Tercera Conferencia de Directores de Tecnología de Información, TICAL 2013.
Gestión de las TICs para la investigación y la Colaboración. Cartagena de Indias 8 y 9 de Julio.

ESTRATEGIAS PARA LA IMPLEMENTACION DE ISO 20000 E ISO 27001 EN UNA UNIVERSIDAD PÚBLICA COLOMBIANA.

Diana Rocio Plata Arango[1,a]

[a]Universidad Pedagógica y Tecnológica de Colombia, Coordinadora Grupo Organización y Sistemas. Km1. Av. Central del Norte. Tunja – Boyacá, Colombia.
diana.plata@uptc.edu.co

Resumen. La Gestión de Servicios de Tecnología de Información se ha convertido en un requisito, para las Organizaciones y en las Universidades no hay excepción, cada vez es más común que se requiera calidad en la prestación de los servicios, el reto para los Departamentos de Tecnología es cada día mayor, dados los diferentes estándares, para la adopción de buenas prácticas que existen en el mercado, no se conoce aún una metodología que se pueda seguir para lograr con éxito la implementación de estándares. Sin embargo persiste la exigencia de ¿qué pasos se deberían seguir para garantizar que los servicios de tecnología en la Universidades están garantizando el servicio, la seguridad y demostrando la mejora continua?, quizá una respuesta es establecer si se puede diferenciar, tomando la ruta de anotar a estándares internacionales como ISO 20000 e ISO 27001, de acuerdo a los servicios que ofrecen, pero queda aún una pregunta de cómo implementarlos? Este documento presenta un caso de Implementación con alcance a la certificación, de las normas ISO 20000 e ISO 27001, en el Grupo Organización y Sistemas (área de Tecnología), en la Universidad Pedagógica y Tecnológica de Colombia, UPTC, donde se resaltan las estrategias que se han llevado a cabo para lograr la implementación.

Palabras Clave: Gestión de Servicios de TI, Buenas prácticas, ISO 9000, ISO 20000, ISO 27000, Mejora Continua, Seguridad de la Información.

1 Introducción

En el TICAL de 2011 se presentó el inicio de este proyecto, ya que con el artículo nombrado como VISION DE LOS BENEFICIOS DE IMPLEMENTAR SERVICIOS DE TI, CON ESTANDARES COMO ISO 20000 E ISO 27001 EN UNA UNIVERSIDAD PÚBLICA COLOMBIANA. Se dejó ver cuales beneficios podían obtener las Universidades al asumir el camino de implementación de las normas mencionadas y se

[1] Ingeniera de Sistemas, Especialista en Gerencia de Proyectos Informáticos, Magistra en Ciencias Computacionales, Auditor ISO 9001, EXIN .Fundamentos IT Service Management de acuerdo ISO 20000.

propuso un modelo por fases para llevar a cabo ese proyecto, teniendo como ventaja el trabajo ya por procesos ganado con la certificación en ISO 9001 y NTCGP 1000.

El hecho de asumir la implementación con fines de certificación, para dos estándares de gestión para las áreas de TI es un reto y más para una Universidad, sin embargo el objetivo final es lograr la satisfacción de los usuarios, ya que las políticas, procesos y procedimientos adoptados no son por capricho si no que siguen un estándar internacional que ha sido probado con lo cual el usuario final es el beneficiado.

Un beneficio adicional, además de la satisfacción de los usuarios es lograr el cambio de percepción en que las áreas de Tecnología son sólo costos, pues con la adopción de buenas prácticas bajo los estándares internacionales se puede evidenciar, como los departamentos de tecnología le agregan valor a la organización y permiten que sean más eficientes en el uso planificado y controlado de los recursos requeridos, ventajas que se pueden obtener con ISO 20000.

Igualmente con la implementación de ISO 27001 se logra asegurar la confidencialidad, disponibilidad e Integridad de la Información, y esto representa enormes beneficios tanto para la organización como para los usuarios finales, ya que se puede lograr disminuir incidentes de seguridad de la información que en la actualidad son tan comunes, como los fraudes a través de correo electrónico y redes sociales, y se debe brindar información a los usuarios para que conozcan y asuman el reto que la responsabilidad de la seguridad de la Información es tarea de todos.

Este Documento presenta en la primera parte cual fue el modelo por fases propuesto en el 2011 y cómo cambio en el proceso de implementación, luego da a conocer las estrategias utilizadas para los procesos que son generales a las dos normas, después se encuentran las estrategias seguidas para llevar a cabo la implementación de los procesos requeridos por ISO 20000 e ISO 27000, al final en el aparte de conclusiones se presenta el resumen de las estrategias, ya que aún no se concluye pues este proyecto sigue en desarrollo y solo cuando esté totalmente implementado se podrá concluir acerca del impacto que ha tenido en la organización la certificación en los dos estándares de TI.

2 Modelo de Implementación propuesto.

La primera estrategia para lograr éxito en el desarrollo de estos proyectos es contar con el apoyo de la alta dirección, para este caso en el 2011, se incluyó el Proyecto "Adopción de buenas prácticas bajo los estándares ISO 20000 e ISO 27001" dentro del Plan de Desarrollo de la Universidad Pedagógica y Tecnológica de Colombia; esto garantiza que se cuenta no solo con el aval de la alta dirección sino con recursos para llevar a cabo las actividades requeridas para lograr en 2014 la certificación con estas normas.

