¿DE ISO 20000 e ISO 27001 LA EVOLUCIÓN HACIA UN MODELO DE GOBERNANZA EMPRESARIAL DE TI?

Diana Rocio Plata Arango
Diana.plata@uptc.edu.co

AGENDA

- INTRODUCCION
- CARACTERISTICAS DE UPTC
- CONCEPTOS
- GOBERNANZA Y MARCOS DE REFERENCIA
- AVANCES EN EL MODELO DE IMPLEMENTACION PROPUESTO

INTRODUCCIÓN

- La Universidad Pedagógica y Tecnológica de Colombia UPTC, comenzó en el año 2011 un proyecto para la implementación de las normas ISO 20000-1 e ISO 27001, con el fín de lograr la certificación.
- Este proyecto busca mostrar la importancia que ha tomado hoy en día para las áreas de Tecnología de las diferentes Organizaciones, el hecho de contar con Gestión de las Tecnologías de la Información y obviamente las Universidades no están fuera de este alcance.
- La Universidad Pedagógica y Tecnológica de Colombia ha establecido su modelo de gestión para el área de TI a través de la implementación de las normas mencionadas anteriormente, el objetivo desde la organización es lograr la satisfacción de los clientes, gestionar la inversión en el área de TI, alineada con el plan estratégico de la Universidad y garantizar buenas prácticas en la seguridad de la información.

INTRODUCCION.

- Actualmente se han establecido los procesos requeridos por las normas, y la documentación necesaria para cumplir el objetivo; y dado que hoy en día se habla de la Gobernanza o gobierno de TI, vale la pena mirar dentro de todos los marcos y estrategias, en donde se ubican estas dos normas y cómo se puede evolucionar hacia un modelo de Gobernanza empresarial de TI a partir de la experiencia de la implementación de las normas ISO 20000- 1 e ISO 27001 en la UPTC.

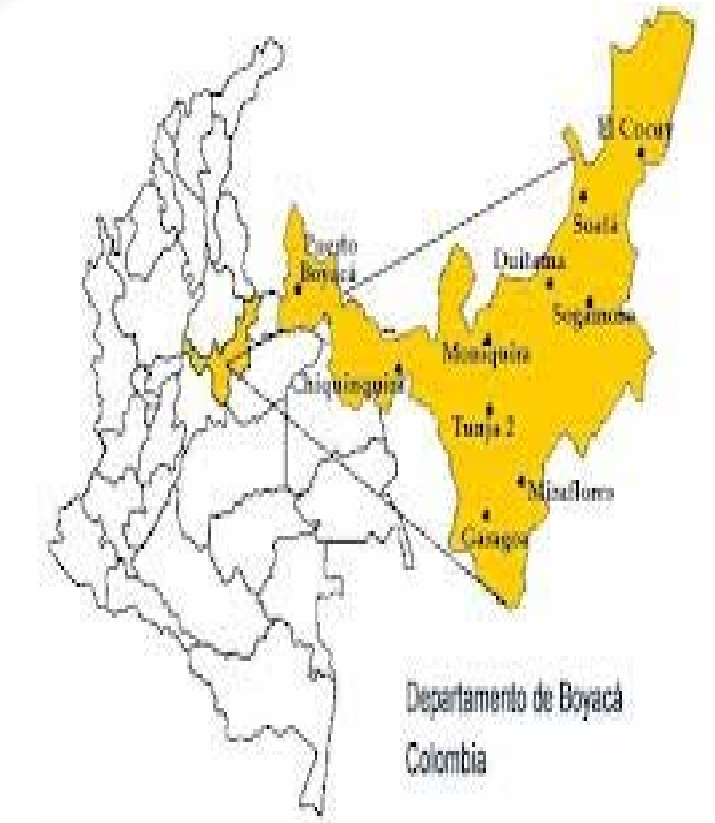
AGENDA

- INTRODUCCION
- CARACTERISTICAS DE UPTC
- CONCEPTOS
- GOBERNANZA Y MARCOS DE REFERENCIA
- AVANCES EN EL MODELO DE IMPLEMENTACION PROPUESTO

