Visión de los beneficios de implementar servicios de TI, con estándares como ISO 20000 e ISE 27001 en una universidad pública colombiana

[a] Diana Rocio Plata Arango[1], [b]Fabian Andrés Medina Becerra[2]

[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

[b]Universidad Pedagógica y Tecnológica de Colombia, Facultad Sogamoso Docente Ingenieria Industrial, Sogamoso, Colombia.
fabian.medina@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, normalmente el paso inicial es el estándar ISO 9000 que le permite a las organizaciones, documentar y estandarizar procesos, para el caso colombiano en las entidades de carácter estatal es obligatorio certificar los servicios bajo la Norma Técnica NTCGP:1000, que contiene a la norma ISO 9001:2008, sin embargo luego de este proceso que implica demostrar que se ha iniciado un trabajo dentro de estándares de calidad, queda la pregunta ¿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 27000, de acuerdo a los servicios que ofrecen. Este documento presenta un caso de Implementación de la norma ISO 9001, para el Grupo Organización y Sistemas (área de Tecnología), en la Universidad Pedagógica y Tecnológica de Colombia, UPTC, y cuál es el panorama para implementar algunos servicios de atención al usuario bajo la norma ISO 20000, y otros servicios de Seguridad bajo la norma ISO 27001, que se debería hacer en cada caso y que beneficios o ventajas le representaría a la Universidad tomar este camino.

Palabras Clave: Gestión de Servicios de TI, Buenas prácticas, ISO 9000, ISO 20000, ISO 27000, Mejora Continua, IT Service Management.

---

[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.

[2] Ingeniero de Sistemas. Especialista en Automatización Industrial. Especialista en Seguridad de la Información. En curso maestría en Seguridad Informática.

1. Introducción

La calidad es un tema que siempre se discute en las Organizaciones, y las Instituciones de Educación Superior, no son ajenas a esa discusión, pues el término "calidad", abarca diferentes opciones dentro del ámbito académico, se requiere calidad en los programas académicos, en la infraestructura, en los procesos, en los materiales educativos y obviamente en la Infraestructura Informática que respalda la misión de las Universidades.

Sin embargo, el término calidad, también es muy amplio y puede tener diferentes criterios, para este caso se aborda desde el punto de vista de cómo mejorar la calidad de los servicios de Tecnología dentro de la Universidad garantizando que se le aporta valor a la organización y que el área de tecnología acredita los servicios prestados a través de estándares.

la Inversión en los departamentos de Tecnología es considerada como un gasto [1] de acuerdo con un estudio elaborado por la consultora SETESCA, basado en una encuesta realizada a más de 1000 CEO's y directores generales, el departamento de informática es uno de los peor percibidos en la relación valor añadido–coste en los procesos estratégicos empresariales.

"Según la investigación, las principales causas para tal valoración son la percepción del departamento de informática como un coste y no como un valor diferencial, la ausencia de comunicación respecto al valor real aportado y la falta de proactividad en la mejora de los procesos de negocio"[3], junto con la percepción del incumplimiento general en la entrega de los proyectos.

Una estrategia para el cambio de esa percepción es enfocar estrategias de buenas prácticas bajo los estándares internacionales que demostrarían, 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.

Además cada día es más común escuchar que se han sufrido ataques informáticos, ejemplos en Colombia para las pasadas elecciones de junio de 2010, o algunos ataques a la banca, Estos casos son más comunes de lo que se piensa, solo que en la mayoría de ocasiones no se conoce la información, ya sea porque no son publicadas para no causar pérdida de imagen corporativa, pérdidas económicas, entre otras; o porque la vulnerabilidad es parchada rápidamente.

Una pregunta recurrente es, cómo evitar este tipo de incidentes? Aunque la respuesta no es tan precisa como quisiéramos, si se puede estar preparado y de alguna manera controlarlos. Una respuesta inmediata es, realizando un debido análisis y evaluación de riesgos, tomando como referencia un modelo formal de seguridad, como por ejemplo la norma ISO 27001.

