PROPUESTA DE MEJORAMIENTO CONTINÚO DE LA SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR

ERIKA VIVIANA BONILLA BONILLA

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
DIVISIÓN DE INGENIERIAS
BOGOTÁ D.C.
2019

PROPUESTA DE MEJORAMIENTO CONTINÚO DE LA SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR

ERIKA VIVIANA BONILLA BONILLA

Monografía

Director:

Ing. Fernando Prieto Bustamante

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
DIVISIÓN DE INGENIERIAS
BOGOTÁ D.C.
2019

TABLA DE CONTENIDO

TABLA DE TABLAS

TABLA DE ILUSTRACIONES

INTRODUCCIÓN

Durante el desarrollo de este documento se hará mención de las diferentes problemáticas relacionadas con seguridad informática y seguridad de la información que se presentan dentro de las organizaciones específicamente en las Instituciones de Educación Superior (dentro de este documento se hablara de ellas como IES) y con esto finalmente poder plantear una propuesta que permita mediante la aplicación de algunos marcos de referencia mitigar y controlar cada uno de los riesgos identificados.

Adicionalmente se hace una breve descripción de algunos términos relacionados con seguridad informática y de la información esto para que sea de fácil comprensión y permita robustecer los conocimientos que se tengan en cada uno de estos temas , como lo son los marcos de referencia ITIL en su versión número tres, COBIT en su versión número cinco e ISO 27001, en cuanto al primero de ellos es una guía de buenas prácticas que gira entorno a aspectos como la calidad y eficacia de los servicios de TI, COBIT por su parte realiza un aporte en la gestión y gobernanza dentro de la organización sin dejar a un lado que su foco son las organizaciones cuyos activos y recursos descansan sobre TI.

La investigación que soporto este trabajo fue llevada a cabo con un análisis cualitativo a partir de experiencias ocurridas dentro de diferentes Instituciones de Educación Superior, para esto se realizaron entrevistas y encuentros con los directores de los departamentos de TI, se omitirá el nombre de las IES y del personal que orto la información para evitar algún agravio o incomodidad con las partes.

Estas entrevistas fueron guía de análisis, desarrollo y definición de problemáticas, con esto se puede consolidar y proponer una solución eficiente de manera general, para esto se realizó un análisis y se determinó una propuesta que permita trabajar de manera robusta con los diversos marcos mencionados anteriormente, tomando de cada uno de ellos los aportes más relevantes.

1. MARCO GENERAL DEL PROYECTO

1.1. PLANTEAMIENTO DEL PROBLEMA

La información es el activo más importante que posee una organización, dentro de una Institución de Educación Superior (IES) se encuentran diversas bases de datos que contienen información de todo el personal que se relaciona con ella de diversas maneras; reportes académicos de gran número de estudiantes, información personal de estudiantes y administrativos ,investigaciones, datos de proveedores o socios, diversos datos que son delicados como nombres de usuario y contraseñas con las que se pueden realizar modificaciones en códigos fuentes de programas , atacar otros equipos y redes , bloquear el sistema de información que puede conllevar a la pérdida total o parcial de la información .

Dentro de los sistemas de información que son implementados por las universidades se identifican algunas vulnerabilidades a nivel físico, es decir, en la infraestructura que es utilizada y en los niveles de seguridad de los activos, con esto se puede hacer distinción entre la seguridad informática y la seguridad de la información.

Dentro de las sugerencias y medidas que se deben adoptar por parte de las universidades para la protección de los sistemas informáticos se tiene; implantar políticas de seguridad, uso de antimalware en todos los equipos pertenecientes a la red y un firewall en la puerta de enlace y en los equipos pertenecientes a la institución, ya que estos son de uso de docentes, estudiantes e incluso personal ajeno a la universidad, uso de contraseñas complejas , es decir, que posean diversos caracteres y que estas sean cambiadas periódicamente, hacer uso de redes virtuales privadas (VPN) ya que para conectar usuarios es una excelente medida que garantiza que la información sea compartida únicamente con quién corresponde , realizar la actualización de los softwares que se encuentran en uso, debido a que es posible acceder al sistema de manera silenciosa mediante las vulnerabilidades que existen en los sistemas operativos y programas instalados en los diferentes equipos, realizar copias de seguridad en la nube periódicamente como un complemento, es decir , las copias que se realizan en otros equipos como respaldo deben realizarse igualmente , proteger los puertos de cada equipo que se encuentre siendo usado, verificar que las paginas sean legítimas para evitar “Phising” y finalmente sugiere la criptografía , como medida para mantener información sensible secreta.

Dentro de los factores de riesgos en los sistemas de información se encuentra los cuidados y vigilancia del software, mejora en los sistemas de los cuales se hace uso, garantía del servicio y operatividad de la compañía, seguridad lógica en plataforma computacional y seguridad física en la infraestructura y elementos pertenecientes a esta.

Para dar solución a estas problemáticas se pretende mediante la revisión de dos marcos de referencia como lo son COBIT, ITILv3 e ISO27001 generar una propuesta de mejora continua que permita que estos riesgos se mitiguen y puedan ser gestionados de la mejor manera para las Instituciones de Educación Superior.

1.2. JUSTIFICACIÓN

Debido a que la información es el activo más importante dentro de cualquier compañía, como puede ser una Institución de Educación Superior; esta maneja grandes cantidades de información relacionada con muchas personas y diferentes aspectos. De aquí la importancia de identificar periódicamente que problemáticas se presentan y cómo dar solución a ellas. Cuando se logra establecer los diferentes tipos de riesgos a los que se ve expuesta la Institución es mucho menos complejo aplicar una solución a estas, por esto mismo es necesario generar estrategias aplicando conocimientos eficaces en diversos entornos y que anteriormente en otras Instituciones y compañías han sido de éxito.

En este caso específico se estudiaron y analizaron algunos marcos de referencia para la realización de este documento, los cuales se han podido comprobar y determinar como una propuesta confiable gracias a las metodologías y recursos que estos adoptan, han sido implementados en la dirección de grandes compañías llevándolas hacia el correcto funcionamiento y con esto al éxito.

Las prácticas que emplean COBIT, ITILv3 e ISO270001 permiten que la compañía desde el inicio marche en forma, adicionalmente permite la optimización de recursos, gestionar los riesgos, la calidad y sobre todo alinear los objetivos de la compañía con las tecnologías de la información.

1.3. OBJETIVOS

1.3.1. Objetivo General

Desarrollar una propuesta para el mejoramiento continuo de seguridad informática y de la información en Instituciones de Educación Superior basado en COBIT, ITILv3 e ISO27001.

1.3.2. Objetivos Específicos

- Identificar las principales problemáticas presentes en los sistemas de seguridad informática y de información de las Instituciones de Educación Superior.

- Definir los principales requerimientos necesarios para fortalecer la seguridad informática de las Instituciones de Educación Superior**.**

- Analizar los principales procesos de los diferentes marcos de seguridad de la información, gestión y gobierno de TI que impactan en la operación del área de tecnología en las Instituciones de Educación Superior

.

- Establecer una propuesta para el mejoramiento continuo de seguridad informática y de la información en Instituciones de Educación Superior basado en COBIT, ITIL v3 e ISO27001.

1.4. ALCANCE

De acuerdo al título y el objetivo general planteado para el desarrollo de este documento se busca establecer una propuesta de mejoramiento continuo de la seguridad informática para las redes de Instituciones de Educación Superior, a partir de la identificación de las problemáticas que se presentan a nivel de seguridad de la información e informática, las cuales serán mitigadas y por la cuales se planteara la adopción de dos marcos de referencia para la gestión y prestación de servicios de TI.

1.5. MARCO TEÓRICO

1.5.1. Conceptos claves

- ✓ Gestión, se puede reconocer como todo proceso donde se llevan a cabo diligencias para permitir la realización de una operación o proyecto. Tiene como objetivo primordial aumentar los resultados óptimos dentro de una compañía. [Pérez Porto Julián, 2012].
- ✓ Herramientas, en el ámbito comercial y empresarial hace referencia a aquellos instrumentos que permiten ya sea tangibles o no que al ser usados permiten llevar a cabo un proyecto y se encuentran direccionados a conseguir un objetivos. [Merino María, 2013].
- ✓ Servicio, es considerado como la acción o bien que satisface una necesidad especifica establecida por un cliente, a cambio de una redistribución económica. [Sánchez Galán Javier, 2019]
- ✓ Incidente, es toda aquella acción o evento que interviene el transcurso normal de una situación. Puede ser una o múltiples situaciones, y en algunos casos obligan a reprogramar las actividades que se debieron suspender. [Ucha Florencia, 2011].
- ✓ Disponibilidad, término que expresa que un producto, elemento o servicio puede ser utilizado por personas [Bembibre Cecilia, 2010].
- ✓ Riesgo, Evento de exposición de un activo ante una amenaza que en caso de efectuarse puede causar efectos negativos. Es lo que puede ocurrir cuando los activos no son protegidos de manera correcta. [Universidad Veracruzana, 2017]
- ✓ Amenaza, Es un evento negativo que al consumarse puede provocar un incidente afectado los sistemas y activos. [Universidad Veracruzana, 2017].
- ✓ Vulnerabilidad, Cuando un sistema se presume débil y puede ser afectado por una o más amenazas. [Universidad Veracruzana, 2017].
- ✓ Impacto, Cuando se efectúa una amenaza sobre un activo o sistema. [Universidad Veracruzana, 2017].
- ✓ Tratamiento de datos personales, Cuando se opera o manipula mediante procesos automatizados, manuales, mecánicos o electrónicos los datos o sistema de datos con información personal. [Universidad Veracruzana, 2017].

1.5.2. Seguridad informática

La seguridad informática es considerada como el mecanismo adoptado para evitar que un sistema informático sea violentado, es decir, cumple la función de adoptar medidas y técnicas para el correcto funcionamiento y protección de la infraestructura.

Se destacan aspectos influyentes como:

Ilustración 1. Seguridad en los sistemas informáticos
Fuente: Elaboración propia

1.5.2.1. Tipos de Seguridad Informática

1.5.2.1.1. Seguridad Online

Existen algunos delitos en la red como lo son los virus, los robos de identidad, las intrusiones ilegales, entre otros, para estos eventos existen algunas medidas que permiten mejorar la seguridad en la red de manera sencilla y eficiente como lo son los antivirus, los antispyware, cortafuegos e incluso las VPN. [OBS Bussines School, 2019].

Todas estas herramientas tienen como finalidad brindar mayor protección a las redes y evitar el ingreso de amenazas que pueden afectar al correcto funcionamiento de esta, aunque se recomienda manejar diversas estrategias como lo son el manejo de diversos niveles de seguridad. [OBS Bussines School, 2019].

1.5.2.1.2. Seguridad de Software

Hasta hace algunos años e software no era un aspecto importante para tomar en consideración cuando se habla de seguridad informática pero esto cambio cuando se evidencio que los fallos en este pueden repercutir y afectar los sistemas y permitir el ingreso de ciberdelincuentes. Las herramientas creadas para proteger el software fueron establecidas hace poco tiempo pero son necesarias en asuntos como la implementación del mismo e incluso en los errores de diseño. [OBS Bussines School, 2019].

1.5.2.1.3. Seguridad de Hardware

Los fabricantes alrededor del mundo han establecido que es necesario tomar medidas para garantizar la seguridad por eso fueron creados los cortafuegos, firewalls de hardware y los servidores de proxy. Las herramientas mencionadas anteriormente tienen como finalidad controlar el tráfico que viaja a través de la red. [OBS Bussines School, 2019].

