¿Estos privilegios se revisan periódicamente?		
RTA	*No. Cada seis meses el sistema pide automáticamente cambio de contraseña. Para eliminación de privilegios, se espera una notificación de la Oficina de Personal, para hacer el retiro correspondiente.*		
49	¿Qué medidas de protección se implementan al utilizar dispositivos móviles, como herramienta de trabajo?		
RTA	Se utiliza el congelador y a través de logueo con usuario y contraseña.		
50	¿Qué procedimientos se implementan para impedir el acceso no autorizado a los servicios red?		
RTA	*Se utiliza un firewall para cada red. Para la red inalámbrica, el servicio es abierto.*		
51	¿Qué medidas se tienen en cuenta al momento de compartir recursos o información confidencial?		
RTA	*A través de usuario y contraseña*		
52	¿Existe algún procedimiento que indique como minimizar el impacto en caso de pérdidas de activos de información, ya sea a causa de desastres naturales, accidentes, fallas del equipo u otras acciones deliberadas?		
RTA	Existe un plan de contingencia	AP08	
53	¿A nivel de sistemas de información, la Universidad cuenta con un Plan de Continuidad de Negocio?		
RTA	No.		
54	¿Dicho Plan se ha comunicado/socializado a cada una de las dependencias de la Universidad?		
RTA	No existe.		

Magreth R. Sanguino R.	
MAGRETH ROSSIO SANGUINO REYES AUDITORA	**ANTÓN GARCÍA BARRETO** Jefe División de Sistemas **AUDITADO**

ANEXO B. ENTREVISTA APLICADA AL JEFE DE PERSONAL

R/PT ENT02

Empresa: Entrevistado:	**UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA** **Jefe División de Personal**	Fecha elaboración: 05/02/2015 Fecha revisión: 07/02/2015 Fecha aplicación: 09/02/2015

Objetivo
Evaluar el cumplimiento de las actividades relacionadas con la seguridad de la información de acuerdo con el estándar ISO 27002:2013

ÍTEM	PREGUNTA	RPT	AUDITOR
1	En el proceso de contratación de personal, ¿qué aspectos se tienen en cuenta para evaluar a los diferentes candidatos?		C.L.L.S.
2	Cuando se establece relaciones con terceros (contratistas, proveedores, etc.), ¿se hace verificación de antecedentes como requisito para la contratación?		
3	Cuando se realiza promoción del personal (ascensos), ¿se verifican nuevamente estos antecedentes?		
4	¿Qué aspectos de los antecedentes se revisan?		
5	¿En la etapa de contratación se establece que los empleados deben firmar un acuerdo de confidencialidad, en donde además de especificar las funciones propias de su cargo, se indique la responsabilidad que tienen frente a la información a la cual van a tener acceso?		
6	¿Se establecen acuerdos de confidencialidad con terceros?		
7	¿Están los empleados capacitados en lo relacionado con la protección y manejo adecuado de la información que tienen bajo su responsabilidad?		
8	Existe evidencia del plan de capacitación proporcionada a los empleados en cuanto a seguridad de la información		
9	Existe formalmente alguna sanción o proceso disciplinario para aquellos empleados que cometan alguna falta contra la seguridad de la información (fraude, divulgación no autorizada, pérdida de activos, entre otras)		
10	¿En cuánto a los derechos de acceso a información confidencial o a cualquier otro activo, qué procedimiento se lleva a cabo para eliminar esos derechos, cuando el empleado es retirado o movido de su cargo?		

Cindy lorena lobo S.	
CINDY LORENA LOBO SÁNCHEZ AUDITORA	**NUBIA PATRICIA RAMIREZ** Jefe División de Personal AUDITADO
OBSERVACIONES: La Jefe de la División de Personal, manifiesta que las respuestas a las preguntas de la entrevista se pueden encontrar en los procedimientos descritos en la página web institucional: www.ufpso.edu.co en la sección de Sistema Integrado de Gestión/Gestión Humana.	