Este Documento presenta inicialmente como fue el proceso de implementación y certificación en ISO 9001:2008 para la Universidad Pedagógica y Tecnológica de Colombia, y como el área de Tecnología, certifico su proceso, destacando que beneficios se obtuvo con esta certificación, luego se encuentra una visión de que se puede lograr si se adoptan buenas prácticas en servicios bajo estándares como ISO 20000 e ISO 27000, destacando los pasos a seguir para lograr la adopción de esas buenas prácticas y al finalizar se presentan unas conclusiones, de lo expuesto.

[3] SETESCA es una empresa española dedicada a la reducción de costes e incremento de la productividad en los sistemas de información. URL www.setesca.com

2. Proceso de Implementación y Certificación de los procesos en ISO 9001

Desde el año 2005, la Universidad Pedagógica y Tecnológica de Colombia comenzó el proceso de certificación de los procesos Administrativos en la Norma ISO:9001 versión 2004, pasando por una etapa de capacitación interna a funcionarios para garantizar el conocimiento de la Norma y una asesoría para lograr la implementación ,en diciembre de 2006, se obtuvo el certificado de calidad para los procesos administrativos que incluían el Proceso Gestión de Recursos Informáticos , que cubre el área de Tecnología de la Universidad que es denominada Grupo Organización y Sistemas.

Luego en el año 2007, comenzó un nuevo trabajo, que consistió en preparar a la Universidad para certificar todos los procesos académicos y administrativos bajo la norma de calidad colombiana NTCGP:1000:2004, y que se actualizó en el año 2009, La denominación NTCGP[4] corresponde a las siglas de "Norma Técnica de Calidad en la Gestión Pública" que toma como base las normas internacionales ISO 9000:2005 y la ISO 9001:2008 sobre gestión de la calidad, por lo tanto el cumplimiento de la norma NTCGP 1000, permite el cumplimiento de la norma ISO 9001:2008,puesto que ajusta a la terminología y los requisitos de ésta a la aplicación específica en las entidades [2].

Se realizaron diferentes actividades para conocer la diferencia con la norma en la que ya la Universidad ya estaba certificada, y se observó que la norma NTCGP 1000, es aplicable a las entidades de la rama ejecutiva del poder público y otras entidades prestadoras de servicios, e integra requisitos y conceptos adicionales a la norma ISO, en resumen busca cumplir con eficacia, eficiencia y efectividad los resultados de los procesos junto con la Mejora continua y satisfacción de los clientes logrando integrar el Modelo Estándar de Control Interno y Sistema de Desarrollo Administrativo en el Sistema de Gestión de la Organización, esto permite que se integre entre otros la gestión de riesgos dentro del Sistema de calidad..

Luego de tener claras las diferencias y de recibir la capacitación y asesoría se consolidó en la Universidad el Sistema de Gestión Integrado Académico Administrativa SIGMA, que en Febrero de 2010 fue certificado por parte del ICONTEC, Instituto Colombiano de Normas Técnicas y Certificación, para todos sus procesos. Está conformado por 7 macro procesos, y 32 procesos, el mapa de procesos se observa en la Figura 1.

El proceso Gestión de Recursos Informáticos hace parte de los procesos administrativos y se observa en la Figura 1.

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

[4] La sigla NTCGP, no debe confundirse con la sigla NTC Utilizada por el Organismo Nacional de Normalización en la redacción de otras normas técnicas de carácter voluntario.

- **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

La documentación total del proceso consta de 1 guía, 31 formatos, 7 instructivos y 5 indicadores.