Otro factor en el que se debe hacer énfasis son los módulos de seguridad de hardware HMS cuyo uso es proteger el cifrado. La seguridad de hardware es de las más complejas ya que busca en todo momento proteger los equipos informáticos.

1.5.2.2. Planos de actuación de la seguridad informática

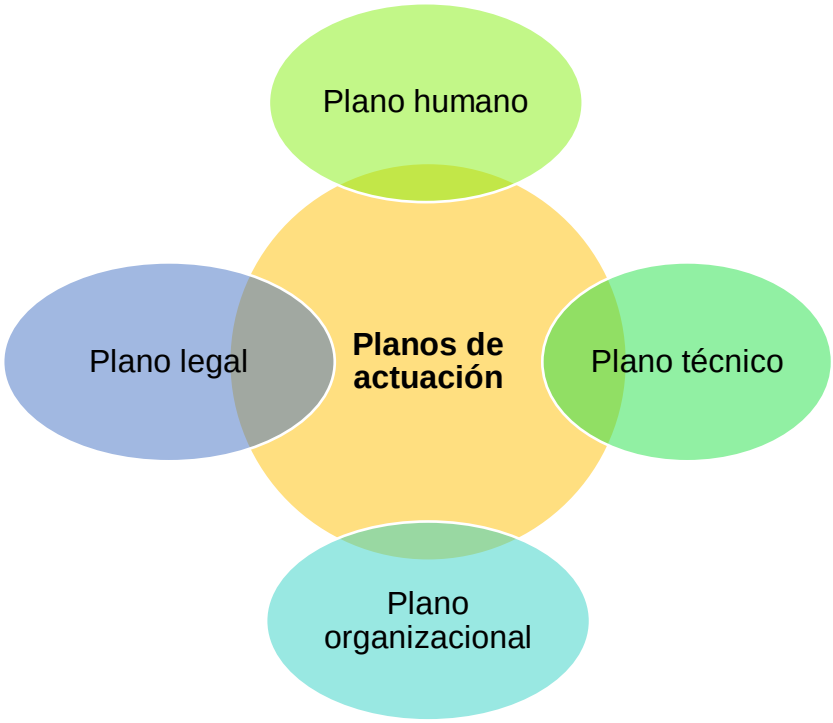

Ilustración 2. Planos de actuación de la seguridad informática
Fuente: Elaboración propia

- ✓ Plano humano: Concientización y formación de empleados supervisión de empleados, determinar funciones y deberes del personal
- ✓ Plano técnico: instalación, configuración, selección, actualización de hardware y software a nivel físico y lógico.
- ✓ Plano organizacional: Regulación, políticas y procedimientos, planes de contingencia y soluciones a problemáticas.
- ✓ Plano legal: Velar por el cumplimiento de las normativas vigentes así como de la adaptación de las mismas.

1.5.3. Seguridad de la información

La seguridad de la información engloba todas las estrategias y medidas que se deben adoptar para proteger los datos, los cuales pueden encontrarse de manera física o digital. Estas estrategias son implementadas y necesarias en diferentes dimensiones como:

- ✓ La confidencialidad que garantiza que solo el personal autorizado es quien manipula y accede a los recursos.
- ✓ La disponibilidad que facultara a determinados usuarios a que acceden a la información de manera oportuna.
- ✓ La integridad que se estipula como la propiedad de mantener la información correcta

Según ISO27001 la seguridad de la información se encarga de proteger los datos de la organización independientemente del tipo de formato en el que se encuentren consignados, estos pueden ser electrónicos, papel, audio y video, entre otros.

1.5.3.1. Elementos de la Seguridad de la Información

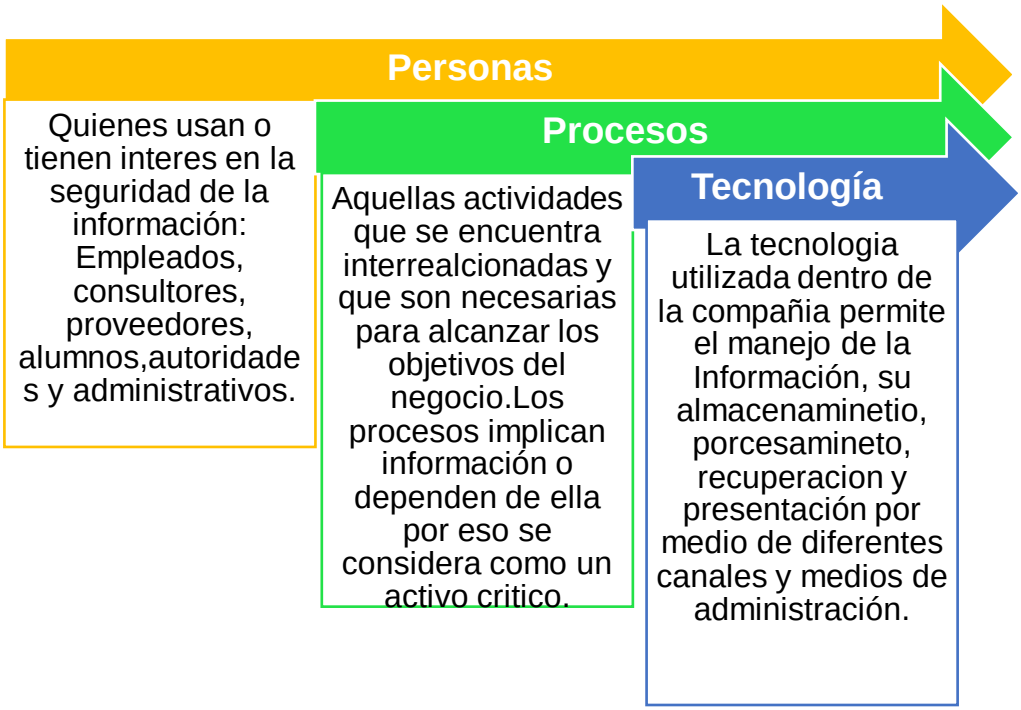

Ilustración 3. Elementos de la Seguridad de la Información
Fuente: Elaboración propia

1.5.3.2. Activos de la Seguridad de la Información

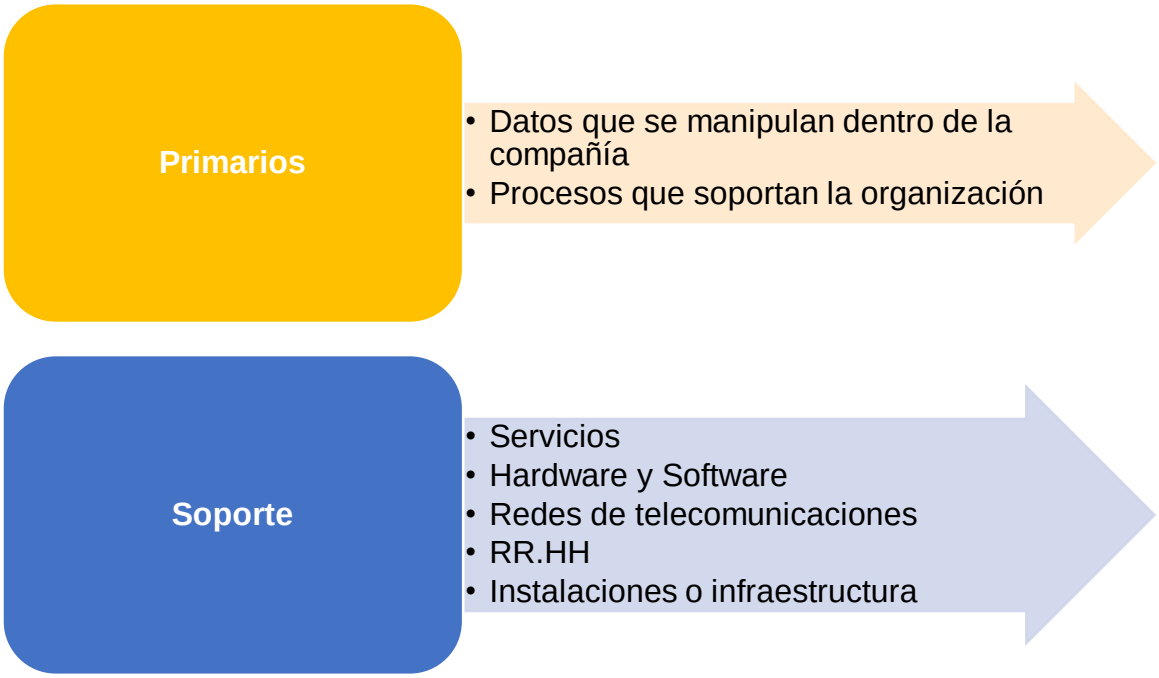

Ilustración 4. Activos de la Seguridad de la Información
Fuente: Elaboración propia.

1.5.4. Marcos de referencia

Son considerados como la herramienta principal para poder llevar a cabo la implementación de la arquitectura de TI a nivel mundial y de igual manera permitir que se realice la habilitación de estrategias para los servicios, la gestión, el gobierno, seguridad y privacidad dentro de las organizaciones que se encuentran logadas al sector de la TI.

Los marcos de referencia están basados en una serie de lineamientos cuyo objetivo es llevar a las compañías al cumplimiento de todos y cada uno de sus objetivos. Entre los antecedentes ITIL ha sido el mayormente acogido para la gestión de servicios de TI, aproximadamente desde los años 70's, aunque este no es el único también son de gran conocimiento y trayectoria COBIT que se encuentra un poco más enfocado hacia el control de los proyectos de TI y los riesgos que estos pueden implicar, CMMI enfocado hacia los servicios y como aplicar mejoras practicas dentro de la organización, MOF, ISO/IEC, eTOM entre otros.

Dentro de la metodología propuesta para el desarrollo de este proyecto se pretende realizar la aplicación de dos de los marcos mencionados en el grupo

inmediatamente anterior, los cuales son ITIL, COBIT e ISO270001 los cuales serán tratados de forma un poco más profunda a continuación.

1.5.5. COBIT

Objetivos de control para la información y la tecnología relacionada, tiene como funcionalidad controlar y gestionar las TI a través de un modelo de Gobierno de TI como pauta para diversas empresas del sector.

En este marco se encuentra un gran número de lineamientos que permiten realizar la Gestión de diversas áreas de la organización. COBIT se encuentra compuesto básicamente por cuatro grandes procesos y por treinta y cuatro subprocesos que permiten que con este marco se puedan tratar temas referentes a la eficiencia, disponibilidad, calidad e integridad, entre muchos más.

Cada proceso busca el cumplimiento de las actividades clasificadas como prioritarias, buscando el uso eficiente y optimizado de los recursos para alcanzar las metas previamente establecidas, a esto se le conoce como planear y organizar.

Dentro del proceso adquirir e implantar el ideal es la clasificación, adquisición y mantenimiento de los recursos tecnológicos para posteriormente ser utilizados en cada uno de los procesos de la organización.

El proceso de entregar y brindar soporte tiene básicamente la misión de salir y poner en marcha los servicios ofertados y adquiridos por el cliente y así mismo brindar garantía de soporte sobre lo pactado.

Y por último se encuentra monitorear y enviar que pretende hacer un seguimiento y control de los diferentes sectores y componentes tecnológicos que se encuentran en la organización.

1.5.6. ITIL V3

Es el marco de referencia con mayor uso nivel mundial, este marco de referencia busca establecer las mejores prácticas para la gestión de servicios de tecnologías de la información haciendo uso de un conjunto de funciones y procesos que permitan que la organización alcance el éxito y eficiencia en cada una de sus operaciones.