Esto se convierte en un reto como se dijo anteriormente, ya que no hay Universidades Certificadas con ISO 20000 en Colombia y en ISO 27001 se han adoptado las buenas prácticas pero no todas tienen la certificación en el estándar, la Universidad Pedagógica y

Tecnológica de Colombia, es una Universidad Pública de carácter estatal, que actualmente tiene 27000 estudiantes, 1600 profesores, y 1100 funcionarios y Una sede Central Ubicada en Tunja y 3 sedes seccionales ubicadas en Duitama, Sogamoso y Chiquinquirá en el Departamento de Boyacá. Además de 25 CREADS en diferentes lugares del País.

Cuenta con una infraestructura informática que corresponde con una organización de tamaño medio – alto así:

- Conexiones a Internet y Canales de Datos dedicados.
- Conexión de Fibra óptica entre los edificios y cableado certificado en categoría 5E.
- Data Center con 30 servidores, nivel de seguridad de acceso y respaldo eléctrico en UPS y Planta Eléctrica.
- 23 Sistemas de Información. 20 propios y 3 de terceros.

En la Tabla 1 se observa un resumen de los recursos de Infraestructura por cada una de las sedes:

Tabla 1. Recursos Informáticos de las Sedes de la UPTC. Fuente Grupo Organización y Sistemas UPTC

SEDE	INTERNET	DATOS	COMPUTADORES	CENTROS DE CABLEADO
Tunja	120 Mbps	40 Mbps	1900	23
Duitama	50 Mbps	6 Mbps	250	6
Sogamoso	50 Mbps	6 Mbps	250	7
Chiquinquira	25 Mbps	4 Mbps	100	3
Tunja – Salud		14 Mbps	100	1

.

Luego de contar con el apoyo de la alta dirección la Siguiente estrategia es definir el alcance de las normas, es decir a que dependencias o procesos se va a dar cobertura con la aplicación de las normas. La manera más recomendable de iniciar es elegir el proceso de Tecnología, pues la aplicación de los estándares luego se podrá ampliar a las otras áreas y/o procesos.

En la Universidad se eligió El proceso Gestión de Recursos Informáticos para el alcance de las normas que hace parte de los procesos administrativos dentro del Sistema de calidad. Este proceso es el que contempla las actividades realizadas actualmente en el Grupo Organización y Sistemas que tiene definidas 4 áreas de trabajo:

1. Desarrollo y administración de los sistemas de Información,
2. Redes y Telecomunicaciones
3. Soporte a Usuarios en Hardware y Software.

4. Administración de aulas de Informática para préstamo a Docentes y estudiantes.

El objetivo del proceso es: *"Gestionar La Infraestructura Informática Y De Telecomunicaciones, Que Permita La Prestación De Servicios Para La Satisfacción De Necesidades De Los Clientes"* [3] y contiene 4 procedimientos que integran el quehacer del Grupo Organización y Sistemas dentro de la Universidad Pedagógica y tecnológica de Colombia, así:

- **Procedimiento para la Incorporación de Sistemas de Información**.: Este procedimiento busca identificar y satisfacer las necesidades específicas de los sistemas de información requeridos por los procesos del Sistema Integrado de Gestión de la Universidad Pedagógica y Tecnológica de Colombia, lo cual implica conceptuar para compra, desarrollo y/o implantación de sistema de información
- **Soporte y Administración de Recursos Informáticos**: Este procedimiento busca cubrir las necesidades de todos los procesos del Sistema Integrado de Gestión de la Calidad relacionados con la prestación de servicios que garanticen la funcionalidad básica del hardware y software
- **Seguridad de la Información**: Este procedimiento permite salvaguardar y proteger la información almacenada por los sistemas de información de la Universidad, los cuales gestionan las operaciones transaccionales de la Institución
- **Administración de Aulas de Informática**: Velar por el correcto funcionamiento de la infraestructura informática de las Aulas y coordinar la prestación del servicio según disponibilidad, teniendo en cuenta el número de clientes, recursos de software y hardware

Ahora sí, luego de conocer acerca de la Universidad y del proceso elegido, en el 2011, se presentó el siguiente modelo como propuesta para la implementación de las dos normas:

En la fase inicial o fase 0, se considera realizar un diagnóstico con respecto a las normas planteadas en este documento. En términos de consultoría se denomina análisis GAP o análisis de brecha, con el fin de conocer el estado de la Universidad frente a la norma. Se considera muy importante conocer el estado actual de la Organización, con el fin de evitar esfuerzos en procesos, procedimientos y/o elementos ya existentes. Al finalizar este proceso se obtendrá el diagnóstico de la Organización y se enfocarán los esfuerzos en los dominios con menor cantidad de controles implementados.

En la fase 1 se incluirían la gestión de activos, gestión de riesgos; de parte de la norma ISO 27001 que se complementan con la gestión de capacidad, procesos de presupuesto y contabilidad, y de gestión de Nivel del servicio para la norma ISO 20000.

En una segunda fase, gestión de incidentes, gestión de la cultura, gestión de cumplimiento desde ISO 27001 y des de ISO 20000 los procesos de control, los procesos de relación y los procesos de solución.

Se finalizaría en la tercera fase con la gestión de la continuidad desde ISO 27001 y los procesos de puesta en producción, y gestión de la continuidad y disponibilidad del servicio desde ISO 2000.