ANEXO C. ENTREVISTA AL JEFE DE ALMACÉN

			R/PT ENT03
Empresa: Entrevistado:	**UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA** **Jefe Unidad de Almacén**	Fecha elaboración: 05/02/2015 Fecha revisión: 07/02/2015 Fecha aplicación: 09/02/2015	
Objetivo Evaluar el cumplimiento de las actividades relacionadas con la seguridad de la información de acuerdo con el estándar ISO 27002:2013			
ÍTEM	**PREGUNTA**	**RPT**	**AUDITOR**
1	¿Existe inventario de todos los activos de información de la Universidad?		C.L.LS.
RTA	*Si existe un inventario de muebles, enseres y equipos. Todo está en el sistema.*		
2	¿Se realiza alguna clasificación de los activos? ¿Qué criterios de clasificación se utilizan?		
RTA	*Si se realiza una clasificación de los activos. Dependiendo de los bienes se clasifica y se incluyen en el sistema.*		
3	¿Existe un responsable de la protección de estos activos?		
RTA	*De cada dependencia hay un responsable*		
4	¿Se realiza verificación a los inventarios con el propósito de actualizarlos?		
RTA	*Depende, si hay cambio de responsable, es obligatorio.*		
5	¿Existen procedimientos para el etiquetado de los activos, que sea acorde con el esquema de clasificación?		
RTA	*Si existen procedimientos para el etiquetado de los activos, a través de un código contable.*		
6	¿Existen procedimientos para el manejo, procesamiento, de-clasificación y destrucción de activos, por cada nivel de clasificación?		
RTA	*Si existen procedimientos para el manejo y destrucción de activos. El responsable debe seguir unos pasos*		
7	Los acuerdos con otras organizaciones que incluyen intercambio de información, ¿establecen procedimientos para identificar o interpretar las etiquetas de clasificación?		
RTA	*Para la clasificación de los activos se utilizan códigos contables, usan el PUC - Plan Único de Cuentas.*		
8	¿Qué procedimiento se utiliza para la eliminación de los medios de almacenamiento de información que hayan cumplido su ciclo de vida?		

RTA	*Se utiliza un procedimiento para dar de baja a los bienes y activos*		
9	¿Qué tipo de documentación le asegura la veracidad del vendedor y la calidad del producto?		
RTA	*Subdirección administrativa se encarga de esta parte, almacén solo recibe los activos*		
10	¿Qué procedimientos siguen ustedes para verificar el estado y calidad de los productos recibidos?		
RTA	*Únicamente se verifica el estado y la cantidad.*		
11	¿Existe alguna persona encargada de supervisar los servicios prestados por parte de las empresas que suministran los bienes a la Universidad?		
RTA	Si existe y se encarga de verificar si se entregó oportunamente los activos, la calidad y el precio.		

Cindy lorena lobo S.	
CINDY LORENA LOBO SÁNCHEZ AUDITORA	**NAHUN LOBO** Jefe Unidad de Almacén AUDITADO

ANEXO D. ENTREVISTA AL JEFE DE CALIDAD

R/PT ENT04

Empresa: Entrevistado:	**UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA** **Jefe Oficina de Calidad**	Fecha elaboración: 05/02/2015 Fecha revisión: 07/02/2015 Fecha aplicación: 10/02/2015

Objetivo
Evaluar el cumplimiento de las actividades relacionadas con la seguridad de la información de acuerdo con el estándar ISO 27002:2013

ÍTEM	PREGUNTA	RPT	AUDITOR
1	¿Existen documentos de los controles, políticas y estatutos que se manejan en la Universidad?		M.A.A.S
RTA	*Sí, en el normograma interno y externo.*		
2	¿Se hace seguimiento al cumplimiento de tales políticas, procedimientos y estándares?		
RTA	*A través de auditorías internas*		
3	¿Se tiene conocimiento de que exista un documento de políticas de seguridad de la información?		
RTA	*Procedimientos (copias en el servidor), repositorio interno con copias mensuales FTP*		
4	¿Existe algún procedimiento que asegure el cumplimiento de los requisitos legales sobre el uso de cualquier material con respecto al cual puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentado?		
RTA	*No existen procedimientos que asegure el cumplimiento de los requisitos legales sobre el uso de cualquier material*		
5	¿Las actividades y requerimientos de auditoría que involucran chequeos de los sistemas de información, se encuentran debidamente reglamentados?		
RTA	*En la oficina de calidad se audita sobre la norma, no sobre los sistemas*		

MARÍA ALEJANDRA ARRIETA SÁNCHEZ AUDITORA	**YURLEY MEDINA** Jefe Oficina de Calidad AUDITADO