ITIL v3 está compuesto por 5 libros, en el que se consolida el modelo de “Ciclo de Vida del Servicio”, conformado de la siguiente manera:

Ilustración 5. Ciclo de vida de ITIL v3
Fuente: http://issuu.com/biable_mei/docs/manual_itil_integro_para_publicaciones_cc

1.5.6.1. Estrategia del servicio

En esta sección del libro lo que se busca es identificar y establecer las necesidades a las que se quiere brindar solución, ya que de esto se parte para fijar los objetivos estratégicos y las políticas que se deben seguir para una correcta gestión. Aunque sin dejar de lado el mercado en el que se pretende impactar, esta es la raíz para garantizar un servicio adecuado y eficiente.

La estrategia del servicio se compone de cuatro aspectos según lo formulo Henry Mintzberg en su ciclo de las 4 P's.

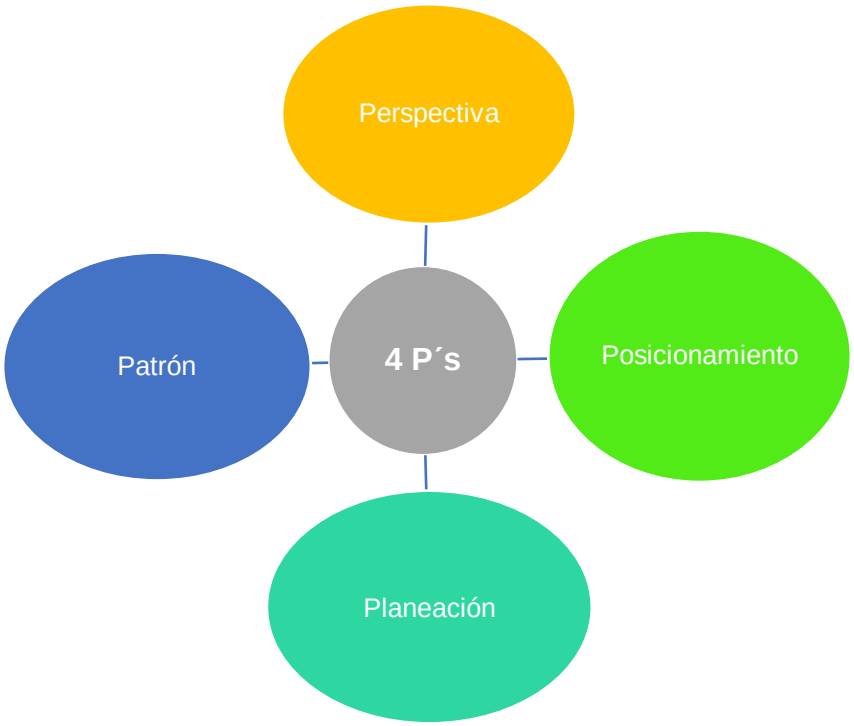

Ilustración 6. 4P´s
Fuente: Elaboración propia

- ✓ Perspectiva, se debe establecer como se espera que sea el servicio en un futuro determinado y cuál es el objetivo de este en relación con cada uno de los actores que se relaciona con este.
- ✓ Posición, hace referencia al bien o servicio que se pretende ofertar, ya sea con un único servicio o por el contrario con un amplio portafolio. Este servicio debe ser diferenciador y de calidad.
- ✓ Planificación, es ideal establecer etapas y funciones, cuando se logra controlar y actuar de manera eficiente es posible que los servicios de TI dentro de la Institución sean de acuerdo a lo pautado con el cliente y sobretodo permitiendo una optimización en cada uno de los recursos.
- ✓ Patrón, se debe seguir de manera secuencial los procedimientos realizados anteriormente que han sido exitosos.

1.5.6.2. Diseño del servicio

Se estudian las políticas necesarias que orienten el negocio hacia el producto que se quiere entregar, de igual manera se identifican los recursos que se emplearan y los requerimientos que se deben cumplir para satisfacer las necesidades establecidas.

En esta parte del ciclo se deben tener en cuenta aspectos tales como el mercado y la solución objetivo, definición de procesos, mecanismos de control de calidad del servicio.

En el diseño del servicio encuentran diversos sectores que intervienen de manera dinámica para culminar con este.

Ilustración 7. Actores y sectores participantes en el diseño del servicio
Fuente: Elaboración propia

1.5.6.3. Transición del servicio

Cuando se pretende modificar o integrar un servicio novedoso es necesario supervisar que este sea eficiente y brinde la calidad que cada uno de los clientes espera, de manera que se mitiguen los riesgos de implementación, la capacidad y los recursos de los que demanda para que el cumplimiento y disponibilidad no se vean afectados. Cuando se realizan cambios en el servicio es primordial tener en cuenta que estos se deben registrar, analizar, aceptar o declinar según sean pertinentes, priorizar o postergar, planear, testear, implementar, documentar y supervisar.

Se deben gestionar estas configuraciones, de esto se tiene:

- ✓ Sistema de Gestión de la configuración CMS: Acá se almacena y gestiona todo lo referente a incidentes, problemas y cambios.
- ✓ Sistema de Gestión de la configuración CMDB: Son bases de datos más robustas que guardan los registros de los elementos de configuración.

- ✓ Sistema de Gestión del conocimiento del servicio SKMS: Almacena los documentos de los procesos, los roles de la compañía y toda la información necesaria para la gestión del servicio.

1.5.6.4. Operación del servicio

El usuario recibe finalmente el servicio por el que ha pautado según los acuerdos de nivel de servicio (SLA), debido a esto hay que tener en cuenta que se debe cumplir con los procesos de ejecución y dar seguimiento del servicio que está percibiendo el usuario final, sin dejar de lado la gestión de riesgos e incidencias con lo que se pretende que estas no se presente nuevamente y la mejora continua sea un proceso eficaz y marche según los objetivos de TI de la Institución.

1.5.6.5. Mejora continua del servicio

Está ligada directamente a cada una de las fases anteriores del ciclo, acá se analiza los procesos y políticas para cada servicios y los cambios que se deben realizar para que el cliente tenga una percepción de que el servicio y su calidad se mantiene. Los cambios que se realizan deben ser enfocados en las necesidades del negocio que permitan que este mejore de manera significativa

En el ciclo de Deming se establecen cuatro aspectos importantes para la mejora continua de los procesos.

Ilustración 8. Ciclo de Deming
Fuente: Elaboración propia

1.5.7. Los 7 pasos de mejora continua

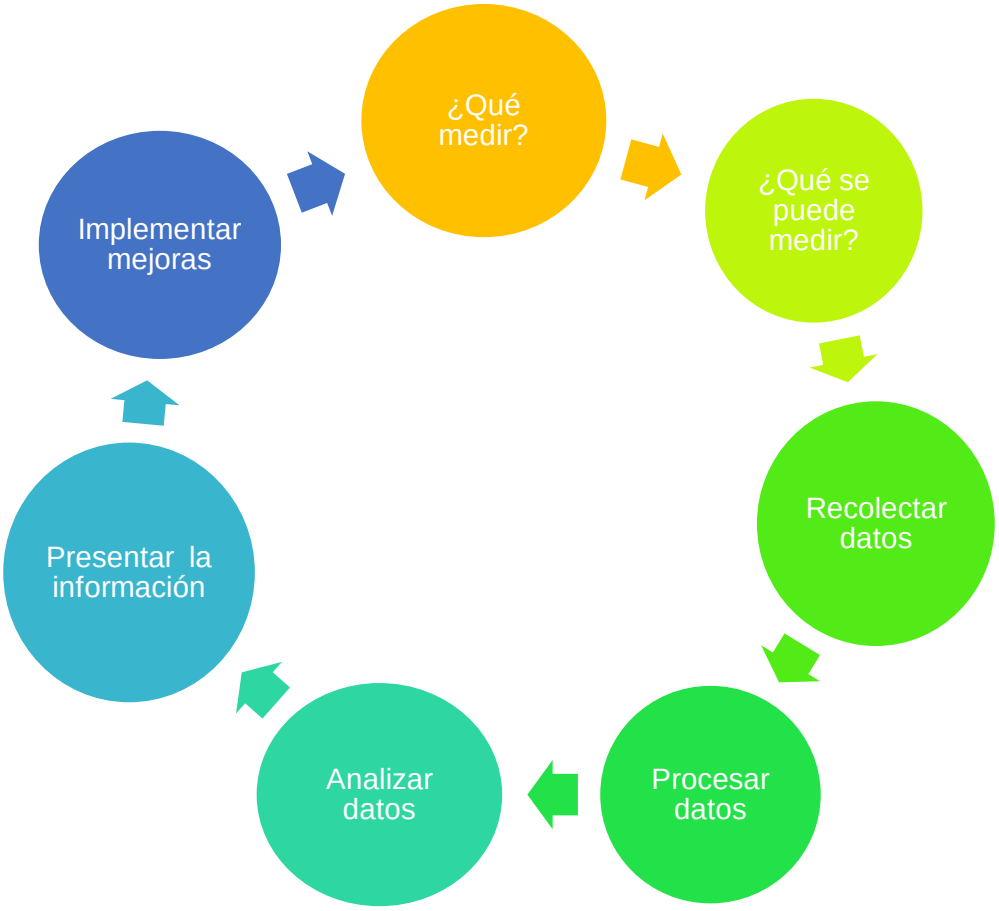

Ilustración 9. Siete pasos de mejora continúa
Fuente: http://itilenespanol.blogspot.com/2015/05/072-mejora-continua-del-servicio.html

1.5.7.1. ¿Qué se debe medir?

A partir de esta pregunta se debe identificar qué estrategia seria la ideal para alcanzar los objetivos de cambio y mejora que se encuentran enfocados con la visión del negocio.

Este paso debe ser revisa con frecuencia ya que es necesario verificar la alineación de los objetivos con el negocio. Se pueden tener algunos indicadores que permitan establecer como se encuentra el proceso de mejora. Entre estos esta la realización de planes estratégicos de negocio, reuniones donde se revise el servicio, analizar el cumplimiento de los requerimientos legislativos, controles de gobierno corporativo y encuestas a los clientes para analizar la percepción del servicio. [Giraldo Juan, 2015].

1.5.7.2. ¿Qué se puede medir?

En este paso se establece que se puede medir de acuerdo a los servicios que se ofertan para a partir de esto establecer que deficiencias se presentan y generar un plan de acción y mejoramiento.

Se deben realizar mediciones que arrojen resultados cuantitativos y cualitativos, los resultados deben ser claros y permitir identificar si se genera valor para el cliente por eso debe recurrir a indicadores como SLA's , revisión del catálogo de servicios, ciclo del presupuesto, datos de benchmarking y planes para la mitigación de los riesgos. [Giraldo Juan, 2015].

1.5.7.3. Recolectar datos

Se debe realizar un monitoreo de los servicios, los procesos y la tecnología implementada. En este paso se debe definir quien realizara la recolección de los datos, la frecuencia con la que se recolectara y monitoreara, comunicar a todas las partes acerca del desarrollo, actualizar los planes de cómo se realizara la recolección y como se evaluaran. [Giraldo Juan, 2015].

1.5.7.4. Procesar datos

La información captada con anterioridad deberá ser llevada a un formato de comprensión global.

En este paso se realizara el análisis mediante técnicas establecidas con anterioridad, aunque se debe considerar la frecuencia con la que se realizara el procesamiento, las herramientas para procesarlos y las técnicas de evaluación. Se puede n manejar los listados de métricas, SLAs, CSF como indicadores. [Giraldo Juan, 2015].

1.5.7.5. Analizar datos

Se debe conocer el contexto ya que esta es uno de los pasos más complejos e importantes. Para el análisis se debe tener en cuenta si se responde a las siguientes preguntas: ¿Se encuentra como se había planeado? Esto respecto a un plan de proyecto, a la gestión de disponibilidad, continuidad y capacidad, ¿se está cumpliendo con los SLAs? , ¿Se debe realizar una mejora?, ¿Existen tendencias?, ¿Son positivas o negativas? [Giraldo Juan, 2015].