En la Figura 1, se puede observar de manera gráfica que procesos se implementarían en cada fase por cada norma.

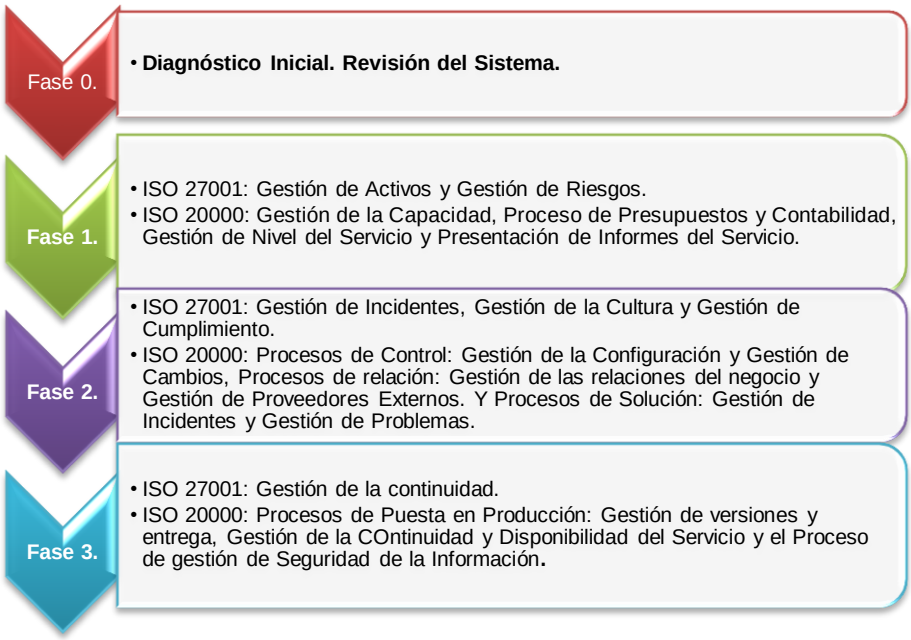

Fig. 1. Fases para la implementación de servicios con las normas ISO 2000 e ISO 27000. Fuente Autor.

Luego de comenzar el proceso se dio un cambio al modelo propuesto, dejando la Fase 0 o fase inicial como estaba prevista, ya que este paso, generó avances importantes y permitió establecer un punto de partida para cada norma.

En la Figura 2, se observa el modelo propuesto luego de la ejecución del análisis GAP para las dos normas.

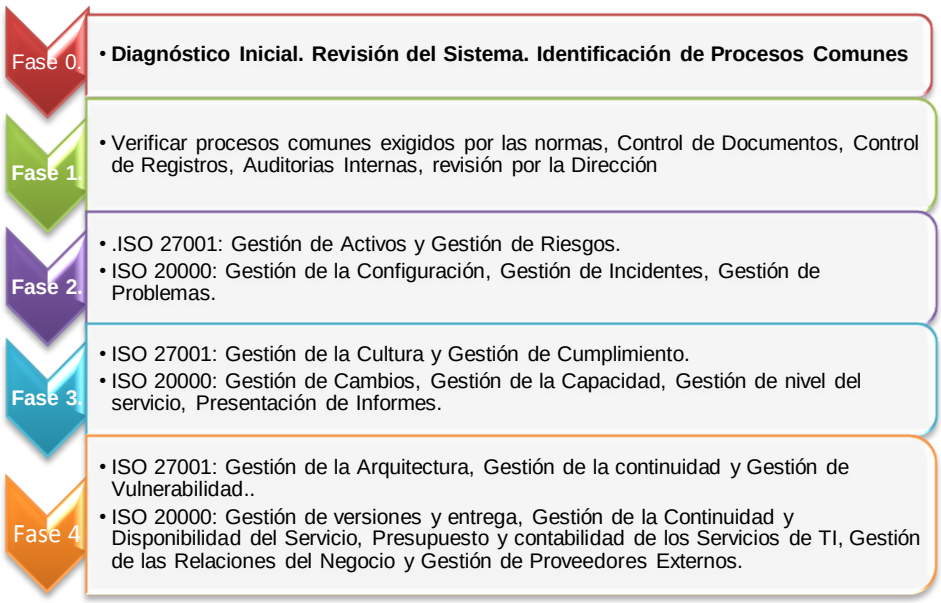

Fig. 2. Fases para la implementación de servicios con las normas ISO 2000 e ISO 27000, luego del Análisis GAP. Fuente Autor.

Como se puede observar el nuevo modelo incluye una fase adicional y en cada una de las fases se realizan las siguientes actividades.

En la fase inicial o fase 0, se realizó un diagnóstico con respecto a las normas planteadas en este documento. Aquí se cuenta con otra estrategia que es contratar con empresas de consultoría expertas en implementación de las normas para adelantar este proceso, así se logró establecer cuál es el estado de la Universidad frente a la norma y así evitar esfuerzos en procesos, procedimientos y/o elementos ya existentes. Como resultado de este proceso se identificó las fortalezas y debilidades frente a lo requerido en cada norma y de las dos se pudo establecer la ventaja de tener organizada ya la Universidad en el trabajo por procesos de acuerdo con la certificación de ISO 900, con lo cual se contaba con los procesos comunes requeridos por la norma.