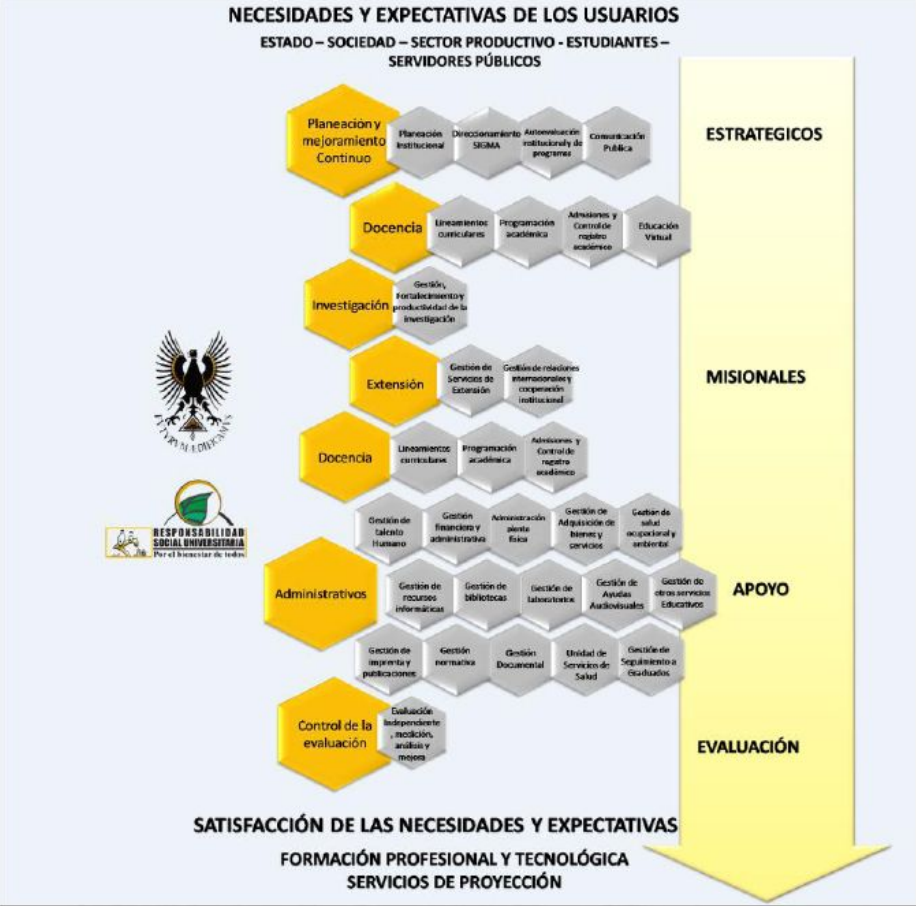

Fig. 1. Mapa de procesos de la UPTC. Se observan los 7 macroprocesos y 32 procesos. Fuente: SIGMA- UPTC.

El Grupo Organización y Sistemas tienen 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.

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

- Una sede Central Ubicada en Tunja y 3 sedes seccionales ubicadas en Duitama, Sogamoso y Chiquinquirá en el Departamento de Boyacá.
- 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	60 Mbps	8 Mbps	1900	23
Duitama	35 Mbps	2 Mbps	250	6
Sogamoso	35 Mbps	2 Mbps	250	7
Chiquinquira	10 Mbps	1 Mbps	100	3

La Universidad cuenta con una población de 26000 estudiantes, 1536 docentes, y 1031 funcionarios.

2.1 Qué se ha logrado con la implementación de ISO 9001:2008?

En la sección anterior se describía el proceso que ha llevado la Universidad, para lograr la implementación y certificación de su Sistema Integrado de Gestión, para todos los procesos académicos y administrativos, 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.

Además el Grupo Organización y Sistemas apoyo el Sistema de Gestión de manera transversal y desarrolló un Sistema de Información para almacenar toda la Documentación del Sistema, además de crear y guardar directamente en el sistema los procesos, procedimientos, sin necesidad de generar información en procesadores de Texto como Word, todo se almacena directamente en el Sistema de Información. En la Figura 2, se observa una pantalla de opciones del Sistema SIGMA.