1.5.7.6. Presentar de la información

Se debe exponer los resultados de cada etapa, es decir, los reportes de monitoreo, encuestas, planes de acción y mejora, entre otros.

En este paso se debe tener en cuenta los tipos de interesados a los que va dirigida la información, entre ellos se encuentran los clientes, quienes reciben información

acerca de los servicios y atención oportuna cuando estos fallen, los gerentes de TI, quienes deben de analizar el desempeño, el departamento de TI que analizan las métricas y ayudan a coordinar y diseñar las estrategias de mejora continua y los proveedores quienes vela por las actividades relacionadas con los productos que proveen. [Giraldo Juan, 2015].

1.5.7.7. Implementar las mejoras

En esta etapa se debe actuar respecto a los resultados y la experiencia adquirida sobre la toma de decisiones. Esta etapa puede estar relacionada con otras etapas del ciclo de vida de un servicio. Cuando se decide poner en marcha la implementación de las mejores se comunica a la organización para alcanzar una mejora eventual y completa.

Al finalizar la implementación se debe realizar un registro de lo la situación inicial y final. [Giraldo Juan, 2015].

1.5.8. Bases legales

Ley 1581 de 2012

Esta ley se reglamentó hacia el año 2012, se encuentra compuesta por un total de 28 artículos, y considera Sobre el manejo, tratamiento y autorización de los datos personales.

"(…) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma" 1.

1. Ministerio de Comercio, Industria y Turismo, Decreto Número 1377 de 2013, pg.1.

A continuación se realizara una breve conceptualización de algunos de los términos y artículos de este decreto que se encuentran ligados directamente con la integridad de la información.

Según se dispone en el artículo 3 algunas definiciones que deben ser consideradas en el efecto de la ley como lo son:

Aviso de privacidad, en el que se entiende que el titular debe ser anunciado acerca de la forma y la finalidad de usar su información así como la responsabilidad y acuerdo moral del uso de estos.

Dato público, son aquellos que pueden ser consultados y acceder a estos desde bases públicas, se encuentran contenidos allí debido a la calidad de ciudadano.

Datos sensibles, son aquellos que transcienden en el campo íntimo y negativamente pueden ser utilizados como factores discriminantes, como la raza, grupo étnico, religión e incluso inclinación sexual.

Transferencia, Cuando el responsable comparte los datos con alguien fuera o dentro de la misma nación.

Transmisión, Cuando el responsable de los datos debe realizar tratamiento de los datos independientemente de su ubicación.

En el artículo 4 se habla acerca de la recolección de los datos y se menciona que deben ser únicamente por personal autorizado y se debe cumplir con la finalidad informada. Según la Superintendencia de industria y comercio los responsables de la recolección deben dejar claro cada uno de los procesos y procedimientos que se realizaran y de igual manera no se deben utilizar medios engañosos para recolectar la información.

En el artículo 5 referente a la autorización es decir, el tratante de los datos en el momento de la recolección de los datos deberá pedir la autorización para el uso de estos y de igual manera informar en el futuro acerca de cambios o modificaciones en estos.

En el artículo 6 se habla del tratamiento de los datos sensibles y que esto debe ser informado al titular ya que por ser de esta naturaleza no se encuentra en la obligación de aceptar.

Los artículos faltantes engloba temáticas relacionadas con las políticas del tratamiento de datos, la legitimación y la responsabilidad frente a su uso.

1.6. METODOLOGÍA

Con la finalidad de identificar las problemáticas que se encuentran relacionadas con la seguridad informática y de la información para las redes de Instituciones de Educación Superior se realizó una investigación a nivel nacional e internacional de cuales han sido aquellos aspectos que se han propiciado problemáticas y fallas en el correcto funcionamiento de las redes y así mismo se identificó cuáles de estos están ligados con la parte de hardware y software. De igual manera a raíz de la identificación de las fallas y errores muchas de las fuentes en sus portales y a través de su experiencia hacen mención de algunas de las medidas que tomaron posteriormente no solo para subsanar y remediar las situaciones desfavorables sino adicionalmente para reducir la posibilidad de ocurrencia de las mismas u otros factores negativos.

Posteriormente se realiza el análisis de diversos marcos de referencia de los cuales se eligen algunos que aunque tienen un foco levemente diferente es posible abarcar de manera completa las problemáticas y a partir de la composición de cada uno de ellos determinar qué aspectos específicamente se pueden abordan, realizando una comparación del estado inicial, es decir el problema, como al aplicar determinado marco de referencia se puede dar un tratamiento a este teniendo así un estado final, es decir, una solución.

La solución propuesta en este documento se dio a través de los diversos marcos de referencia utilizados a nivel mundial, con el objetivo de mitigar los riesgos y problemáticas que de mano del departamento de TI de la Universidad Santo Tomás se pudieron establecer, estas problemáticas no son únicamente a nivel de infraestructura algunas de ellas tienen su origen en falta de planeación, en un rezago tecnológico, en la falta de capacitación del personal, entre otros.

De todo lo anterior se puede concluir que este documento se abordó desde una metodología netamente cuantitativa, partiendo de casos reales tanto a nivel nacional como internacional y los cuales fueron estudiados de manera profunda para poder ser considerados una fuente confiable.

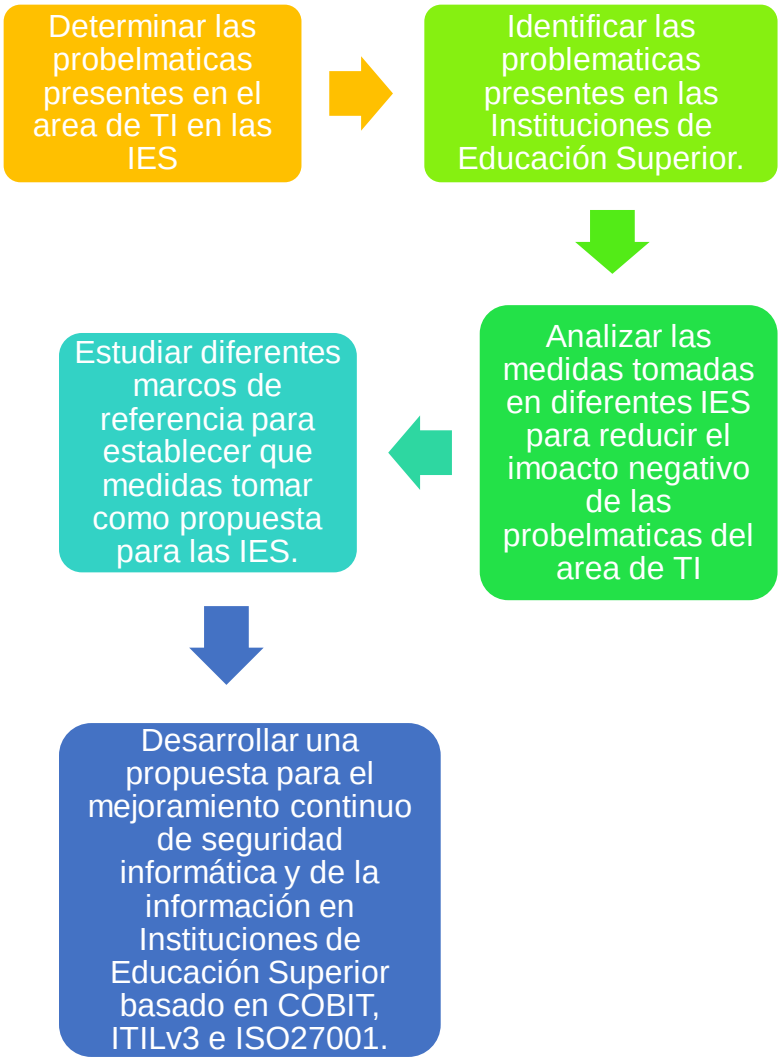

Ilustración 10. Metodología planteada para el desarrollo de la propuesta.
Fuente: Elaboración propia

2. DESARROLLO

2.1. Problemáticas en los sistemas de seguridad informática y de información en las IES

De acuerdo a los objetivos planteados en este proyecto a continuación se dará desarrollo a cada uno de estos.

Inicialmente tenemos un listado de algunas de las problemáticas presentes en diversas Instituciones de Educación Superior, tales como:

- ✓ Los datos desencriptados son transmitidos por la red.
- ✓ Las aplicaciones que se encuentran instaladas no son actualizadas frecuentemente.
- ✓ Existen problemas de comunicación entre el personal a cargo.
- ✓ Existen partes aisladas.
- ✓ No se realiza mantenimiento preventivo.
- ✓ La gestión del tiempo es un aspecto que se deja de lado, disminuyendo así la productividad y la realización de tareas de forma acertada.
- ✓ Los niveles de calidad se encuentran por debajo de lo ideal.
- ✓ Falta de capacitación y competitividad entre el personal de TI.
- ✓ La gestión no está basada totalmente en un modelo que permita orientar la organización.
- ✓ La infraestructura tecnológica es deficiente, existe un rezago tecnológico en el departamento y el despliegue en la Institución.
- ✓ No se realizan controles administrativos con frecuencia.
- ✓ Se presenta resistencia al cambio.
- ✓ No se documentan los sistemas informáticos y los cambios realizados en ellos.
- ✓ No se ejecuta de manera eficiente el presupuesto asignado para el departamento de TI.
- ✓ No existen lineamientos globales que permitan que el multicampus pueda ser gestionado y controlado de forma uniforme.
- ✓ Establecer estrategias que vayan de la mano para el correcto funcionamiento de la seguridad perimetral.
- ✓ Es ideal realizar una segmentación de la red para aumentar el rendimiento de la misma.
- ✓ Los procedimientos que se realicen deben ser claros y se debe realizar un control sobre estos.
- ✓ En cuanto a la planeación se debe contar con un plan estratégico de tecnologías de la información PETI.
- ✓ Los canales en que operan los servicios y tecnologías inalámbricas deben ser acorde a la cantidad de usuarios que los utilizan.
- ✓ Las conexiones y la infraestructura debe ser supervisadas periódicamente.

- ✓ La capacitación a todo el personal es una tarea que no se puede ni se debe dejar de lado, ya que el sector de las comunicaciones y las tecnologías es de los más cambiantes.
- ✓ Control y creación de redes virtuales privadas.
- ✓ Automatización de los sistemas y de tareas.
- ✓ Autenticación y verificación de usuarios en todo momento, no únicamente para personal administrativos sino comunidad en general.
- ✓ Encriptación de los portales que se utilizan.
- ✓ Control de acceso.

Para profundizar un poco en el impacto que tiene cada una de las problemáticas anteriores, a continuación se adjunta una tabla con una breve descripción de cada una de ellas para comprender la importancia de mitigar estas fallas en las IES.

Problemática	Descripción
Los datos desencriptados son transmitidos por la red.	Cuando los datos no están encriptados cualquier persona que tenga acceso a la red puede acceder a ellos y usarlos de manera incorrecta.
Las aplicaciones que se encuentran instaladas no son actualizadas frecuentemente.	Las actualizaciones permiten corregir errores que existen en las versiones previas, además de que proporcionan nuevas herramientas haciéndolas más dinámicas y eficientes.
Existen problemas de comunicación entre el personal a cargo.	Cuando en la organización no se transmite la información de manera eficaz, el personal posiblemente no comprende o corrige problemáticas que impactan dentro del departamento de TI.
Existen partes aisladas.	Se deben definir roles y cada dependencia debe saber de qué se encargan las demás para saber a quién acudir.
No se realiza mantenimiento preventivo.	No se debe actuar únicamente en caso de fallos, es necesario que se tomen medidas antes de que ocurran. Se debe analizar que funciona correctamente.