En la fase 1, se revisó los procesos comunes requeridos por las normas, como son Control de Documentos, Control de registros, Auditorías Internas y Revisión por la Dirección, donde se requerían ajustes pequeños pues ya estaban creados de ISO 9001.

En una segunda fase, gestión de activos y gestión de Riesgos desde ISO 27001 y en conjunto la gestión de incidentes con ISO 20000, además los procesos de Gestión de la Configuración, gestión de incidentes y gestión de problemas.

En la tercera fase se trabajaran los procesos de Gestión de la Cultura y Gestión de Cumplimiento desde ISO 27001 y los procesos de Gestión de cambios, Gestión de la Capacidad, Gestión de Nivel del Servicio y presentación de Informes en lo que tiene que ver con ISO 20000

En la cuarta y última fase la gestión de la continuidad, Gestión de Arquitectura y Gestión de Vulnerabilidad desde ISO 27001 y los procesos gestión de la continuidad y disponibilidad del servicio, Presupuesto y Contabilidad de los servicios de TI, Gestión de las Relaciones del Negocio y Gestión de Proveedores externos desde ISO 2000.

2. Estrategias en la Implementación de los procesos Comunes a las dos Normas.

Como se mencionó anteriormente, de la fase Inicial, se encontró como una ventaja el trabajo realizado con ISO 9001:2008, y donde se observa el proceso Gestión de Recursos Informáticos y los procedimientos que incluye, después de conocer como está conformado el proceso y la infraestructura que administra la dependencia encargada del mismo, es importante presentar los resultados de adoptar el trabajo en el área de sistemas bajo la norma ISO 9001:2008.

Antes del año 2006, se realizaban tareas y funciones relacionadas con la administración de tecnología, de acuerdo a la manera que consideraba la persona que estaba a cargo de la Dirección de Sistemas y de los funcionarios que debían realizar las labores; a partir del año 2006, cuando se dio inicio al trabajo de procesos bajo la norma ISO 9001:2004, se logró tener los procedimientos documentados, para estandarizar el trabajo que se realiza al interior del Grupo Organización y Sistemas, agilidad en la atención de solicitudes de soporte, pues se establecieron tiempos para la atención de los mismos, , Identificación de los servicios que se ofrecían en el Grupo Organización y Sistemas, Control en la atención de las solicitudes, mejora continua del proceso estableciendo acciones de mejora o preventivas cuando se han detectado no conformidades dentro del proceso.

Con la estandarización, se comenzó a trabajar en mejorar las actividades realizadas a través de Sistemas de Información y se consolidó el Sistema Mesa de Ayuda, donde se reciben las solicitudes de soporte de los usuarios, se asignan a un técnico, se atienden y se realiza la actualización en el sistema, estas actividades están contempladas en el Proceso de Administración y Soporte de Recursos Informáticos. Este soporte contempla actividades de Hardware, Software, soporte a los Sistemas de Información, redes y telecomunicaciones.

Para la Administración de las Aulas de Informática, se implementó también un sistema de Información SCAI, Sistema de Control de Aulas de Informática, que permite registrar

las solicitudes de Aulas de Informática que realizan los docentes bien sea para todo el semestre o una fecha específica y luego poder visualizar su horario, además por ser este un procedimiento relacionado con la parte misional de la Universidad que es la Educación, se establecen también actividades encaminadas al alistamiento de las aulas con el software y hardware requerido por los docentes.

El Desarrollo de los Sistemas de Información se documentó en el procedimiento de Incorporación de Sistemas de Información, y garantiza que desde el momento de solicitud de la creación de un sistema de información, un nuevo módulo para uno existente o una mejora, quede documentadas todas las actividades realizadas de análisis, diseño, desarrollo y pruebas desde el modelo de ciclo de vida clásico del Software. Así los funcionarios responsables de estas actividades documentan los sistemas de Información en cada una de las fases.

Garantizar que la Información registrada en los diferentes sistemas de Información se salva guarda de manera apropiada es lo que se logró con el procedimiento Seguridad de la Información, pues ha permitido programar las copias de seguridad de los servidores, y de los equipos activos para no perder configuraciones. Así se garantiza que en caso de algún daño o desastre se pueda recuperar la información con las copias de seguridad diarias de la información de misión crítica.

Finalmente se logró medir el desempeño del proceso a través de los indicadores, con lo cual se puede ver la evolución en la prestación de los servicios y también generar acciones en los casos que se requiera.

Con lo presentado como estado inicial del proceso desde ISO 9001:2008 se realizó el análisis GAP por parte de las empresas consultoras y aquí se encontró de los procesos comunes requeridos por las normas:

1. Proceso Control de Documentos, se tiene ya plenamente establecido, en el cual se protegen y controlan los documentos, además se observa que se tienen previsto las actividades para elaboración, actualización y control de versiones de los documentos que hacen parte de los sistemas de Gestión.
2. Proceso Control de Registros, el proceso existente garantiza que se establecen y se mantienen los registros para establecer la evidencia y la conformidad con la operación y los requisitos de los dos estándares.
3. Proceso Auditorías Internas. Las dos normas lo requieren y este proceso debe contar con los criterios, el alcance, la frecuencia y los métodos de auditoria además los criterios de selección de los auditores.
4. Proceso de Revisión por la Dirección. Se establece la frecuencia, y las entradas para el proceso de la revisión tal como está requerido por los dos estándares.