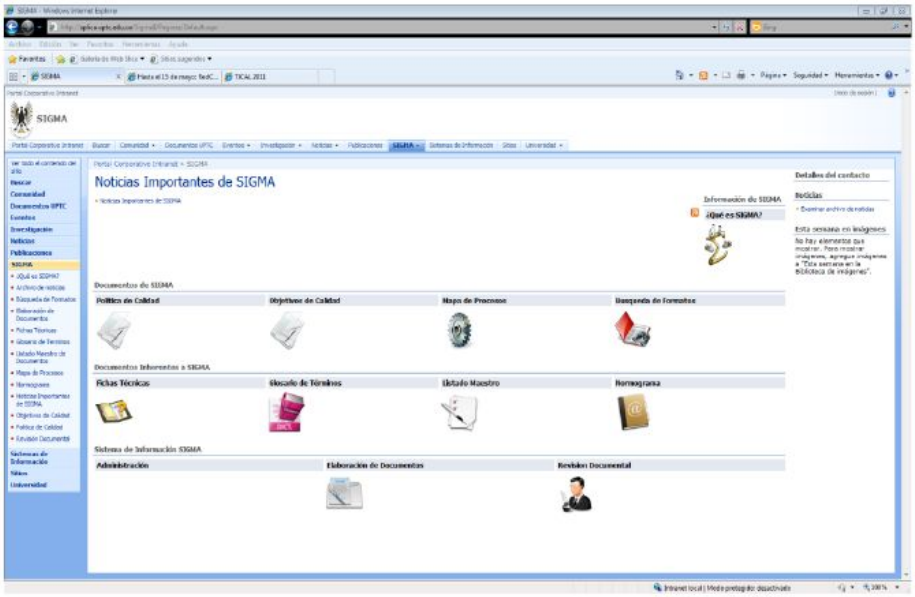

Fig. 2. Sistema de Información SIGMA que respalda toda la documentación de los procesos del Sistema Integrado de Gestión Académico Administrativo SIGMA.

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.

3. Servicios que se Pueden Implementar bajo la Norma ISO 2000.

Los beneficios de trabajar bajo un estándar como ISO 9001:2008 se revisaron en la sección anterior, pero buscando cumplir con ese mismo estándar se observa que dentro de la mejora continua, y dado el tamaño de la organización, del inventario de elementos que se debe administrar y de los servicios que se prestan por el Grupo organización y sistemas se deben buscar estrategias que permitan garantizar los servicios de TI y la gestión que se realice sobre estos.

La norma ISO 20000, se presenta como una de estas alternativas, 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[5] [6], donde se ve la interacción de los procesos.

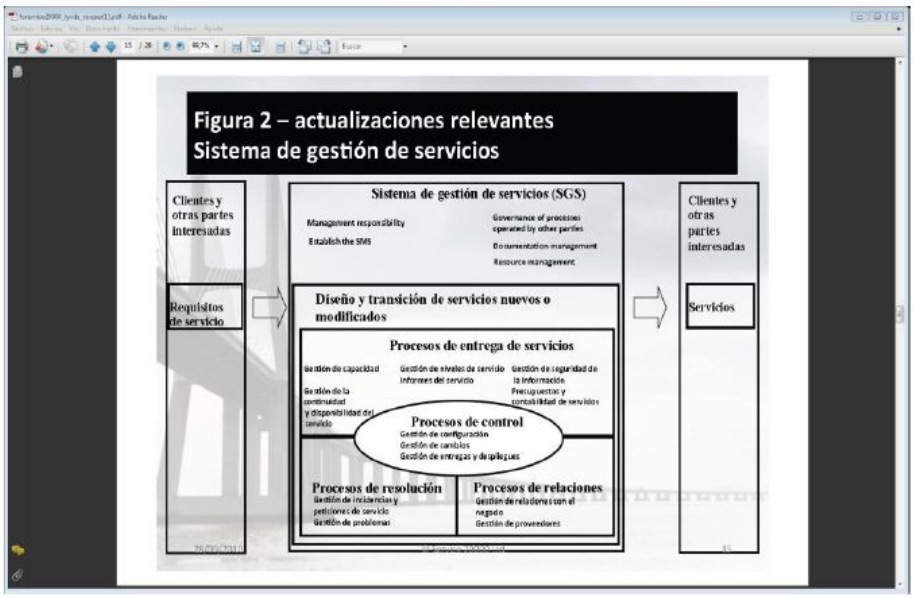

Fig. 4. Relación de los procesos de Gestión de Servicios en ISO 20000.