La gestión del tiempo es un aspecto que se deja de lado, disminuyendo así la productividad y la realización de tareas de forma acertada.	Se debe respetar y cumplir con los cronogramas ya que si una tarea se retrasa o no se realiza las demás posiblemente no funcionen de forma correcta.
Los niveles de calidad se encuentran por debajo de lo ideal.	La calidad debe ser uno de los objetivos primordiales, se debe trabajar en que sea el nivel pactado con las partes.
Falta de capacitación y competitividad entre el personal de TI.	El personal debe tener conocimiento técnico y administrativo de las labores realizadas, es por esto que se deben formar cuando se adquieran equipos o se realicen modificaciones.
La gestión no está basada totalmente en un modelo que permita orientar la organización.	Se deben seguir guías que permitan que se alcancen cada uno de los objetivos y que se puedan optimizar los recursos.
La infraestructura tecnológica es deficiente, existe un rezago tecnológico en el departamento y el despliegue en la Institución.	Se deben adquirir equipos y elementos que cumplan con las necesidades de los usuarios finales, que brinden capacidad, robustos. Ideal que todos pertenezcan al mismo proveedor para cuestiones de compatibilidad y servicio técnico.
No se realizan controles administrativos con frecuencia.	Se debe verificar por parte de los directivos que todo funcione en correcta forma y no esperar que el personal técnico se enfrente a fallos.
Se presenta resistencia al cambio.	Se deben manejar planes de mejora y ejecutarse de forma y en el tiempo oportuno.
No se documentan los sistemas informáticos y los cambios realizados en ellos.	Se debe registrar los cambios para evidenciar el proceso y posteriormente tomar medidas pertinentes.
No se ejecuta de manera eficiente el presupuesto asignado para el departamento de TI.	El dinero dispuesto al departamento se debe invertir de acuerdo a temas importantes y urgentes. Se debe estudiar previamente que se necesita y prever percances futuros.

No existen lineamientos globales que permitan que el multicampus pueda ser gestionado y controlado de forma uniforme.	Cada sede funciona de forma independiente esto puede traer algunas problemáticas, sería ideal manejar un modelo de gestión y administración que sea igual para todas ,de esta manera se podría actuar de manera rápida y eficiente
Establecer estrategias que vayan de la mano para el correcto funcionamiento de la seguridad perimetral.	Se debe proteger el entorno sistemático, tomar diferentes medidas para que este no se vea vulnerado de ninguna manera.
Es ideal realizar una segmentación de la red para aumentar el rendimiento de la misma.	Se debe dividir según las necesidades y las áreas en las que se desempeñen.
Los procedimientos que se realicen deben ser claros y se debe realizar un control sobre estos.	No se deben realizar cambios sin un fundamento, y cuando estos se realicen deben ser documentados y supervisados.
En cuanto a la planeación se debe contar con un plan estratégico de tecnologías de la información PETI.	Una planeación estratégica de TI permitirá abarcar toda el área y verificar el funcionamiento como un todo.
Los canales en que operan los servicios y tecnologías inalámbricas deben ser acorde a la cantidad de usuarios que los utilizan.	Si la cantidad de usuarios crece se debe prever este hecho para de igual manera expandir y adecuar los sistemas y equipos para que el servicio recibido sea el esperado por los clientes finales.
Las conexiones y la infraestructura deben ser supervisadas periódicamente.	Se debe revisar periódicamente que la red y sus terminales soporten la capacidad de usuarios y funcionen de forma adecuada.
La capacitación a todo el personal es una tarea que no se puede ni se debe dejar de lado, ya que el sector de las comunicaciones y las tecnologías es de los más cambiantes.	El personal debe estar a la vanguardia de los equipos, su operación y mantenimiento.
Control y creación de redes virtuales privadas.	Las VPN permitirán que ciertos usuarios de la misma red se conecten

	y compartan información de manera rápida aunque se debe verificar que los que se encuentren en ellas tengan relación con la información manejada.
Automatización de los sistemas y de tareas.	Es preferible la automatización de tareas para lograr la optimización de recursos y disminuir los errores humanos.
Autenticación y verificación de usuarios en todo momento, no únicamente para personal administrativos sino comunidad en general.	Se debe autenticar quienes son las personas que usan la red y sus terminales y con qué fin lo hacen.
Encriptación de los portales que se utilizan.	La encriptación permite que los datos y toda la información contenida en los portales se blinden con claves que solo poseen los usuarios autorizados para así evitar el robo y manipulación de este activo.
Control de acceso.	Se debe comprobar que los usuarios que ingresan o hacen uso de determinados elementos realmente tengan autorización y sean personal idóneo para esto.

Tabla 1. Tabla de problemáticas en las IES
Fuente: Elaboración propia

2.2. Requerimientos para fortalecer los sistemas de seguridad informática en las IES

A partir del análisis previo y con ayuda del listado de problemáticas, se pueden establecer algunos de los requerimientos mínimos que deben ser adoptados por las Instituciones de Educación Superior para que sus redes y sistemas sean robustos y se puedan mitigar los fallos en estos.

De acuerdo al listado anterior se puede determinar que las problemáticas tienen una raíz diferente algunas de estas se deben inicialmente a la falta de planeación y gestión por esto es necesario revisar la documentación existente y los marcos en los que se apoya cada Institución, entre estos documentos se encuentra el PETI, este documento permitirá que la organización alcance el futuro deseado basándose en la situación actual y en los factores que pueden influir en el alcance de los objetivos. Así mismo, cuando se cuenta con una planeación estratégica la compañía puede establecer planes flexibles y adaptables, que permitan que las diferentes áreas cumplan con sus asignaciones.

Para que el PETI abarque todas las dependencias y acerque a la compañía al cumplimiento de objetivos es necesario que su estructura este conformada por los objetivos que se desean alcanzar, la delimitación del alcance, el marco normativo y regulatorio que rige sobre la compañía, analizar la situación actual, determinar que brechas o rupturas estratégicas, entendimiento estratégico, un modelo de gestión y de planeación.

Cuando se habla del análisis de la situación actual es necesario hacer énfasis que alguna problemáticas se presenta debido a que no se realiza una correcta gestión de TI en la entidad, en este aspecto es importante definir la estructura organizacional para determinar responsabilidades, así como el número de personas en cada una de las áreas existentes, las funciones que desempeñan, procesos y perfiles.

Otro aspecto que requiere mejora es la infraestructura de la red y los sistemas que pertenecen a esta, es decir, la seguridad y el correcto funcionamiento de estos se debe garantizar mediante una gestión de algunos factores como lo son planes de contingencia frente a fallos e incidentes, análisis de los riesgos, capacidad, implementación de controles, disminución del rezago tecnológico ,estas y muchas más áreas pueden ser tratadas mediante un Sistema de Gestión de Seguridad de la información, con este sistema se podrán evaluar todos los riesgos y amenazas, se podrá determinar estrategias y controles para minimizarlos.

Todas las compañías están sometidas a las auditorías por eso es indispensable que se cuente con un modelo guía que permita que los interesados e involucrados en la gestión, gobierno de TI, control empresarial, mejora de procesos, gestión de riesgos y calidad esto se puede realizar mediante la adopción de un marco de referencia como COBIT, marco que engloba conceptos de gobierno corporativo, técnicas y

principios de gestión , herramientas de análisis y modelos que fortalecen la confianza y el valor de los sistemas de información.[Kimat empresa de grupo Scanda ,2018].

Por otro lado los servicios y la percepción que recibe el usuario final es uno de los requerimientos más importantes, ya que son estos los que sustentan económicamente las instituciones, los servicios de TI que se entregan deben ser apropiados y acorde con lo pactado desde el inicio, apostando a que se alcancen las metas establecidas y retornar resultados beneficiosos.

Se reconoce a nivel global ITIL como un marco que permite apoyar los proyectos desde el inicio hasta el final de este, siendo un mecanismo para definir, diseñar, implantar, operar y supervisar los servicios en todo momento, permitiendo que sea una solución funcional permanentemente.

En conclusión se pueden englobar algunos de estos requerimientos que son mínimos para garantizar que las instituciones de educación superior cuenten con sistemas que protejan y gestionen de forma adecuada la seguridad informática y de la información.

	Se cumple					**No se cumple**
Indique el nivel de cumplimiento siendo 1 el valor mínimo y 5 el máximo	**1**	**2**	**3**	**4**	**5**	
Requerimiento						
Sistemas y redes robustos			x			
Falta de planeación y gestión de TI			x			
Planes flexibles y adaptables			x			
Establecer el alcance y las limitaciones de la compañía.				x		
Asignación y verificación de las responsabilidades en cada área.				x		
Planes de contingencia				x		

Diseño de la infraestructura tecnológica bajo lineamientos de calidad		x				
Apropiación de la tecnología e innovación			x			
Implementacion de un Sistema de Gestión de Seguridad de la información.		x				
Establecer políticas de seguridad			x			
Protección de los puertos en cada uno de los equipos						x
Conexiones seguras con los usuarios						x
Uso de un directorio activo			x			
Protección de los datos personales de todos los usuarios de las redes				x		
Copia en servidores de datos de respaldo.				x		
Administración de permisos		x				
Uso de cortafuegos para la separación de las redes			x			

Tabla 2. Requerimientos básicos para los sistemas y redes de las IES.
Fuente: Elaboración propia

2.3. Marcos de seguridad, gestión y gobierno de TI

Con el reconocimiento de las problemáticas y requerimientos que se planteó previamente, se puede establecer mediante el estudio de los marcos de referencia una relación entre cual se ajusta y permite dar un mejor manejo de cada una de las situaciones establecidas.

Esto a manera de cuadro comparativo permite reconocer y las características de cada uno de ellos.

	ITIL v3	COBIT	ISO 27001	ISO 20000	eTOM
Origen	La agencia central de telecomunicaciones CCTA, lo desarrollo hacia el año 1987	La Asociación de Auditoria y Control de Sistemas de Información ISACA, creo este marco en el año 1996	Emitida por la Organización Internacional de Normalización ISO, en el año 2005.	Fue la primera norma en el mundo dirigida a la gestión de servicios de TI, publicada finalizando el año 2005.	Fue desarrollado en el año 2001, por el foro de empresas de comunicaciones TM Forum y publicado por la UIT en una de sus recomendaciones.
Contexto	Gestión de servicios de TI.	Gobierno y auditoria de TI.	Gestión de seguridad de la información	Gestión de la calidad y sistemas para para la gestión	Gestión y operación de procesos de empresas de telecomunicaciones.
Última versión	4	5	ISO/IEC 270001:2013	ISO/IEC 20000-1:2018	5
Enfoque	Realizar un ciclo de seguimiento a los resultados de la prestación de servicios de TI.	Busca separa el Gobierno y la Gestión, para poder jerarquizar procesos.	Velar por los activos de información de las compañías a través de un sistema de Gestión de Seguridad de	Implementación y planeación para desarrollar servicios de TI que sean confiables y que sean efectivos,	Busca poder automatizar y categorizar las tareas dentro de la organización para optimizar los recursos.

			la Información.	es decir, de calidad.	
Ventajas	Maneja un vocabulario consístete que es de fácil comprensión para las diversas áreas. Los servicios están enfocados hacia los clientes y los SLA's. Los costos y calidad de los servicios son controlados de forma efectiva. Posee un modelo de gobernabilidad ajustable.	Puede ser empleado en cualquier tipo de empresa. La toma de decisiones por parte de la lata gerencia es basada en criterios confiables. Asegura la continuidad de servicio. Es eficiente en la realización de procesos de auditoria	Proporciona una metodología que permite cumplir con los requerimientos legales. Posibilita ahorrar dinero gracias a que se evitan incidentes de seguridad. Alienta a las empresas a escribir sus procesos mejorando la organización	Enfocada a todo tipo de empresas, sin importar su tamaño. Los resultados se pueden evidenciar en corto plazo. Optimiza recursos económicos gracias al uso adecuado de los materiales usados. Se eliminan los procesos redundantes. Se presenta incremento en la productividad y mejora en la calidad.	Tiene una aplicación más enfocada en ciertas áreas, lo que permite que sea más eficiente. Existe una interrelación entre los procesos aplicados. Tiene una visión integradora entre el cliente y la compañía. Permite definir flujos extremos a extremo dentro de la empresa.