Además las dos normas tienen procesos en donde se cruzan, así que la estrategia es trabajarlas al tiempo para que el esfuerzo sea uno solo, estos procesos son:

- Proceso Gestión de Incidencias requerido por las dos normas.

- Proceso Gestión de activos en ISO 27001 se relaciona con Gestión de la Configuración en ISO 20000.
- Proceso Seguridad de la Información, requerido por ISO 20000 se cumple con las políticas adoptadas a partir de ISO 27001.

3. Estrategias en la Implementación de la Norma ISO 2000.

La norma ISO 20000, se presenta como una opción para mejorar el proceso desde ISO 9001:2008, en especial para mejorar los procedimientos de administración y soporte de recursos informáticos, ya que involucra muchos elementos de ITIL, ahora es el momento de tener claro el concepto de ITSM, IT Service Management, o en español Gestión de Servicio de las áreas de Tecnología de Información.

ITSM:IT Service Management es la disciplina que se enfoca a la gestión del conjunto "personas, procesos y tecnología" que cooperan para asegurar la calidad de los servicios TI, con arreglo a unos niveles de servicio acordados previamente con el cliente.[4] En la Figura 3 se observa gráficamente la integración del conjunto personas, procesos y tecnología.

Fig. 3. Representación Gráfica del Concepto de Gestión de Servicios de Tecnología.

El hecho de contar con este concepto permite observar que con la administración de los servicios de Tecnología pueden lograr que se realice una Alineación de los servicio de TI con las Necesidades de la Universidad contempladas en el plan maestro de desarrollo, además entregar servicios TI con alta calidad y costos efectivos, estructurar y establecer

buenas relaciones con clientes y proveedores y establecer acuerdos de niveles de servicio y alta satisfacción de los clientes.

Ahora la Norma ISO 2000 incluye el conjunto de los requisitos obligatorios que debe cumplir el proveedor de servicios TI, para realizar una gestión eficaz de los servicios que responda a las necesidades de las empresas y sus clientes, de acuerdo con esa definición, y la contenida en la parte 1 de ISO 2000 el proveedor de servicios de TI [5] es la Organización que tiene como meta lograr cumplir la norma NTC ISO 20000, para el caso de la Universidad es ella el proveedor de servicios TI.

En la figura 4 se observa la relación delos procesos de gestión de servicios que contiene la norma ISO 20000 en su propuesta de actualización para el año 2011, de acuerdo con Linda Cooper[2] [6], donde se ve la interacción de los procesos.

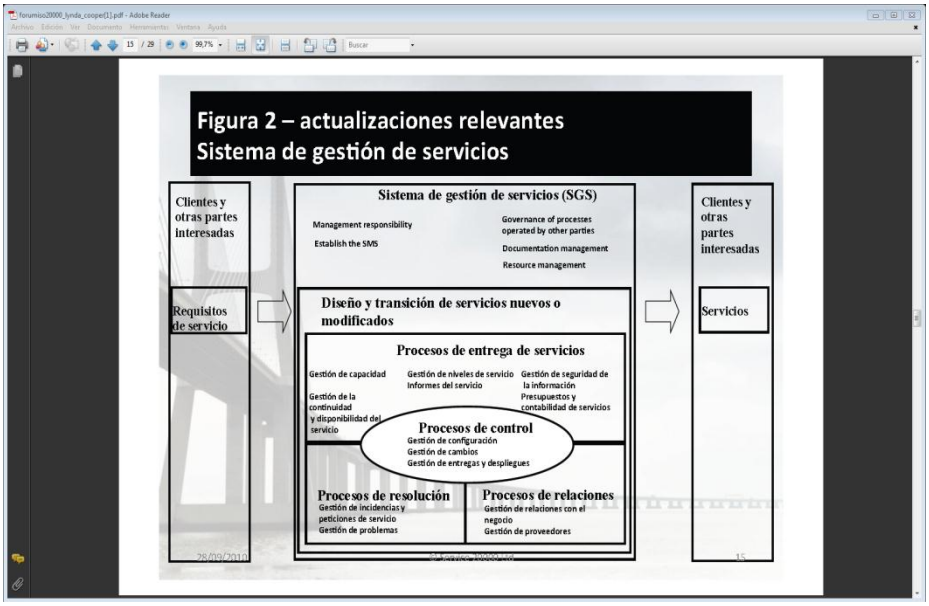

Fig. 4. Relación de los procesos de Gestión de Servicios en ISO 20000.

3.1. Que hacer para lograrlo?

Actualmente las empresas dedicadas a ofrecer servicios de TI, son las mas interesadas en certificar sus servicios bajo este estándar. De tal forma que se han desarrollado diferentes herramientas de Software que ayudan a cumplir los procesos de ITIL que son la base de ISO 20000, es así que con el acompañamiento de la empresa consultora se buscó opciones

[2] Linda Cooper es coautora de la Norma ISO 20000.
RepresentantedelReinoUnidoenISO/IECSC7JTC1WG25.ITILMaster.Formadorayconsultoraindependiente

de herramientas de software que cumplieran con los procesos de ISO 20000 y que ayudaran a implementar de manera más rápida con algunos de los procesos requeridos por la norma: Entra las disponibles se encuentran:

- SAP Solution Manager.
- BMSC Software ITSM V 8.1
- PROACTIVA NET v8
- EASY VISTA 2012
- HELPEOPLE
- ARANDA SOFTWARE

Entre otras más que se pueden encontrar en la página de Pink Elephant http://www.pinkelephant.com/PinkVERIFY/PinkVERIFY_2011_Toolsets.htm el cual es un ente certificador de dichas herramientas para verificar cuantos procesos de ITIL cunplen al 100%.