3.1. Cómo llevarlo a cabo?

Dentro de lo que tiene actualmente la Universidad, y para certificar el servicio de soporte a los usuarios se requiere, tener en cuenta pasos como los siguientes:

- Crear una política en el Sistema de Gestión de Calidad que permita la gestión y la implementación efectiva de todos los servicios de Tecnología de la Información.
- Mejorar la documentación de los procedimientos existentes que ayuden a cumplir con los requisitos de la documentación, que incluyan las políticas y planes de la gestión del servicio y los acuerdos de niveles de servicio, además de crear los nuevos procedimientos requeridos por la norma.
- 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 deben crear todos los procesos exigidos por la norma que no existen hoy en el mapa de procesos de ISO 9000, que serían:
- Proceso de implementación de nuevos servicios o servicios modificados.

[5] Linda Cooper es coautora de la Norma ISO 20000. Representante del Reino Unido en ISO/IECSC7JTC1WG25. ITIL Master. Formadora y consultora independiente.

- Proceso de Prestación del servicio, que consistiría en modificar el procedimiento actual de administración y soporte de recursos informáticos, para lograr incorporar los acuerdos de niveles de servicio, la documentación de los mismos, junto con los informes que se deben presentar y lograr la gestión de la continuidad y disponibilidad del servicio.
- 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.
- Crear el procedimiento de Gestión de la capacidad.
- Crear el procedimiento de Seguridad de la Información, y desde este vincular lo que se verá en el capítulo siguiente de la norma 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.
- Crear los procesos de solución, para gestión de incidentes y gestión de problemas. Identificando muy bien cada uno de ellos para dar la solución correcta en cada caso.
- Establecer los procesos de control, donde se incorpora la Gestión de la configuración y la gestión del cambio y se busca que el enfoque sea integrado para la planificación de los dos. Para estos procesos es bueno contar con alguna herramienta de software puede ser de las existentes en el mercado o desarrollar una que permita tener la base de datos de la gestión de la configuración, se considera para el servicio de soporte que se desearía implementar bajo estas buenas prácticas que los elementos de configuración a administrar son todos los equipos de cómputo de la Universidad.
- Implementar el proceso de puesta en producción.

Al trabajar en la documentación requerida y probar los procesos y procedimientos, se pasaría de tener 1 solo proceso para el área de tecnología a tener por lo menos 5 más con alrededor de 12 procedimientos.

Como está alineado con ISO 9001, se pueden realizar auditorías a los procesos y procedimientos implementados para cumplir con lo requerido y determinar las acciones a que haya lugar, en el sistema actual existe el proceso de auditorias internas ya muy bien establecido y tiene un sistema de información de apoyo para llevar a cabo la preparación de la auditoría y la presentación de los informes al final del proceso.

Para llevar a cabo estos cambios y mejorar 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 y que se pueda contar con asesoría de personal experto mientras se realiza la implementación.

3.2. Beneficios de seguir Buenas Prácticas con ISO 20000

Al implementar buenas prácticas para el servicio de soporte y atención a usuarios que es transversal a toda la gestión de Tecnología que se realiza en la Universidad, se obtendrían 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:

- 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. Qué Servicios se pueden Implementar bajo la Norma ISO 27001

Hasta este punto se ha presentado que se puede hacer para implementar algunas buenas prácticas con ISO 20000, en el proceso Gestión de Recursos Informáticos existente en la UPTC, a partir de la certificación que tienen con ISO 9001:2008, y en puntos como seguridad de la información y manejo de riesgos se nombro que se realizaría mejor con ISO 27001, así que se va a presentar ahora cómo integrar a ISO 27001 en este panorama de mejorar la gestión de los servicios de Tecnología.

Las vulnerabilidades son un tema común actualmente, según algunas fuentes periodísticas y de organismos del Estado, se realizó un 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, desconociendo hasta el momento los motivos del mismo, es decir, si se realizó para alterar algún resultado o simplemente por crear caos e inestabilidad en la información procesada.

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).

Caso reciente de Bancolombia, cuyos clientes aparecían con saldos que no correspondían a la realidad, causando un gran caos y confusión, no solo entre clientes sino socios comerciales y filiales extranjeras, a lo cual Bancolombia respondió que se trataba de fallas técnicas, más no de ataques. Para ampliar esta información se recomienda ver: http://www.portafolio.com.co/noticias/finanzas/tecnologia-golpea-el-servicio-de-banca.

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, en la Figura 5 se observa una estadística de este tipo de ataques y se puede comprobar que el número va en aumento.