ANEXO E. PRUEBA DE CUMPLIMIENTO UNO

	R/PT PRC01
Empresa: **Universidad Francisco de Paula Santander Ocaña** Proceso**: Gestión de la Seguridad de la Información** Área: **División de Sistemas**	Fecha: 14/02/2015
OBJETIVO Verificar la eficiencia en la implementación de los controles contemplados en el estándar ISO/IEC 27002:2013.	
TÉCNICA EMPLEADA: Revisión	
TIPO DE PRUEBA Cumplimiento __X_ Sustantiva ____ Doble Finalidad ____	
PROCEDIMIENTO A EMPLEAR: **1.** Realizar la revisión del documento de Políticas de Seguridad de la Información. **2.** Realizar una entrevista al Jefe de la División de Sistemas para conocer aspectos relacionados con la gestión de la seguridad de la información. **3.** Comprobar la información obtenida de las fuentes anteriores.	
RECURSOS Políticas de Seguridad de la Información V2 - División de Sistemas de la Universidad Francisco de Paula Santander Ocaña	
RESULTADOS DE LA PRUEBA	
HALLAZGOS	**R/PT**
Actualmente la Universidad Francisco de Paula Santander Ocaña, no cuenta con un marco regulatorio para iniciar y controlar los procesos de implementación de la seguridad de la información dentro de la Institución. Existen procedimientos establecidos para algunos de los procesos institucionales; sin embargo, no son suficientes. De igual manera, no existen responsabilidades claramente definidas para la protección de los activos individuales; la responsabilidad de los activos, recae sobre el jefe del área. Por otra parte, el documento de políticas de seguridad V2 emitido por la División de Sistemas, no es del conocimiento de todos los miembros de la comunidad universitaria, puesto que no se ha publicado oficialmente, ni a través de la plataforma Web, ni por medios impresos.	**POL01**
CAUSA	

No se reconoce actualmente la necesidad de implementar tales procedimientos.	
SITUACIÓN DE RIESGO QUE GENERA	
Se puede presentar pérdida parcial o total de la información u otros activos de la Universidad, sin poder asignar responsables. Igualmente, el desconocimiento de las políticas de seguridad puede generar el uso inadecuado de la información y la divulgación no autorizada de la misma a terceros.	
RECOMENDACIONES DE AUDITORIA	
Se sugiere definir un marco regulatorio que garantice el cumplimiento de los controles de seguridad contemplados en la política de seguridad de la información de la Universidad.	
ELABORADO POR: **Esp. MAGRETH ROSSIO SANGUINO REYES** Auditora Líder	APLICADO POR: **Esp. MAGRETH ROSSIO SANGUINO REYES** Auditora Líder

ANEXO F. PRUEBA DE CUMPLIMIENTO DOS

	R/PT PRC02
Empresa: **Universidad Francisco de Paula Santander Ocaña** Proceso**: Gestión de la Seguridad de la Información** Área: **División de Personal**	Fecha: 14/02/2015
OBJETIVO Verificar la eficiencia de la implementación de los controles de contemplados en el estándar ISO/IEC 27002:2013.	
TÉCNICA EMPLEADA: Revisión	
TIPO DE PRUEBA Cumplimiento __X_ Sustantiva ____ Doble Finalidad ____	
PROCEDIMIENTO A EMPLEAR: **1.** Realizar la revisión de los procedimientos contemplados en el proceso de Gestión Humana del Sistema Integrado de Gestión. **2.** Realizar una entrevista a la Jefe de la División de Personal, para conocer de primera mano, aspectos relacionados con la seguridad de la información ligada a los recursos humanos. **3.** Comprobar la información obtenida de las fuentes anteriores.	
RECURSOS Procedimientos y formatos procesos Gestión Humana – Sistema Integrado de Gestión	
RESULTADOS DE LA PRUEBA	
HALLAZGOS	**R/PT**
Los contratos laborales aunque no estipulan una cláusula de confidencialidad específica, contienen un ítem que se refiere a la reserva total de la información a la cual tendrá acceso cada funcionario y a las sanciones o llamados de atención por incumplimiento al mismo. El contrato de trabajo tampoco contempla reglas claras para el uso aceptable de algunos activos como correo electrónico, dispositivos, datos, equipos, entre otros.	**AP09**
Se pudo evidenciar que los empleados no reciben información específica en cuanto a procedimientos de seguridad de la información que tienen bajo su responsabilidad. Tampoco se protocoliza la entrega de información relacionada con la información de acceso a los módulos o sistemas de información que manejarán.	**ENT05**
CAUSA	
No se ha implementado este procedimiento.	
SITUACIÓN DE RIESGO QUE GENERA	

Omisiones en el manejo de información confidencial. Divulgación no autorizada de información confidencial.	
RECOMENDACIONES DE AUDITORIA	
Definir un acuerdo de confidencialidad para cada uno de los empleados de la Universidad, que contemple los requerimientos legales para proteger la información que tiene a su cargo. Así mismo, establecer procedimientos formales para la entrega y actualización de la información relacionada con los derechos de acceso de los usuarios a los sistemas de información.	
ELABORADO POR: **Esp. MAGRETH ROSSIO SANGUINO REYES** Auditora Líder	APLICADO POR: **Esp. MAGRETH ROSSIO SANGUINO REYES** Auditora Líder