La Universidad UPTC seleccionó PROACTIVA NET, cumple 10 procesos, es muy fácil de manejar, se encuentra en español y ofrece una interfaz muy amigable al usuario final, con la selección de esta herramienta se contaba con el avance en los siguientes procesos:

1. Gestión de la Configuración y gestión de activos, ofrece diferentes opciones para el levantamiento de información de los diferentes elementos de Configuración que hacen parte de la Infraestructura dela Universidad, es decir equipos de cómputo, portátiles, servidores, impresoras, switch, Teléfonos IP, Software. A partir de esto se puede crear la CMDB, junto con el catálogo de servicios que ofrece el área de TI..
2. Gestión de Incidentes, Gestión de problemas. Ofrece toda la infraestructura para el reporte de incidentes y la debida atención por parte de los técnicos de primer y segundo nivel, además el escalamiento en caso de que se conviertan en problema se puede realizar automáticamente y allí dejar definidos los diferentes reportes de cada caso.
3. Gestión de cambios y Gestión de entregas. Se realizan las solicitudes y se generan los planes requeridos para nuevas implementaciones y la debida implementación de las mismas.
4. Gestión del nivel del servicio y presentación de Informes. La herramienta genera todos los reportes al nivel de detalle que se desee, además allí mismo se crean los acuerdos de niveles de servicio, y se puede realizar el seguimiento del cumplimiento que se le da a los mismos.

Adicional a la selección de la herramienta se debe aprovechar el conocimiento de la empresa consultora para crear las políticas del Sistema de Gestión de Servicios de TI SGSTI, y un primer borrador de la documentación requerida como planes de la gestión del servicio, esto es crear el plan de gestión del Servicio que se entiende como un Plan Estratégico de tecnología Informática que debe ir alineado con los objetivos de la

universidad y el plan de desarrollo para garantizar asignación de fondos y presupuestos, funciones y responsabilidades y riesgos entre otros.

Se debe identificar la relación con los otros procesos como Talento Humano, Jurídica y manejo de proveedores, para implementar los roles requeridos por la norma, la aplicación de acuerdos de nivel de servicio en el manejo de contratos, entre otras características.

Mejorar el proceso actual existente para la gestión financiera, de tal forma que incorpore el presupuesto y contabilidad de los servicios de Tecnología de la Información.

El procedimiento de Seguridad de la Información, se vincula con lo desarrollado en ISO 27001.

Mejorar el proceso existente para el manejo de los proveedores con el fin de que tenga en cuenta los requisitos de la norma, basada en el entendimiento del cliente y su negocio, para los proveedores internos y los proveedores externos.

Una de las estrategias más importantes para lograr llevar a cabo estos cambios y mejoras en el sistema actual es requerido que se capacite al personal del área de tecnología y del sistema de calidad de la Organización acerca de la norma. Hay que motivar mucho al personal de TI, para que vean los beneficios y no lo conciban como más trabajo, socializar con la alta dirección los avances que se van presentando y dejar ver siempre cuales son las ventajas y beneficios que se obtienen con la implementación, enfatizar siempre que el más beneficiado es el usuario final.

3.2. Beneficios de implementar ISO 20000.

La implementación de la Norma ISO 20000 en la Universidad, se obtendrán beneficios como los presentados a continuación que no son solo para el área de Tecnología sino que impactan a la organización logrando evidenciar como el área le agrega valor y al usuario final donde sus solicitudes pueden ser atendidas mejor:

- La estrategia de Tecnología alineada con el Plan de Desarrollo de la Universidad.
- Costos reducidos y controlados, esto se logra a través de la aplicación de los procedimientos de Gestión financiera para el área de TI.
- Tiempo más rápido en la implementación de los cambios, debido a que se encuentran controlados y descritos en los procedimientos, no solo las actividades a realizar en un cambio sino el responsable de llevarlo a cabo.
- Fiabilidad y Disponibilidad del servicio , lo que resulta en la satisfacción del cliente, esto llevado a cabo a través de los acuerdos de nivel de servicio y la correcta gestión de incidencias o de problemas según sea el caso.
- Integración con los proveedores y socios, pues estarán más enfocados en los servicios requeridos por la Organización y el correcto cumplimiento de lo contratado.
- Reducción y Control de los riesgos, aunque en este punto se lograrán mejores resultados combinando con ISO 27000.

- Calidad de los servicios de Tecnología de la Información y Fiabilidad de los Sistemas de Tecnología.
- Motivación y compromiso en el personal.