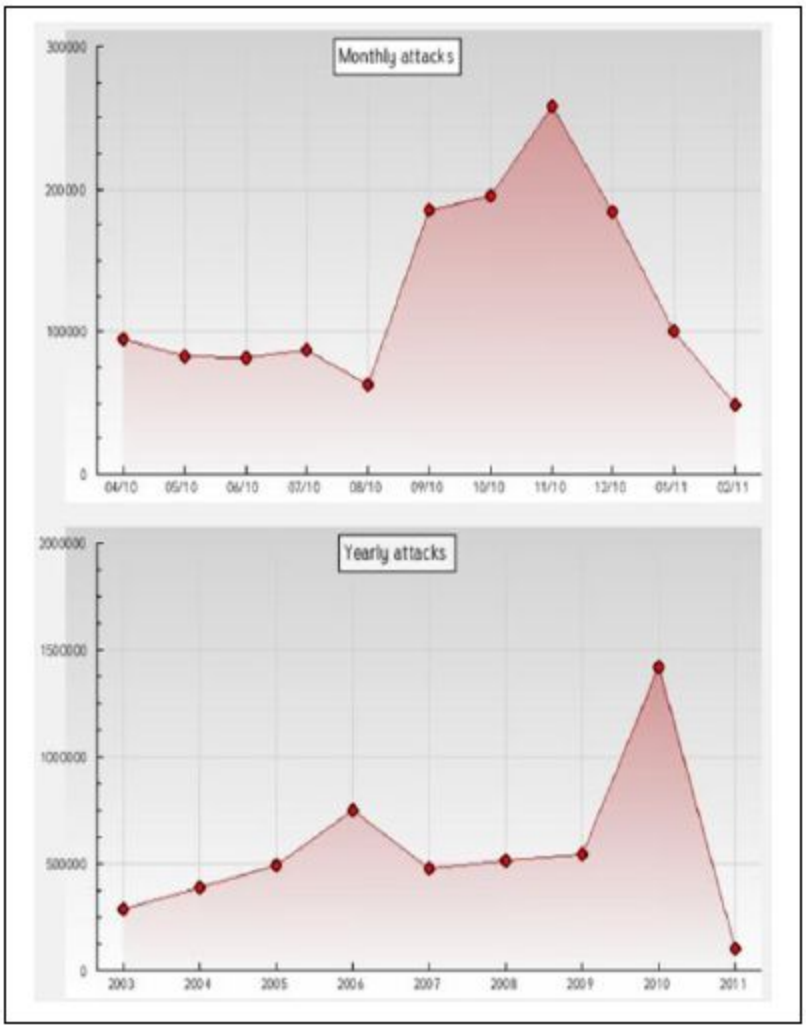

Fig. 5. Estadísticas de ataques. Mensual y anual.
Fuente: http://www.zone-h.org/stats/ymd

Una pregunta recurrente es, cómo evitar este tipo de incidentes? Aunque la respuesta no es tan precisa como quisiéramos, si se puede estar preparado y de alguna manera controlarlos. Una respuesta inmediata es, realizando un debido análisis y evaluación de riesgos, tomando como referencia un modelo formal de seguridad, como por ejemplo la norma ISO 27001.

Un ejemplo lo podemos ver en la circular 052 de la Superintendencia Financiera de Colombia, en la cual se imparten instrucciones relacionadas con los requerimientos mínimos de seguridad y calidad en el manejo de información, a través de medios y canales de distribución de productos y servicios para clientes y usuarios. (http://www.superfinanciera.gov.co).

Si bien es cierto que la norma es clara y debe ser llevada a la práctica, cómo debe ser la estrategia a seguir para que una Organización tenga en cuenta la ISO 27001 y lleve a cabo con éxito su implantación?

Si no es posible contar con un experto en la materia o carece de recursos financieros para contratar una empresa de consultoría, o simplemente hacer realidad este proceso, a continuación se presenta una estructura de la misma norma que pretende mostrarlo de una forma más clara.