ANEXO G. PRUEBA DE CUMPLIMIENTO TRES - UNO

	R/PT PC03-1
Empresa: **Universidad Francisco de Paula Santander Ocaña** Proceso**: Gestión de la Seguridad de la Información** Área**: División de Sistemas**	Fecha: 17/02/2015
OBJETIVO Evaluar las acciones contempladas en el Plan de Contingencias para la protección de los equipos de cómputo contra amenazas de tipo ambiental y otros factores internos y externos.	
TÉCNICA EMPLEADA: Revisión	
TIPO DE PRUEBA Cumplimiento __X_ Sustantiva ____ Doble Finalidad ____	
PROCEDIMIENTO A EMPLEAR: **1.** Realizar la revisión del Plan de Contingencias de TI de la División de Sistemas de la UFPSO. **2.** Realizar una entrevista al Jefe de la División de Sistemas para conocer aspectos sobre la seguridad de los equipos de cómputo de dicha área. **3.** Comprobar la información obtenida de las fuentes anteriores.	
RECURSOS **1.** Plan de Contingencias de TI – División de Sistemas de la Universidad Francisco de Paula Santander Versión 1.0 **2.** Procedimiento Administración de los recursos informáticos - División de Sistemas de la Universidad Francisco de Paula Santander	
RESULTADOS DE LA PRUEBA	
HALLAZGOS	**R/PT**
No existe un generador de emergencia (planta eléctrica) para los casos en los que se presente una interrupción prolongada del servicio eléctrico y que permita seguir prestando los servicios básicos de información.	
CAUSA	
La Universidad no ha adquirido esta planta eléctrica.	
SITUACIÓN DE RIESGO QUE GENERA	
Se puede presentar pérdida de información sensible y daños en los equipos y servidores principales.	
RECOMENDACIONES DE AUDITORIA	

Se sugiere implementar un sistema de suministro de corriente alternativo (generador de emergencia) que soporte la carga de los equipos principales y que permita dar continuidad a los servicios informáticos de la Universidad.	
ELABORADO POR: **Esp. MAGRETH ROSSIO SANGUINO REYES** Auditora Líder	APLICADO POR: **Esp. MAGRETH ROSSIO SANGUINO REYES** Auditora Líder

ANEXO H. PRUEBA DE CUMPLIMIENTO TRES – DOS

			R/PT PC03-2
Empresa: **Universidad Francisco de Paula Santander Ocaña** Proceso: **Gestión de la Seguridad de la Información** Área**: División de Sistemas**			Fecha: 17/02/2015
OBJETIVO Evaluar las acciones contempladas en el Plan de Contingencias para la protección de los equipos de cómputo contra amenazas de tipo ambiental y otros factores internos y externos.			
TÉCNICA EMPLEADA: Revisión			
TIPO DE PRUEBA	Cumplimiento __X_	Sustantiva ____	Doble Finalidad ____
PROCEDIMIENTO A EMPLEAR: **1.** Realizar la revisión del Plan de Contingencias de TI de la División de Sistemas de la UFPSO. **2.** Realizar una entrevista al Jefe de la División de Sistemas para conocer aspectos sobre la seguridad de los equipos de cómputo de dicha área. **3.** Comprobar la información obtenida de las fuentes anteriores.			
RECURSOS **1.** Plan de Contingencias de TI – División de Sistemas de la Universidad Francisco de Paula Santander Versión 1.0 **2.** Procedimiento Administración de los recursos informáticos - División de Sistemas de la Universidad Francisco de Paula Santander			
RESULTADOS DE LA PRUEBA			
HALLAZGOS			**R/PT**
No existen medidas de seguridad efectivas para controlar el acceso a las áreas críticas como la sala de servidores. Sólo existe una puerta con llave.			
CAUSA			
No se han hecho inversiones en tecnología para control de acceso a áreas.			
SITUACIÓN DE RIESGO QUE GENERA			
La pérdida de información y de cualquier otro elemento dentro de la sala de servidores es un riesgo latente que puede afectar la disponibilidad de la información sensible.			
RECOMENDACIONES DE AUDITORIA			

Implementar un sistema biométrico para controlar el acceso al cuarto de servidores.	
ELABORADO POR: **Esp. MAGRETH ROSSIO SANGUINO REYES** Auditora Líder	APLICADO POR: **Esp. MAGRETH ROSSIO SANGUINO REYES** Auditora Líder