4. Estrategias en la implementación de la Norma ISO 27001

En lo que se ha mencionado hasta ahora se ha dejado ver puntos de interacción y de integración delas dos normas, así que se va a presentar ahora cómo integrar a ISO 27001 en este panorama de mejorar la gestión de los servicios de Tecnología.
Actualmente son muy comunes los ataques informáticos, y los usuarios que se ven afectados por desconocer de qué manera pueden protegerse, incluso el Estado colombiano ha comenzado programas como Gobierno en línea donde unos de los componentes importantes busca que las organizaciones estatales generen estrategias relacionadas con la seguridad de la Información. Otra iniciativa es la Ley de protección de Datos personales que se aplica al tratamiento de datos personales efectuado por entidades públicas o privadas, dentro del país o cuando el Responsable o Encargado no establecido en territorio nacional lesea aplicable la legislación colombiana en virtud de normas y tratados internacionales. Casos para recordar el ataque hacia la plataforma tecnológica de la Registraduría del Estado Civil de Colombia, durante la realización de las pasadas elecciones presidenciales del mes de junio de 2011, y no muy lejano el de las pasadas elecciones en Venezuela en el mes de abril de 2013, donde ingresaron a la cuenta del entonces candidato Nicolas Maduro.

Otro ejemplo hace referencia a los casos de suplantación de identidad (phishing), mediante correos que supuestamente llegan de nuestras entidades bancarias o de los administradores de nuestras cuentas de correo electrónico y que pretenden mediante un engaño, se haga entrega de los datos de ingreso (usuario y contraseña). Además los más recientes conocidos de estafas e incluso secuestros y muerte a través de los contactos en redes sociales como Facebook.

Estos casos son más comunes de lo que pensamos, solo que en la mayoría de ocasiones no nos enteramos, ya sea porque no son publicadas para no causar pérdida de imagen corporativa, pérdidas económicas, entre otras; o porque la vulnerabilidad es parchada rápidamente.

Con estos ejemplos cobra mayor importancia la implementación de los estándares de ISO 27001 en una organización para proteger no solo la información propia de su negocio, sino para generar la cultura de la seguridad en todos los usuarios ya que la norma es clara cuando indica que la misma es responsabilidad de Todos.

La estrategia aquí nuevamente comienza con contar con la ayuda de expertos, contrate una empresa consultora con experiencia en el mercado en implementación y certificación

en la norma, así los asesores le ayudarán en los procesos más difíciles como son gestión de activos, gestión de riesgos y gestión de la continuidad.

Gestión de activos. La gestión de activos busca, entre otros, identificar todos aquellos activos que componen un proceso o la cadena de valor de la Organización, indicando la propiedad de los mismos. Así mismo se deben establecer las directrices de clasificación de los activos identificados, además de los procedimientos para etiquetar y manejar la información. Todo esto se puede resumir en el inventario y clasificación de activos de información.

Activo: cualquier cosa que tiene valor para la Organización. Ejemplo de activos son: documentación, software, personas, imagen, servicios, etc. [7]

Dado que es el primer paso, de esta tarea se desprenden los insumos necesarios para procesos posteriores y es muy importante que se realice concienzudamente, involucrando personal de la Organización, pues no más que ellos son los que conocen a fondo los procesos, Además se logra avanzar con la base de datos de la gestión de la configuración (CMDB), que se obtiene de las buenas prácticas de ISO 20000 y que se nombraba anteriormente que sería alcanzable con la herramienta de software.

La información que resulta de este proceso aporta la metodología para la valoración de activos que es requerida por la norma y se une con la gestión de configuración en ISO 20000

Gestión de riesgos. Comprende el conjunto de actividades para controlar y dirigir la identificación y administración de los riesgos de la seguridad de la información para poder alcanzar los objetivos del negocio. En este punto se trabaja con los activos inventariados y clasificados anteriormente y para lograr el objetivo es necesario identificar las amenazas contra tales activos y las vulnerabilidades que se pueden aprovechar. La gestión de riesgos debe garantizar que el impacto de las amenazas que explotan las vulnerabilidades estén dentro de los límites y costos aceptables.

El riesgo es una característica inherente en el negocio y resulta muy complejo y costoso eliminar todos los riesgos, por lo que toda Organización tiene un nivel de riesgo que acepta. Según la norma, las características a tener en cuenta en el evento de la materialización de un riesgo son la Confidencialidad, la Integridad y la Disponibilidad [8], lo cual genera un impacto ya sea de imagen, financiero, ambiental, legal o humano.

Como resultado de este proceso se obtiene tratamientos inmediatos, o en el peor de los casos planes de tratamiento para, reducir la probabilidad de ocurrencia, reducir el impacto, evitar el riesgo o transferir el riesgo. Tales tratamientos se expresan mediante controles.

Se puede consultar la norma ISO 27005 o metodologías tales como OCTAVE, MAGERIT o CRAMM, con el fin de obtener un acercamiento más adecuado a la gestión de riesgos, sin embargo la norma no exige alguno en específico solamente que se cuente con una metodología que es lo que resulta de este proceso.

Gestión de la continuidad. Consiste en desarrollar y administrar una capacidad para responder ante incidentes destructivos y perjudiciales, relacionados con la seguridad de la

información y la forma de recuperarse de los mismos. En otras palabras, permitirle a la Organización continuar con sus operaciones en caso de una interrupción y restaurar los servicios tan rápida y eficazmente como sea posible.