4.1 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. En este punto es bien importante resaltar la ventaja que la Organización cuente con un enfoque basado en procesos, es decir, que su cadena de valor sea fácilmente identificable, de no ser así la labor sería mucho más compleja. Ventaja que ya posee la UPTC, con su certificación en ISO 9001:2008., 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 a través de algún software de los que ya existen en el mercado y que involucran estándares de ITIL.

4.2 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. En la Figura 6 se puede apreciar las relaciones entre los diferentes elementos que intervienen en la gestión de riesgos.

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.

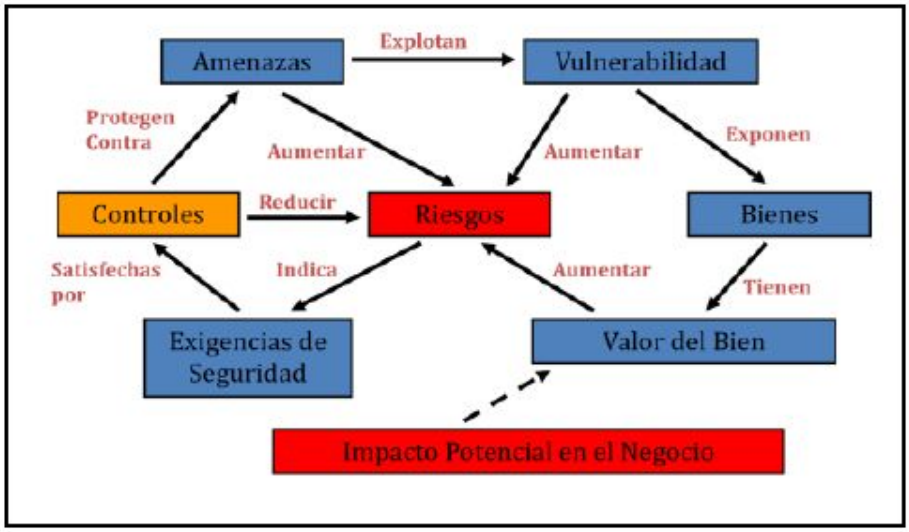

Fig. 6. Relación riesgo – amenaza – vulnerabilidad – control.

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.

4.3 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.

4.4 Gestión de la cultura en seguridad de la información

Premisa: no existen parches para lidiar con el desconocimiento de las personas. 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.

4.5 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 deben tener en cuenta leyes (Habeas data y Delitos Informáticos, por ejemplo), normatividad del sector (circulas 052 y 038 de la SFC), normatividad interna (resoluciones), políticas (de seguridad de la información) y en general todos aquellos requisitos legales y de cumplimiento que la Organización debe cumplir.

Para lograr este objetivo es necesario iniciar por la revisión de las políticas actuales, generar la declaración de aplicabilidad, definir la política de seguridad corporativa, además de los estándares y procedimientos necesarios para dar cumplimiento a lo estipulado tanto en los requisitos como en los controles. Es posible contar con el asesoramiento de un experto en derecho informático.

4.6 Gestión de incidentes

El último y no menos importante proceso, hace referencia a la gestión de incidentes. Es muy importante resaltar 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].

Se debe contar con un procedimiento, escalado, si es necesario, para darle tratamiento a todos los incidentes que se presenten en la Organización, desde el ingreso de un virus hasta la sustracción de información por cualquier medio, es decir, la Organización debe estar preparada en caso de ocurrencia seguir el procedimiento con el fin de superar el evento.

5. La Propuesta

En principio todo lo anterior parece una tarea colosal, de hecho lo es, si se tomaran todos los procesos de la Organización y si se realizara en un solo esfuerzo. Una de las maneras más prácticas de llevar a cabo un proyecto de este tipo, y así lo han realizado Universidades Colombianas, tales como la Universidad del Valle y la Universidad Tecnológica de Pereira, consiste en dividirlo en fases, de tal forma que en cada fase se incluya los elementos de gestión anteriormente mencionados, para el caso de la Universidad Pedagógica y tecnológica de Colombia representa una ventaja contar ya con un modelo funcionando por procesos bajo el enfoque de norma ISO 9001:2008.

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 7, se puede observar de manera gráfica que procesos se implementarían en cada fase por cada norma.