ANEXO I. PRUEBA DE CUMPLIMIENTO CUATRO

			R/PT PRC04
Empresa: **Universidad Francisco de Paula Santander Ocaña** Proceso: **Gestión de la Seguridad de la Información** Área**: División de Sistemas**			Fecha: 28/04/2014
OBJETIVO Evaluar las acciones contempladas en el Plan de Contingencias para la protección de los equipos de cómputo contra amenazas de tipo ambiental y otros factores internos y externos.			
TÉCNICA EMPLEADA: Revisión			
TIPO DE PRUEBA	Cumplimiento __X_	Sustantiva ____	Doble Finalidad ____
PROCEDIMIENTO A EMPLEAR: **1.** Realizar la revisión del Plan de Contingencias de TI de la División de Sistemas de la UFPSO. **2.** Realizar una entrevista al Jefe de la División de Sistemas para conocer aspectos sobre la seguridad de los equipos de cómputo. **3.** Comprobar la información obtenida de las fuentes anteriores.			
RECURSOS **1.** Plan de Contingencias de TI – División de Sistemas de la Universidad Francisco de Paula Santander Versión 1.0 **2.** Procedimiento Administración de los recursos informáticos - División de Sistemas de la Universidad Francisco de Paula Santander			
RESULTADOS DE LA PRUEBA			
HALLAZGOS			**R/PT**
Las copias de seguridad de la información sensible son almacenadas solo por cuatro días consecutivos en un data center externo contratado por la Universidad.			**AP10**
Se encontró que las copias de respaldo que se hacen diariamente por una parte, quedan almacenadas en el mismo servidor y una copia se guarda en el servidor de backup interno. Este último, se encuentra también en el cuarto de servidores, presentándose la misma situación de ineficiencia en los controles de acceso.			
CAUSA			
No se han asignado recursos para la mejora de la infraestructura física y tecnológica que permita administrar de forma segura la información respaldada.			
SITUACIÓN DE RIESGO QUE GENERA			

Pérdida de información y/o modificaciones no autorizadas a la misma.	
RECOMENDACIONES DE AUDITORIA	
Incluir dentro del presupuesto de la Universidad, un rubro para mejoramiento de la infraestructura física y tecnológica, de tal manera que se pueda construir o asignar un espacio, fuera de las instalaciones de la Universidad, con las condiciones requeridas para el almacenamiento y administración de las copias de respaldo de la información.	
ELABORADO POR: **Esp. MAGRETH ROSSIO SANGUINO REYES** Auditora Líder	APLICADO POR: **Esp. MAGRETH ROSSIO SANGUINO REYES** Auditora Líder

ANEXO J. PLAN DE TRABAJO PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN

Empresa: **Universidad Francisco de Paula Santander Ocaña**	Fecha Final: 10/09/2014 Fecha Inicio: 20/04/2015

Objetivo General
Diseñar el Plan Estratégico de Tecnologías de la Información para la Universidad Francisco de Paula Santander Ocaña.

RESPONSABLES
Magreth Rossio Sanguino Reyes - Cindy Lorena Lobo Sánchez - María Alejandra Arrieta Sánchez

No.	ACTIVIDAD	FECHA
1	Reunión del equipo de trabajo para definir responsabilidades y tareas.	16/09/2014
2	Solicitud de documentación de los diferentes procesos de la Universidad soportados por la infraestructura tecnológica (fuentes primarias).	18/09/2014
3	Reunión del equipo de trabajo para el análisis de la documentación obtenida.	22/09/2014
4	Diseño de instrumentos de recolección de información (fuentes secundarias).	15/10/2014
5	Aplicación de instrumentos para la realización de la auditoría de cumplimiento bajo el estándar ISO 27002:2013	09/02/2015
6	Elaboración de herramientas para realizar pruebas de verificación (tercera fuente de información)	12/02/2015
7	Análisis de la gestión de la seguridad de la información – situación actual.	18/02/2015
8	Determinación del estándar para la elaboración del PETI	03/03/2015
9	Recolección de información adicional	16/03/2015
10	Definición de Componentes Estratégicos	20/03/2015
11	Elaboración Documento PETI	20/04/2015

ANEXO K. INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

I. Sistemas de Información

La Universidad Francisco de Paula Santander Ocaña cuenta con varios Sistemas de Información los cuales permiten de una manera óptima manejar la información, logrando así, un mejor aprovechamiento del recurso humano y físico de la institución.