Desventajas	Tiene un foco muy subjetivo y debe ser implantado por segmentación. Demanda una gran cantidad de tiempo para ser adoptado. La puesta en marcha en su versión inicial implica algunos costos. El personal a cargo debe dedicar un 10 o 15% de su jornada laboral. Existe un cambio en la mentalidad y rutinas laborales que afloran reticencias.	Tiene un foco muy subjetivo y debe ser implantado por segmentación. Demanda una gran cantidad de tiempo para ser adoptado	La puesta en marcha en su versión inicial implica algunos costos. El personal a cargo debe dedicar un 10 o 15% de su jornada laboral. Existe un cambio en la mentalidad y rutinas laborales que afloran reticencias	Se ve afectada la independencia entre departamentos. En empresas pequeñas es posible que se evidencie resistencia al cambio. Demanda una inversión de recursos económicos considerable.	Se encuentra dirigido en mayor parte a grandes compañías. Es variante según la organización en la que se emplee.
Cantidad de procesos	25	37	10	13	49

Procesos más relevantes	Gestión de la estrategia. Gestión de la demanda. Gestión del catálogo de servicios. Gestión del nivel de servicio. Gestión de la capacidad , Gestión de la continuidad del Servicio, Gestión de la seguridad de la información. Gestión de los cambios. Evaluar los cambios. Gestión de incidentes. Gestión de acceso. Siete pasos para la mejora.	Asegurar el establecimiento y mantenimiento del marco del Gobierno. Gestionar el marco de Gestión de TI. Gestionar la introducción de cambios organizativos. Gestionar los programas y proyectos. Gestionar el conocimiento. Supervisar, evaluar y valorar el rendimiento y conformidad. Supervisar, evaluar y valorar la conformidad con los requerimientos externos	Contextualización de la organización Liderazgo. Soporte. Evaluación de desempeño. Mejora	Generación de informes del servicio. Gestión de las relaciones con el negocio. Gestión de cambios. Gestión de la entrega y despliegue.	Asegurar la entrega de los servicios. Asegurar la optimización de los recursos. Asegurar la transparencia hacia las partes interesadas. Gestionar la innovación. Gestionar el presupuesto y los costos. Gestionar los recursos humanos. Gestionar los acuerdos de servicios. Gestionar los proveedores.

Tabla 3. Cuadro comparativo de los marcos de referencia
Fuente: Elaboración propia.

2.4. Propuesta de mejoramiento continúo

Con los tres ítems anteriormente desarrollados y a partir de un análisis más detallado de la situación problema, se puede establecer una propuesta de mejoramiento continuo enfocada en aspectos como la seguridad informática y de la información adoptando los marcos de referencias mencionados durante este documento que permitan que las Instituciones de Educación Superior logren un excelente funcionamiento, que sus sistemas y redes sean óptimos y que sus usuarios tengan calidad en los servicios tecnológicos.

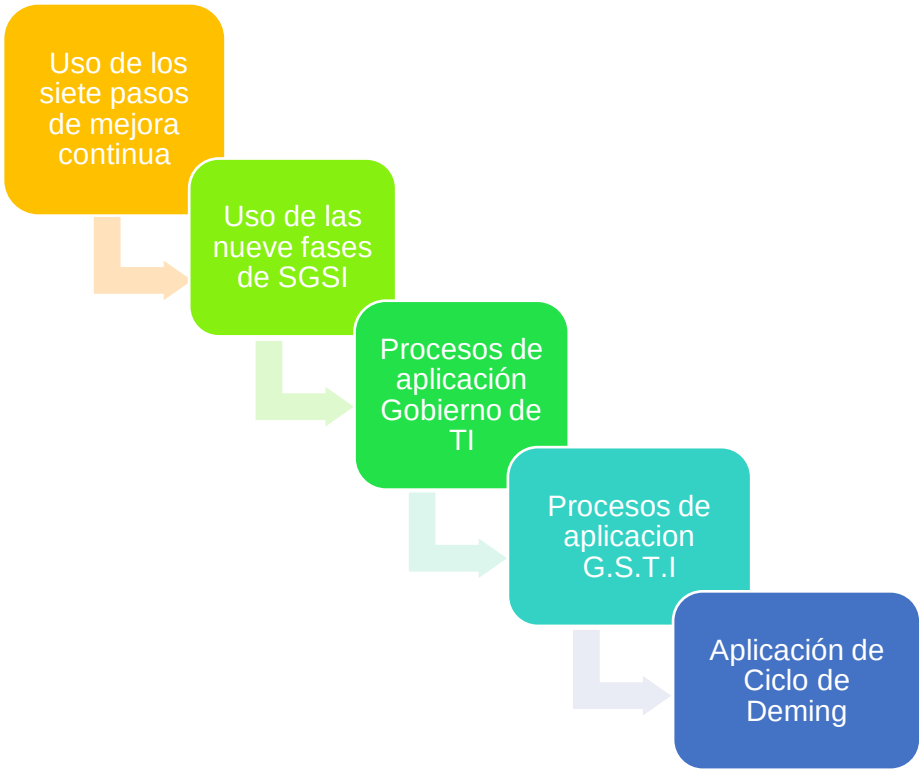

Ilustración 11. Propuesta de mejora continúa
Fuente: Elaboración propia

Se propone la adopción de un proceso de mejora continua, para esto se tomaran pautas presentes en el marco de referencia ITIL, de igual manera se adoptara procesos presentes en ISO 270001 y COBIT, ya que como se mencionó en la introducción de este documento se busca presentar una solución a partir del estudio de diversos marcos de referencia que sea óptima y completa, por esto es que se

hará referencia de más de uno de ellos, ya que cada uno cuenta con un enfoque diferente pero trabajan en conjunto siendo un todo confiable y eficiente.

ITIL en su proceso de mejora continua cuenta con siete pasos, a continuación se habla de cada uno de ellos y como se puede a partir de esto tomar medidas que contribuyan en el beneficio de la Seguridad Informática y de la Información en las Instituciones de Educación Superior.

Para pensar en el proceso de mejora continua hay que analizar cuál es la finalidad de este, es decir, saber porque se busca esto. El proceso de mejora continua busca mediante un monitoreo constante y la verificación de las actividades brindar al usuario final servicios de calidad y con valor que se adapten a sus requisitos y necesidades.

Seguido se debe tener en cuenta los pasos que componen el proceso

1. ¿Qué se debe medir?
2. ¿Qué se puede medir?
3. Recolectar datos
4. Procesar datos
5. Analizar datos
6. Presentar la información
7. Implementar mejoras.

¿Qué se debe medir?

Para dar solución a este paso se puede partir desde algunos interrogantes como ¿Cuál es la visión de la organización? Y ¿Cuál es el funcionamiento o estado ideal?, cabe destacar que la respuesta a estas problemáticas tiene su fundamento en la misión general de las IES, es decir, es una respuesta objetiva como las que se presentaran durante el desarrollo de este capítulo. Esto con el fin de identificar los objetivos de la organización y su relación con las TI.

Pregunta problema base	Respuesta
¿Cuál es la visión de la organización?	Formar profesionales competentes, dirigentes y éticos, que brinden soluciones y apoyo a la sociedad. Rigiéndose bajo principios y valores en pro de la mejora del sector en el que se desempeñan.
¿Cuál es el funcionamiento o estado ideal?	La infraestructura de TI debe soportar la cantidad de usuarios sin que estos vean afectada la calidad del servicio y que esta sirva como herramienta para

	el desarrollo académico y personal de los usuarios finales.

Tabla 4. Preguntas problema
Fuente: Elaboración propia

Con el listado de problemáticas que se encuentran al inicio de este capítulo se pueden establecer algunos cambios que permitirían disminuir su impacto y corregir algunos fallos.

Cambio planteado	¿Qué se debe medir?
Ampliar los canales para la transmisión	Porcentaje de usuarios satisfecho y el nivel de satisfacción respecto a los servicios de TI que le brindan las IES. La capacidad de la infraestructura inalámbrica
Definir cronogramas para la actualización de programas y sistemas.	Tiempos entre la realización de las actualizaciones de las aplicaciones y los sistemas que pertenecen a la red.
Realizar capacitaciones a todo el personal relacionado con las TI, con periodos de tiempo prudentes.	Tiempos entre las capacitaciones del personal técnico y administrativo. En qué porcentaje fue comprendido y útil la capacitación.
Documentar los cambios y trabajar bajo lineamientos completos.	Por qué se realizaron los cambios. Quien los realizo. Que parámetros se tuvieron en cuenta para realizar los cambios.
Establecer la finalidad de los recursos económicos y rendir cuentas.	Porcentaje del uso del dinero destinado a las mejoras y ajustes del departamento de TI se ejecutó. Como se determinó que aspectos eran más necesarios para invertir

Tabla 5. Mejoras propuestas
Fuente: Elaboración propia

Al obtener estas mediciones se pueden planear los cambios que se deben de implementar, es decir, se da inicio a la planificación.

¿Qué se puede medir?

En el paso anterior se generaron diez aspectos que se deben medir, de estos diez desde en el interior de la organización todos son factibles para realizar la medición

Son mediciones relacionadas con la gestión del tiempo y el cumplimiento de algunas tareas, con la percepción de los usuarios, los controles y las acciones que se toman de manera preventiva.

Recolectar datos

Para la recolección de los datos las IES pueden realizar encuestas de satisfacción, pueden realizar con apoyo de personal técnico revisiones para determinar el estado actual, de igual manera se debe tener dentro de cada departamento de TI reuniones donde se pueda poner sobre la mesa las diversa situaciones relacionadas con los servicios de TI así con esto se puede identificar que está bien y que requiere un cambio. Como parte de la gestión de la comunicación se pueden crear boletines de operación retroalimentados por los usuarios, de allí se puede trabajar en conjunto para verificar las metas alcanzadas y conocer de cerca la percepción para trabajar en el momento justo e incluso optimizar recursos.

Procesar datos

El procesamiento de los datos debe realizarse de manera que se puedan tener resultados para análisis cualitativo y cuantitativo, se deben procesar por personal que conozca del tema y sin tergiversar los resultados. En el procesamiento de los datos se debe evidenciar el cumplimiento y los avances en los cambios planeados y registrar estos.

Analizar datos

Se verifica que los servicios están siendo de total aceptación, además de si estos cumplen con las condiciones de funcionamiento y la transición del servicio. Acá también se debe establecer que decisiones se deben tomar con conocimiento de causa, a través de tendencias, esto debe ser realizado por personal con alta experiencia.

Presentar la información

Todas las partes involucradas deben ser informadas acerca de lo sucedido en cada uno de los procesos previos, es decir, empezar por las mejoras, el porqué de que estas se efectúen, y cuál es el propósito de la adopción de los procesos de mejora continua.