En este punto es importante la realización de tres etapas:

- Análisis de impacto al negocio, BIA
- Análisis de riesgos por pérdida de disponibilidad
- Definición de la estrategia(s) de recuperación

Al finalizar, la Organización contará con un documento, que, dependiendo del alcance (DRP, BCP), contiene todos aquellos procedimientos que involucran tecnología, personas, procesos, etc, el cual debe ser actualizado ante cualquier cambio de estos elementos, debidamente probados y con roles y funciones claramente definidas. Para ampliar información al respecto se recomienda tener en cuenta la norma BS 25999. Aquí cuenta mucho el alcance definido para establecer cuál es el alcance también del plan de continuidad en su primera versión, pues vale la pena tener en cuenta que se va madurando en la medida que el Sistema de Gestión de Seguridad de la Información se va consolidando en la organización.

Gestión de la cultura en seguridad de la información.. Para llevar a buen término la implantación de un SGSI es importante tener en cuenta las personas. Todo el personal de la Organización debe estar involucrado y debe hacer parte activa del proceso y parte de la exigencia de la norma de contar con el apoyo manifiesto de la Alta Gerencia.

La gestión de la cultura incluye desde la inclusión del personal en todo el proceso del SGSI, su capacitación, hasta la creación de políticas producidas y promovidas por la gerencia, que deben ser publicadas y conocidas por clientes, proveedores, empleados y contratistas de la Organización. Estrategias realice un primer levantamiento de información a través de encuestas y entrevistas y luego divulgue a través de diferentes medios como radio, videos, correos, pagina web, intranet.

Gestión del cumplimiento. Hace referencia al cumplimiento de todos aquellos requisitos legales, políticas y normas de seguridad de la información y algunas consideraciones de auditoría exigidas por la norma. Se debe tener en cuenta toda la normatividad aplicable. Estrategia, involucre desde el inicio en el análisis GAP al área o proceso de jurídica y capacítelos frente a los controles requeridos en la norma para contar con la ayuda de ellos en la aplicación de lo que se debe realizar para dar cumplimiento a la norma.

Gestión de incidentes. Este proceso se complementa con ISO 20000 y se realiza la aplicación en la herramienta de Software, en el catálogo de servicios se crea una categoría relacionada con la Seguridad de la Información, sin embargo se debe tener en cuenta la definición de incidente dentro de la norma ISO 27001: evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad

significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.[9]

Gestión de Vulnerabilidad. Para la aplicación de este proceso, contrate una empresa experta o personal experto en realizar test de vulnerabilidad, que le garantice que no se realizará afectación de los servicios, pero sobre todo la confidencialidad de los resultados del test, así como sugerencias en la mejora de las vulnerabilidad encontradas y a partir de allí generar un plan de tratamiento de las mismas.

Gestión de Arquitectura. De la mano con la gestión de activos y la Gestión de la configuración se deben generar las políticas requeridas para garantizar el acceso y control de la arquitectura de red y comunicaciones de la Organización. Este trabajo se debe realizar con el personal del área de TI encargado de los roles de administración y seguridad de la red

Conclusiones.

- Cuente con el apoyo de la Alta Dirección.
- Contrate con empresas expertas para dar inicio al proceso.
- Si ya cuenta con una gestión por procesos como ISO 9001:2008 ya hay bastante abonado para los procesos comunes. Sino el trabajo por procesos sirve para las dos normas.
- Reúna a los líderes de procesos como talento Humano, Financiera, Proveedores y Jurídica.
- Capacitar al personal del área de TI en las normas.
- Socialice y capacite a otros líderes de proceso
- Genere estrategias para la divulgación a los usuarios finales, videos, radio, impresos, mensajes al correo, en la intranet.
- Para ISO 27001 permita que los asesores de la empresa consultora realicen el análisis GAP, la gestión de activos, gestión de riesgos y gestión de continuidad.
- Empodere al personal de Administración de redes y servidores para generar políticas para proteger los activos de los equipos.
- Capacitarse en Auditorías internas de cada norma para conocer el punto de vista del auditor y preparase para las auditorías internas y de certificación.
- Realice auditorías internas.

Referencias

1. Departamento de Informática es Considerado un Gasto. Fuente Setesca. 29/03/2011. http://www.diarioti.com/gate/n.php?id=29358.
2. INSTITUTO COLOMBIANO DE NORMA TECNICAS Y DE CERTIFICACION. Norma Técnica de Calidad en la Gestión Pública NCTGP 1000:2009. P 1.
3. Sistema Integrado de Gestión Académico Administrativa SIGMA. http://desnet.uptc.edu.co/Sigma.
4. OSIATIS. Formación ITIL, Fundamentos de la Gestión de Servicios de TI. http://www.osiatis.es/formacion/Formacion_ITIL_web_version2.pdf.
5. INSTITUTO COLOMBIANO DE NORMA TECNICAS Y DE CERTIFICACION. Norma Técnica Colombiana. NTC-ISO/IEC 20000-1. P 3.
6. Cooper, Linda.: La Evolución de la ISO 20000, 1er Forum Internacional ISO 20000, marzo de 2011. www.forumiso20000.com
7. INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y DE CERTIFICACIÓN. Norma Técnica Colombiana Sistemas de Gestión de la Seguridad de la Información. NTC-ISO/IEC 27001. P 2.
8. INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y DE CERTIFICACIÓN. Norma Técnica Colombiana Sistemas de Gestión de la Seguridad de la Información. NTC-ISO/IEC 27001. P 5.
9. INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y DE CERTIFICACIÓN. Norma Técnica Colombiana Sistemas de Gestión de la Seguridad de la Información. NTC-ISO/IEC 27001. P 3.