Los Sistemas de Información están desarrollados con el sistema manejador de base de datos relacional "RDBMS ORACLE 10G BAJO LINUX" el cual permitió diseñar un eficiente modelo relacional que garantiza la integridad y seguridad de la información, permitiendo la definición de diferentes políticas para su administración:

SIA - Sistema de Información Académico

Es una aplicación elaborada para facilitar la administración de los diferentes procesos académicos que se llevan a cabo en la intranet de la Universidad.

Desarrollos Web del Sistema de Información Académico:

- *Digitación de Notas*
- *Inclusiones y/o Cancelación*
- *Solicitud de becas trabajo y/o Monitorias*
- *Solicitud de Financiación de la Matricula*
- *Solicitud de Vacacionales*
- *Registro de Hora Cátedra*
- *Peticiones, quejas y Reclamos*
- *Evaluación Docente*
- *Inscripción en Línea de Aspirantes*
- *Modulo para el manejo de los Cursos de Inglés (Inscripción, Matricula, Gestión de Grupos).*

SIB - Sistema de Información de Biblioteca

El S.I.B. cuenta con una Base de Datos diseñada en el Formato MARC para Datos Bibliográficos, que permite manejar información de cualquier tipo de material bibliográfico como lo son libros, tesis, publicaciones seriadas, archivos de computadora y material audiovisual y definir diferentes políticas propias de la Biblioteca Argemiro Bayona Portillo.

Desarrollos Web del Sistema de Información Bibliográfico:

- *Consulta de Bibliografía*
- *Biblioteca Digital – Dspace (Consulta de Trabajos de Grado en Línea)*

SIF - Sistema de Información Financiero

El Sistema de Información Financiera SIF, es una aplicación elaborada para facilitar la administración de los diferentes procesos contables y presupuestales que se llevan a cabo en la intranet de la Universidad. Paralelamente se tiene implementado el SIA y el SIB vía Web, a los cuales se puede acceder desde la página principal de la universidad. A través de estos sitios los estudiantes pueden entre otras cosas consultar la información académica, realizar el proceso de inclusiones y/o cancelaciones, evaluación docente, cursos vacacionales y consultar el material bibliográfico de la institución.

Módulos Desarrollados:

- *Solicitudes de Servicios y Compras*
- *Presupuesto (CDP, Obligaciones, etc.)*
- *Contabilidad (Cuentas por Pagar, Cuentas por Cobrar, Contabilidad)*
- *Subadministrativa (Órdenes, Autorización de pagos, etc.)*
- *Tesorería (Comprobantes de Egresos, Ingresos, etc.)*
- *Recursos Humanos (Nómina).*

SID - Sistema de Información Documental

El sistema de Gestión documental orientado a la Web, permite elaborar documentos y similares en la Universidad, el cual le permite a todas las secretarias generar dichos documentos bajo los parámetros dados en la oficina de archivo y correspondencia.

SIABE - Sistema de Información Académico de Bellas Artes

El sistema de Información Académica de la Escuela de Bellas Artes de la Universidad Francisco de Paula Santander Ocaña, es una aplicación Web que tiene como finalidad dar soporte a los procesos académicos y administrativos de dicha institución, beneficiando a toda la comunidad en especial a estudiantes, docentes y administrativos, quienes podrán consultar toda su información académica en cualquier momento y desde cualquier lugar de forma rápida y segura.

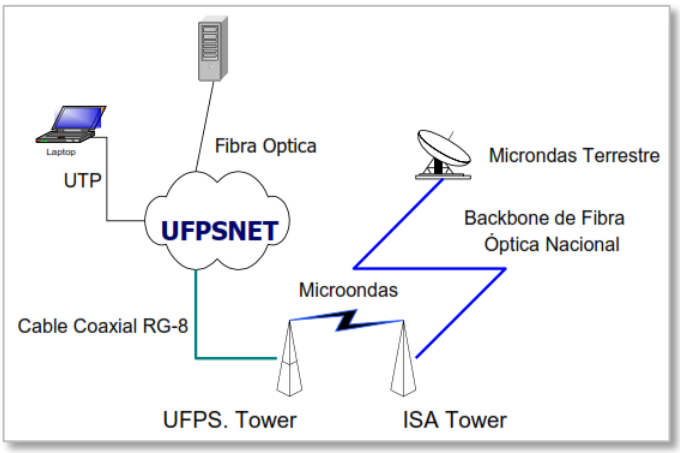
Desarrollos Web del Sistema de Información Académico:

- *Inscripción en Línea de Aspirantes*
- *Matricula por parte del Administrador del Portal.*

- *Digitación de Notas*
- *Registro de Hora Cátedra*
- *Evaluación Docente*

II. Plataforma Tecnológica

En la Universidad Francisco de Paula Santander Ocaña en su Campus Universitario de la sede principal, se extiende un Backbone (Cableado principal de transporte de datos) en fibra óptica con topología estrella, que interconecta el centro de cableado principal ubicado en el edificio División de Sistemas con los demás edificios localmente dispersos mediante Switches.