Implementar las mejoras

En este último paso se empieza a implementar los cambios de acuerdo a la prioridad de estos según los beneficios que estos traigan a la organización. Para que se realice de forma correcta se debe crear un cronograma para seguir un control eficiente y poder acoger de forma correcta ITIL y los diversos marcos de los que se hizo mención.

Por otro lado haciendo énfasis en el uso y apoyo de COBIT e ISO270001, se hace mención de que este último permite hacer uso de sus herramientas para la creación de un Sistema de Gestión de Seguridad Informática que permitirá que las IES puedan proteger la información, mediante la evaluación previa de riesgos y posteriormente estableciendo qué medidas se deben tomar para mitigar los fallos.

Para la implementación de esta norma las IES deben tener en cuenta alrededor de 16 pasos que involucran desde la dirección de la compañía, delimitar el proyecto así como el alcance, la metodología, evaluación y solución de los riesgos, como se aplicaran y se trataran las soluciones, como se realizarán los controles y la medición de la eficiencia, capacitación y concienciación de las partes, realización de auditorías, revisión por parte de los directivos y la implementación de las soluciones.

Se busca que las IES creen y de manejo de un SGSI basado en ISO 270001, por lo que se deben ejecutar las siguientes fases, representadas en el grafico a continuación.

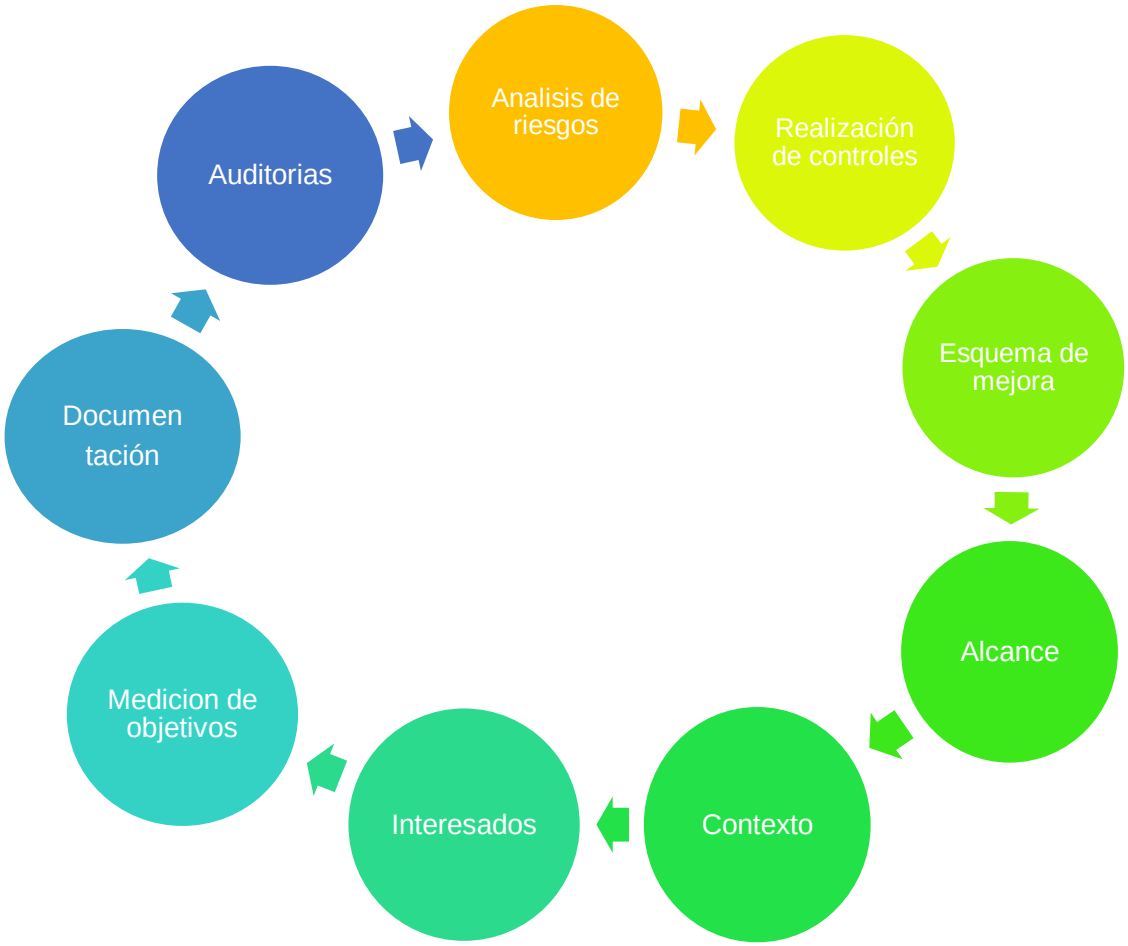

Ilustración 12. Fases para la implementación de un SGSI basado en la norma ISO 27001
Fuente: Elaboración propia

Análisis de riegos

Se deben identificar las amenazas presentes en las IES, se establecen una evaluación y plan de acción de los riesgos. Para identificar los riesgos es necesario identificar qué tipo de información tiene mayor relevancia para la compañía así mismo como que impacto tendría en un caso supuesto de que este activo se viese vulnerado.

Para la evaluación de los riesgos se puede llevar una serie de pasos que permitirán que este proceso sea más confiable, entre esto se pude realizar una clasificación de las amenazas, vulnerabilidades, tipificación de los impactos, evaluación y finalmente el análisis.

De igual manera se debe establecer que tan críticos son los riesgos identificados, si son aceptables o por lo contario es residual, es decir, este persiste posteriormente a la realización de los controles.

Realización de controles

La norma ISO 27001 provee 113 controles divididos en dos grupos. Aunque cada empresa puede crear o modificar los existentes de acuerdo a los planes que manejan para controlar sus operaciones, esto sin que dejen de acogerse a la norma.

Los controles que se realicen pueden eliminar el riesgo si este es crítico y afecta la compañía, mitigarlo si la compañía no le otorga un nivel crítico alto y este con un monitorea puede estar bajo control, y finalmente se encuentra el traslado que ocasionalmente ocurre cuando se adquiere un seguro que se haga a cargo de todas las consecuencias.

Esquema de mejoras

Para establecer las mejoras es necesario que en cada control se asocie un rango determinado. Cuando se implementa un proceso de mejora continua se puede verificar si los controles realizados fueron eficientes o si por el contrario se debe replantear nuevamente.

Alcance

Para delimitar el alcance hay que conocer la organización, es decir, saber el número de empleados y clientes que existen, el tipo de información que maneja, ya que de esto depende la forma en que se debe implementar un Sistema de Gestión de Seguridad de la Información.

De igual manera un SGSI se implementa en determinadas áreas, la elección de estas depende de si son primordiales para dar cumplimiento con los objetivos de la compañía.

Contexto

Se debe realizar previamente a la implementación del SGSI un análisis del contexto de la organización para establecer los problemas, sus orígenes y una matriz DOFA

Interesados

Para determinar el contexto organizacional es necesario que las partes interesadas sean tomadas en cuenta, para que sus necesidades orienten la prestación del servicio.

Entre los interesados se encuentran los proveedores de servicios y productos, los clientes, las autoridades judiciales y la comunidad.

Medición de objetivos

Se deben establecer objetivos para la medición de la gestión de riesgos, estos deben ser medibles más no cuantificables. Estos objetivos deben ser comunicados a toda la compañía para que estos sepan que trabaja por un bien común, de igual manera cada objetivo debe estar ligado con uno o más indicadores para poder realizar un seguimiento.

Documentación

La documentación no debe encontrarse en un formato especifico pero si debe cumplir con determinado proceso de documentación para alcanzar la certificación.

Esta documentación debe estar disponible en todo momento para ser consultada por auditores y por la organización.

Auditorias

Deben realizar auditorías internamente con una frecuencia prudente para garantizar que el SGSI funcione de funcione correcta. Existen dos tipos de auditorías internas; las de gestión y las de control.

Estas auditorías pueden ser realizadas por la alta dirección de la compañía.

Por otro lado es importante hacer referencia a lo beneficioso que llegaría a ser el uso de algunos procesos de COBIT, que posibilitan la implementación de algunas mejoras en el Gobierno de TI.

Se eligieron algunos procesos de COBIT que son una pausa efectiva para el Gobierno dentro de una organización mediante la jerarquización de los procesos.

Objetivo del proceso	Proceso
Evaluar, orientar y supervisar	Asegurar el establecimiento y mantenimiento del marco de Gobierno de TI.
Alinear, planificar y organizar	Gestionar el marco de Gestión de TI.
	Gestionar la introducción de cambios organizativos.
Construir, adquirir e implementar	gestionar los programas y proyectos
	Gestionar el conocimiento
Supervisar, evaluar y valorar	Supervisar, evaluar y valorar el rendimiento y conformidad.
	Supervisar, evaluar y valorar la conformidad con los requerimientos externos.

Tabla 6. Procesos de COBIT elegidos para la mejora continua.
Fuente: Elaboración propia

Adicionalmente para realizar una correcta Gestión de los Servicios de TI se han elegido algunos procesos de los marcos como ITIL, eTOM e ISO 20000.

Por el lado de ITIL se adoptó el proceso de mejora continua y otros adicionalmente, entre ellos:

Área del proceso	Proceso
Estrategia	Gestión de la estrategia.
	Gestión de la demanda.
Diseño	Gestión del catálogo de servicios.

	Gestión del nivel de servicio.
	Gestión de la capacidad ,
	Gestión de la continuidad del Servicio,
	Gestión de la seguridad de la información.
Transición	Gestión de los cambios.
	Evaluar los cambios.
Operación	Gestión de incidentes.
	Gestión de acceso.
Mejora continua	Siete pasos para la mejora

Tabla 7. Procesos de ITIL elegidos para la mejora continua.
Fuente: Elaboración propia

eTOM maneja procesos enfocados hacia la categorización de las tareas dentro de la organización para optimizar los recursos.

Área del proceso	Proceso
Estrategia, infraestructura y producto	Desarrollo y gestión de la mercadotecnia
	Desarrollo y gestión del cliente
	Desarrollo y gestión de los recursos

Operaciones	Gestión y operación de las relaciones con el cliente
	Gestión de los SLA´s
	Gestión y operación de los recursos humanos
Gestión de la empresa	Gestión del conocimiento
	Gestión financiera y de activos

Tabla 8. Procesos de eTOM elegidos para la mejora continua.
Fuente: Elaboración propia

Y finalmente se recomienda la adopción de algunos procesos de ISO 20000 que permitirá que los servicios de TI entregados sean de calidad.

Área del proceso	**Proceso**
Provisión del servicio	Generación de informes de servicio
	Elaboración de presupuesto y contabilidad de los servicios
Relación	Gestión de suministradores
Resolución	Gestión de problemas
Control	Gestión de los cambio

	Gestión de despliegue

Tabla 9. Proceso de ISO20000 elegidos para la mejora continúa
Fuente: Elaboración propia

Finalmente se propone la realización e implementación del ciclo de Deming que permite la mejora de los procesos, que permitirá realizar la autoevaluación periódica de las mejoras previamente implantadas, para establecer cuáles de estas han sido efectivas y deben seguir así y por el contrario cuales deben ser revindicadas.