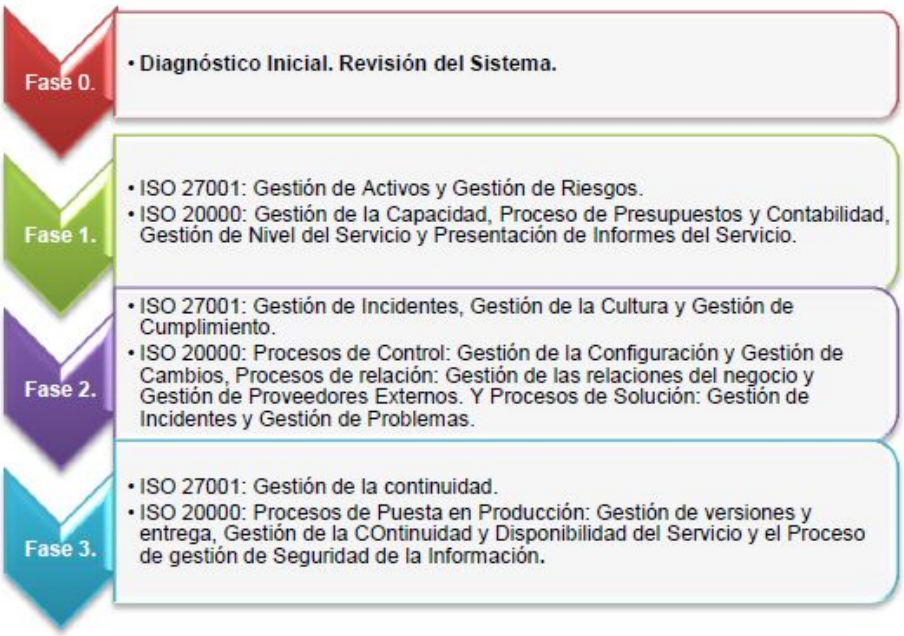

Fig. 7. Fases para la implementación de servicios con las normas ISO 2000 e ISO 27000. Fuente Los Autores.

Lo anterior llevado a la realidad, en términos de tiempo, puede variar de acuerdo a los recursos asignados. Para el caso de las Universidades mencionadas, el tiempo no fue superior a tres años, pero como se indicó, pueden ser más cortos si se tuviera mayor disponibilidad de los recursos.

Todo este proceso no necesariamente con el fin de obtener la certificación, sino, con el propósito de adaptar normas y estándares al día a día de la Universidad, haciendo un uso eficiente de los recursos informáticos y administrativos. Además de esas fases para la implementación se debería realizar una auditoría de tercera parte que permita medir la madurez del sistema y lograr establecer si se está preparado o no para una certificación.

Conclusiones

- La seguridad de la información debe ser parte del día a día de la Organización y deben intervenir todos y cada uno de los involucrados en cada uno de sus procesos
- El modelo por procesos establecido con ISO 9000, se convierte en una ventaja y avance a la hora de implementar otros estándares.

- Con la Gestión de los servicios de Tecnología se logra la alineación del Plan Estratégico de Tecnología Informática con el Plan de Desarrollo de las Organización.
- Entregar servicios de calidad en el área de TI, permite garantizar la satisfacción de los usuarios y mejorar los tiempos de respuesta del área en la prestación de los servicios.
- La disminución de los costos es un factor a realzar, ya que se realizarán las inversiones de manera planificada y organizada, con presupuestos asignados con anterioridad y no bajo improvisación.
- Los acuerdos de niveles de servicio se convierten en una herramienta, para garantizar no solo la correcta atención de los servicios a los usuarios, sino también para que los proveedores cumplan de manera adecuada y oportuna con los compromisos adquiridos.
- En la implementación e implantación de un SGSI se requiere la participación de profesionales de diversas disciplinas, tales como Ingenieros de Sistemas, Electrónicos, Industriales, Contadores, Administradores, etc.
- Es necesario que al interior de las Organizaciones se tome conciencia de las amenazas a las que se ve expuesta por razones inherentes a su objetivo y tomen las medidas correspondientes.
- El sistema de Gestión para el área de TI, debe ser auditado para garantizar la evaluación de sus procesos y generar las acciones que corresponda.

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.