Fuente: UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. Sistemas de Información, Telecomunicaciones y Tecnología. Avances y Proyección Tecnológica, 2015.

Edificios interconectados:

Edificio División de Sistemas (Nodo Principal)
Edificio Casona (Conectado por medio de Fibra Óptica)
Edificio Salas de Cómputo (Conectado por medio de Fibra Óptica)
Edificio Anexos Académicos (Conectado por medio de Fibra Óptica)
Edificio Granja (Conectado por vía Inalámbrica)
Edificio de Aulas (Conectado por medio de Fibra Óptica)

Igualmente existe red de datos en las siguientes sedes: Edificio Sede Primavera y Edificio Escuela de Artes.
En cada uno de los edificios se encuentran conectadas todas las dependencias, las cuales cuentan con características técnicas que permiten una fácil conexión al medio de transmisión, como son los Switches y el cableado estructurado UTP categoría 5e y 7A.

El cableado estructurado de red del campus Universitario cuenta con 800 puntos distribuidos por todos los edificios y soportan la transmisión de datos (600 puntos) y voz (200 puntos) proporcionando flexibilidad de mantenimiento y configuración. Para la administración de voz la institución cuenta con una central telefónica de tecnología digital, para interfaces analógicas y digitales. Además se cuenta con una red inalámbrica que cubre todo el campus universitario brindando respaldo a la red alámbrica, permitiendo el acceso a Internet para dispositivos móviles desde cualquier punto de la Universidad a una velocidad de 54 Mbps.

La UFPS Ocaña tiene un acceso a la red Internet a través de un canal dedicado contratado con la empresa de Telecomunicaciones de Bogotá S.A. - ETB de 92160 Kbps con reusó (1:1) para la sede principal, otro en la sede la primavera de 16384 Kbps para la emisora UFM Estéreo, y 4096 Kbps para la sede de Bellas Artes, con Movistar 30720 Kbps y 100 Mbps de canal de datos con reusó (1:1) para el servicio de UNIRED - RENATA.

La universidad adquirió una antena para recibir y transmitir vía microondas, la cual tiene línea de vista con las antenas de propiedad del Grupo ISA (a través de su filial Internexa), que permite conectarse a la fibra óptica nacional y a su vez al Sistema de Cable Submarino Arcos.

Con la adquisición del canal dedicado se ha implementado acceso pleno a la Web para todas las salas de cómputo y las dependencias de la universidad, el correo electrónico para Docentes, Alumnos y Administrativos (8000 cuentas de correo almacenadas en los servidores de Google) y se ha instalado un servidor Web que presenta la Universidad a la comunidad Internet, a través del enlace **http://www.ufpso.edu.co**. También se han implementado otros servicios que benefician a la comunidad estudiantil como la consulta de la información académica de los alumnos, la plataforma virtual, la emisora en Real Audio.

Actualmente se encuentran funcionando los siguientes servicios de red:

Resolución de nombres de Internet – DNS. Servicio esencial de red que administra los nombres de dominio de Internet.

Resolución de nombres de Intranet – WINS. Servicio de red esencial para redes con estaciones de trabajo Microsoft Windows 9x.

Correo electrónico institucional. A través de este servicio, los miembros de la comunidad universitaria pueden obtener su cuenta de correo de la forma usuario@ufpso.edu.co. Actualmente y utilizando uno de los servicios de Google se dispone de 8000 cuentas de tipo Gmail aproximadamente. A nivel de la intranet se usa el servicio de mensajería instantánea Google Talk.

Hosting – WWW. Los miembros de la comunidad universitaria puede usar este servicio para publicar su sitio Web de la forma sitio.ufpso.edu.co. Actualmente, el sitio más grande que se aloja es el del portal http://www.ufpso.edu.co. Además, es posible ofrecer el servicio de alojamiento para otros dominios diferentes, siempre y cuando sea con fines institucionales.

Transferencia de archivos – FTP. El servidor ftp de la Universidad mantiene tanto software como documentos de interés para toda la comunidad universitaria, los que se pueden descargar desde cualquier computador dentro o fuera del campus.