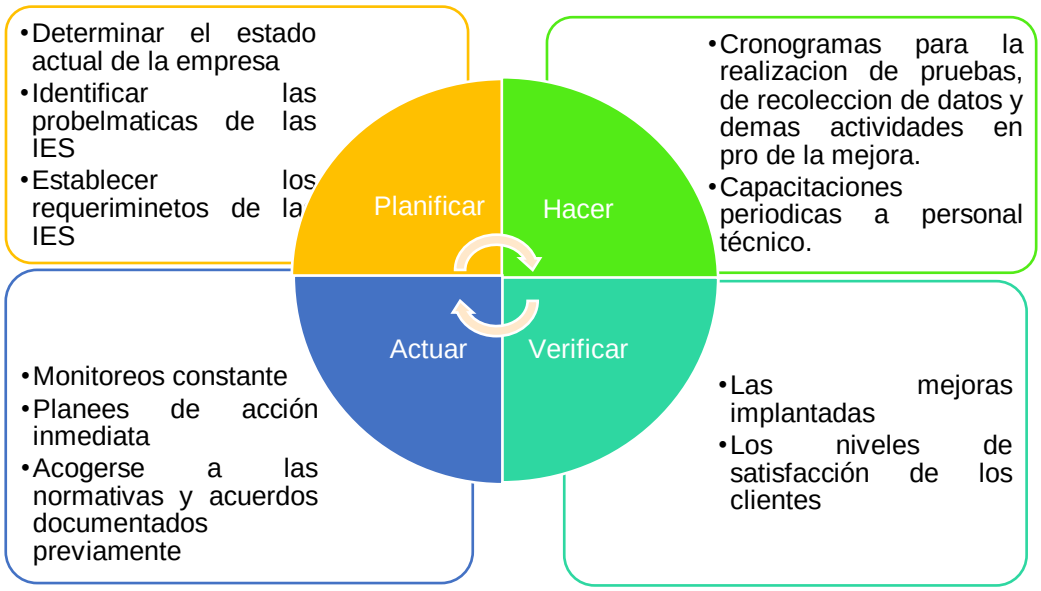

Ilustración 13. Ciclo de Deming
Fuente: Elaboración propia

3. CONCLUSIONES

Las problemáticas presentes en las diversas Instituciones de Educación Superior que fueron consultadas para proponer una mejora en aspectos relacionados con la Seguridad Informática y de la Información en su gran mayoría se pueden evitar o por lo menos disminuir su impacto y frecuencia si se adquieren buenas practicas dentro de la organización , partiendo desde un nivel jerárquico superior, donde allí se maneje un plan de acción y desarrollo de las diversas actividades y labores relacionadas con los elementos y herramientas de TI.

Se justifica la implementación de diversos marcos ya que aunque cada uno de ellos se encuentra bien desarrollados, no tienen el mismo objetivo de aplicación. Así que trabajar con ellos en conjunto permite que la organización abarque diversos aspectos como puede ser la Gobernanza, la Gestión de los Servicios de TI y la Seguridad.

Es necesario conocer la empresa, verificar y analizar sus objetivos, el estado actual de esta e incluso los interesados, de acuerdo esto se determina que aspectos funcionan y se encuentran acorde con la misión y visión corporativa y de igual manera se establece que proceso tomar para corregir lo que no se encuentra dentro de lo deseado.

Con la adopción de los marcos de referencia y la implementación del ciclo de mejora continua las compañías pueden asegurar que los problemas disminuirán y que los servicios que prestan serán de calidad y de acorde a los objetivos y acuerdos pactados con los usuarios.

Los Sistemas de Gestión de la Seguridad Información permitirán la adopción de los procesos que consideren pertinentes, ya que posee un anexo donde la compañía podrá encontrar una breve descripción de cada uno de ellos y elegir cuales son ideales según el estado en el que se encuentre, optimizando tiempo y recursos y haciendo este proceso ágil y sencillo.

Es justo que las Instituciones de Educación Superior inviertan recursos en equipos terminales de última tecnología, no solo por la comodidad de sus clientes sino porque estos poseen características que aportan a temáticas de seguridad, de igual manera se debe considerar los periodos de garantía y mantenimiento de los mismos.

La capacitación del personal que opera y administra los servicios y departamento de TI es un aspecto imprescindible ya que el campo de las comunicaciones y la tecnología cambian rápidamente, se debe tener conocimiento acertado sobre estos y la importancia de que funcionen adecuadamente dentro de una red a la cual

acceden una cantidad considerable de usuarios, los cuales tienen roles diferentes hecho que debe ser importante para gestionar el acceso y la autenticación de usuarios.

Los equipos que pertenecen a la red deben ser configurados y administrados por personal profesional y ético para evitar delitos cibernéticos o acciones que afecten con la integridad de la red y la información que viaja a través de esta.

La gestión del tiempo cuando se lleva acorde a lo estipulado es una herramienta que permite que los servicios sean entregados según lo pactado, de igual manera permiten que la acciones se ejecuten en el momento indicado con esto evitando eventos negativos.

Las actualizaciones del sistema operativo y de los diversos programas instalados en cada uno de los equipos son necesarias, estas deben realizarse con frecuencia ya que estas son diseñadas con nuevas características para la mejora y seguridad.

4. RECOMENDACIONES

De acuerdo a lo comentado por algunas IES es necesario que se cuente con un PETI así como la adopción de un referente para la organización y cada proceso manejada dentro de la misma.

Las redes que se emplean dentro de las IES, deben ser diseñadas por personal capacitado de igual manera deben ser supervisadas ya que en ocasiones estas pueden verse saturadas debido a que la cantidad de usuarios puede cambiar periódicamente.

La red se sugiere que sea redundante para que garantice la disponibilidad, es decir, la red debe poseer la capacidad de recuperarse a los fallos de manera rápida cuando esta falle para que servicio y los usuarios no se vean afectados.

Las IES en sus redes deben contar con algunos elementos que permitan que esta sea segura y funcione de manera eficiente.

A continuación se presenta un modelo básico con los elementos que suele tener una red para una IES.

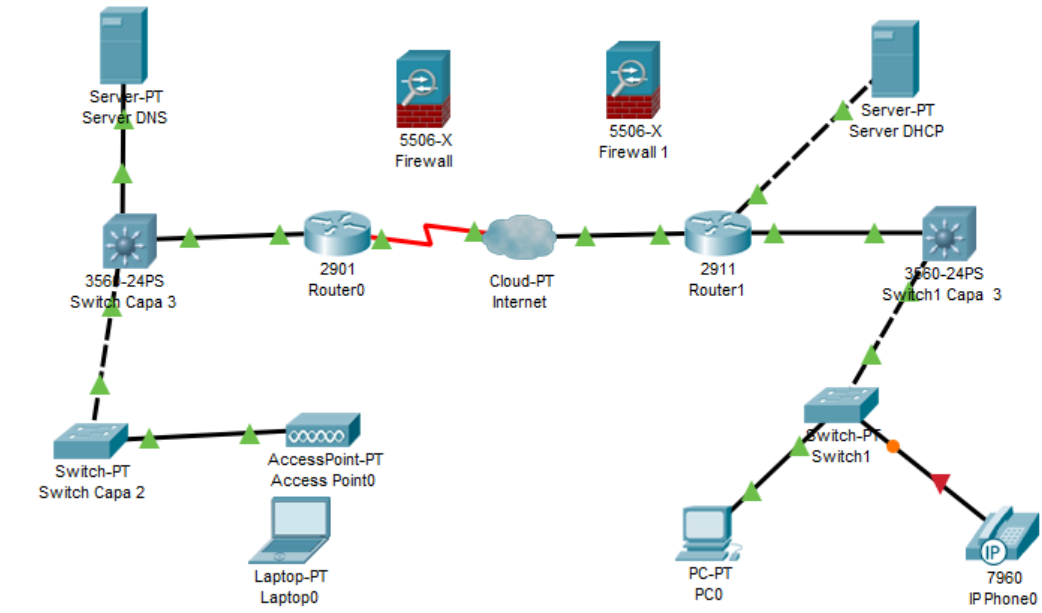

Ilustración 14. Red básica para IES
Fuente: Elaboración propia

Posee elementos desde computadores portátiles los cuales acceden a la red mediante conexión inalámbrica a través de los puntos de acceso o conocidos como Access-point, de igual manera deben existir los firewall que impidan que usuarios no autorizados ingresen a la red, los switch de capa 2 y capa 3 que permiten la conexión de los departamentos y cada uno de los usuarios, existen los servidores DHCP y DNS que se encargan de asignar de forma dinámica las direcciones IP y por otro lado la traducción de una IP a un nombre que dominio. Los routers que se encargan de encaminar los paquetes por la ruta que más adecuada.

Se recomienda que el tráfico que viaja por la red se encuentre cifrado

5. REFERENCIAS

ACCESNSIT.COM (2019) *Seguridad perimetral informática: Información necesaria [*online] Available at: https://www.accensit.com/blog/seguridad-perimetral-informatica-informacion-necesaria/ [Accessed 14 Nov. 2019].

CEUPE, E. (2019). *¿Qué es la gestión del cambio?*. [Online] Available at: https://www.ceupe.com/blog/que-es-la-gestion-del-cambio.html [Accessed 14 Nov. 2019].

CONSULTORA EN TECNOLOGIA, CCTI. *Definición de PETI [*online] Available at: https://ccti.com.co/index.php/es/definicion-peti [Accessed 14 Nov. 2019].

MINTIC.GOV.CO. (2019). *Marco de Referencia Anterior - Arquitectura TI*. [online] Available at: https://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8114.html [Accessed 15 Nov. 2019].

MORAN, L., SANCHEZ, A., TRUJILLO, J. y BATHIELY, D., (2015). *Guía completa de aplicación para la gestión de los servicios de tecnologías de la información* [online] Available at: https://www.proactivanet.com/images/Blog/ISO20000_GuiaCompletadeAplicacion_LuisMoran.pdf. [Accessed 15 Nov. 2019].

OSIATIS, *(2013). ITIL foundation* [online] Available at: http://faquinones.com/gestiondeserviciosit/itilv3/estrategia_servicios_TI/introduccion_objetivos_activos_servicio.php. [Accessed 15 Nov. 2019].

PONTIFICIA UNIVERSIDAD JAVERIANA (2019) *Guía metodológica para implementar COBIT en las áreas de ti* [online] Available at: https://pegasus.javeriana.edu.co/~CIS1210IS02/news/Gu%C3%ADa%20Metodológica%20para%20COBIT%204.1.pdf [Accessed 15 Nov. 2019].

PREZI.COM. (2019). *Marcos de referencia en la gestión de servicios de TI*. [Online] Available at: https://prezi.com/jbs0ybqkybrc/2-marcos-de-referencia-en-la-gestion-de-servicios-de-ti/ [Accessed 15 Nov. 2019].

REPOSITORIO.PUCE.EDU.EC. (2019). [Online] Available at: http://repositorio.puce.edu.ec/bitstream/handle/22000/6078/T-PUCE-6320.pdf?sequence=1 [Accessed 15 Nov. 2019].

SOFTEXPERT EXCELLENCE BLOG. (2019). *COBIT e ITIL: diferencias y conexiones*. [online] Available at: https://blog.softexpert.com/es/cobit-e-itil-diferencias-y-conexiones/ [Accessed 20 Nov. 2019].

TENDENCIAS&INNOVACIÓN. (2019) *Tipos de seguridad informática más importantes a conocer y tener en cuenta* [online] Available at: https://obsbusiness.school/int/blog-investigacion/sistemas/tipos-de-seguridad-informatica-mas-importantes-conocer-y-tener-en-cuenta. [Accessed 20 Nov. 2019].

UNIVERSIDADLIBRE.EDU.CO. (2019). *El decálogo de la seguridad Informática* [online] Available at: http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/247-el-decalogo-de-la-seguridad-informatica. [Accessed 20 Nov. 2019].

UNIVERSIDADVERACRUZANA (2019). *Seguridad de la Información* [online] Available at:
https://www.uv.mx/celulaode/seguridad-info/tema1.html#tema3[Accessed 20 Nov. 2019].