Acceso a Internet. Actualmente, la Universidad accede a Internet a través del proveedor de servicios de Internet ETB. Este servicio deriva los siguientes:

- Gestión de direcciones IP reales
- Gestión de ancho de banda usando squid
- Navegación en Internet a través de Proxy
- Muro cortafuegos o Firewall como medida de protección para seguridad de la red.

Central Telefónica. La universidad cuenta con una central telefónica de tecnología digital, para interfaces analógicas y digitales, habiéndose activado 155 puntos telefónicos en todo el campus universitario. 1 (Actualmente ya existen dos centrales telefónicas funcionando: la anterior mencionada y otra en la sede Primavera)

Telefonía IP. La Universidad incursiona en el servicio de telefonía IP que permite realizar llamadas desde redes que utilizan el protocolo de comunicación IP (Internet Protocol), es decir, el sistema que permite comunicar computadores de todo el mundo a través de las líneas telefónicas. Esta tecnología digitaliza la voz y la comprime en paquetes de datos que se reconvierten de nuevo en voz en el punto de destino.

Plataforma Virtual – Uvirtual. La Universidad Francisco de Paula Santander Ocaña cuenta con una plataforma Virtual soportada sobre la herramienta de software libre Moodle, actualmente la plataforma virtual se utiliza como acompañamiento a las clases presénciales que se imparten dentro de la Institución, en ella se pueden realizar las diferentes actividades que facilita la plataforma. Su objetivo es dar apoyo a la educación presencial, actuando como una herramienta que contribuye en mejorar la dinámica de enseñanza ofreciendo otra alternativa metodológica; lo que se busca es lograr que la práctica pedagógica inicie un proceso de inmersión en el uso de las TIC y se logre contacto con los ambientes virtuales de aprendizaje y los recursos didácticos que ellos ofrecen.

Actualmente se está capacitando a los docentes tanto catedráticos como de tiempo completo en el uso de tecnologías Web 2.0 para la enseñanza, paralelamente dentro de

estas capacitaciones se incluye el uso y aplicación de la plataforma Uvirtual, de igual manera se cuenta con disponibilidad para la orientación de los docentes en el uso de la plataforma virtual.

Moodle fue creada con un enfoque constructivista social, los recursos de TIC utilizan mucho este modelo pedagógico, porque cuando se interactúa con la máquina, con un sistema operativo, con un sistema de información, una red social, entre otros, el usuario va adquiriendo conocimiento a medida que actúa con el entorno, entonces esto contribuye a que el usuario se arriesgue a utilizar la herramienta, pero adicionalmente en la plataforma hay un instructivo para los docentes y se les ofrece soporte.

Real Audio para la Emisora la Ufm Stereo. Este servicio permite a toda la comunidad universitaria y a todos los ocañeros escuchar la emisora UFM Stereo en vivo a través de la página principal utilizando el real audio: http://laufm.ufpso.edu.co/

UTV. Este servicio permite utilizar video por demanda para visualizar los videos de las secciones que componen el programa "Conexiones", un magazín de ciencia, tecnología, academia y vida universitaria producido por la Universidad Francisco de Paula Santander Ocaña a través de la UTV: http://www.ufpso.edu.co/conexiones/video.html

Video por IP y Cámaras de vigilancia. Este servicio permite monitorear las salas de cómputo utilizando cámaras IP, para un mejor uso y administración de la seguridad de las salas. También se encuentran instaladas dos cámaras de video vigilancia en el campus universitario.

Biblioteca digital Dspace. La biblioteca consiste en múltiples repositorios de documentos digitales. El contenido de la biblioteca actualmente son trabajos de grado de pregrado, posgrado, seminarios, manuales y apuntes que son que son realizados por los estudiantes y profesores de la Universidad Francisco de Paula Santander Ocaña. Los sitios de la Biblioteca Digital son los siguientes: Biblioteca Digital UFPS Ocaña: http://bibliotecadigital.ufpso.edu.co/

Hosting Colegios. Este servicio permite a los colegios en convenio con la universidad alojar sus sitios Web y utilizar un aplicativo Web para el manejo de la información académica de las instituciones educativas: http://web.ufpso.edu.co/

SNIES. Este servicio permite ingresar y administrar la información en línea para el SNIES - Sistema Nacional de Información de la Educación Superior del Ministerio de Educación Nacional: http://snies.ufpso.edu.co:8080/PortalIES/

Laboratorio de Radio y Televisión. Estos dos laboratorios están asociados al plan de estudios de Comunicación Social y están orientados a la producción de material por parte

de los estudiantes y que se publican en la emisora, el programa televisivo Conexiones y el circuito cerrado de televisión (CCTV).