Características UPTC

Universidad Pedagógica Y Tecnológica de Colombia

ACREDITACIÓN INSTITUCIONAL DE ALTA CALIDAD
RESOLUCIÓN 6963 DE 2010 MEN



Uptc
Universidad Pedagógica y Tecnológica de Colombia

POR EL RESPETO, LA EXCELENCIA
Y EL COMPROMISO SOCIAL
UPETECISTA

UPTC - cifras

- Estudiantes : 28000
- Docentes: 1600
- Funcionarios: 1100
- Sedes en Tunja, Duitama, Sogamoso, Chiquinquirá.
- Bogotá, Paipa
- 25 CREADS en el país.

Grupo Organización y Sistemas.

Tiene definidas 4 áreas de trabajo que se identifican en 4 procedimientos:
Desarrollo y administración de los sistemas de Información,
Redes y Telecomunicaciones
Soporte a Usuarios en Hardware y Software.
Administración de aulas de Informática para préstamo a Docentes y estudiantes.

SEDE	INTERNET	DATOS	COMPUTADORES	CENTROS DE CABLEADO
Tunja	160 Mbps	50 Mbps	1900	23
Duitama	60 Mbps	8 Mbps	250	6
Sogamoso	60 Mbps	8 Mbps	250	7
Chiquinquira	25 Mbps	5 Mbps	100	3

AGENDA

- INTRODUCCION
- CARACTERISTICAS DE UPTC
- CONCEPTOS
- GOBERNANZA Y MARCOS DE REFERENCIA
- AVANCES EN EL MODELO DE IMPLEMENTACION PROPUESTO

CONCEPTOS

- **Gobierno de TI :** Es la responsabilidad de la dirección y de los ejecutivos. Es una parte integral de la Gobernabilidad corporativa que consiste en el liderazgo, las estructuras organizacionales y los procesos que aseguran que TI soporta y extiende las estrategias y los objetivos de la empresa. .
- Gobierno de TI se refiere a la alineación entre TI y las estrategias del negocio, las decisiones estratégicas de inversión en TI, y la creación de valor corporativo por el uso de TI en el negocio esta definición esta de acuerdo con lo establecido por Dameri and Privitera (2009)
- The IT Governance Institute. www.itgi.org.

CONCEPTOS

- **Gobernabilidad de TI de las empresas (GEIT)***:* de acuerdo con el IT Governance Institute estos son los conceptos de: Gobernanza y Gestión de la Información Empresarial y Tecnologías Relacionadas. Los términos " gobierno" , " gobernanza empresarial " y " GEIT " pueden tener diferentes significados para diferentes personas y empresas en función de (entre otros) el contexto de la organización , por ejemplo , la madurez , la industria y el entorno normativo , o el contexto individual, por ejemplo , papel del trabajo, la educación y la experiencia.

CONCEPTOS

- De acuerdo con COBIT 5, define la ***gobernabilidad*** como : Gobierno asegura que las necesidades de las partes interesadas , las condiciones y las opciones se evalúan para determinar de manera equilibrada y consensuada los objetivos de la empresa que deben lograrse; con el establecimiento de la dirección a través de definición de prioridades, la toma de decisiones, el seguimiento del desempeño y cumplimiento con la dirección y objetivos acordados.

CONCEPTOS

- ***GEIT, Gobernanza Empresarial de TI***, no es una disciplina aislada, sino una parte integral de la gobernanza empresarial. Mientras que la necesidad de una gobernanza a nivel empresarial es impulsada principalmente por la entrega de valor para los accionistas y la demanda de transparencia y una gestión eficaz de los riesgos de la empresa , las importantes oportunidades , costos y riesgos asociados con la TI requieren una dedicación, pero integrada , se centran en GEIT .
- GEIT permite a la empresa sacar el máximo provecho de las TI, maximizar los beneficios , capitalizando las oportunidades y ganando ventajas competitivas.

CONCEPTOS

- AREAS DE INCIDENCIA DE LA GOBERNABILIDAD.

Interacción de TI con el Negocio. Fuente Juan Guillermo Leruga CEO Grupo TEKNE. Argentina.

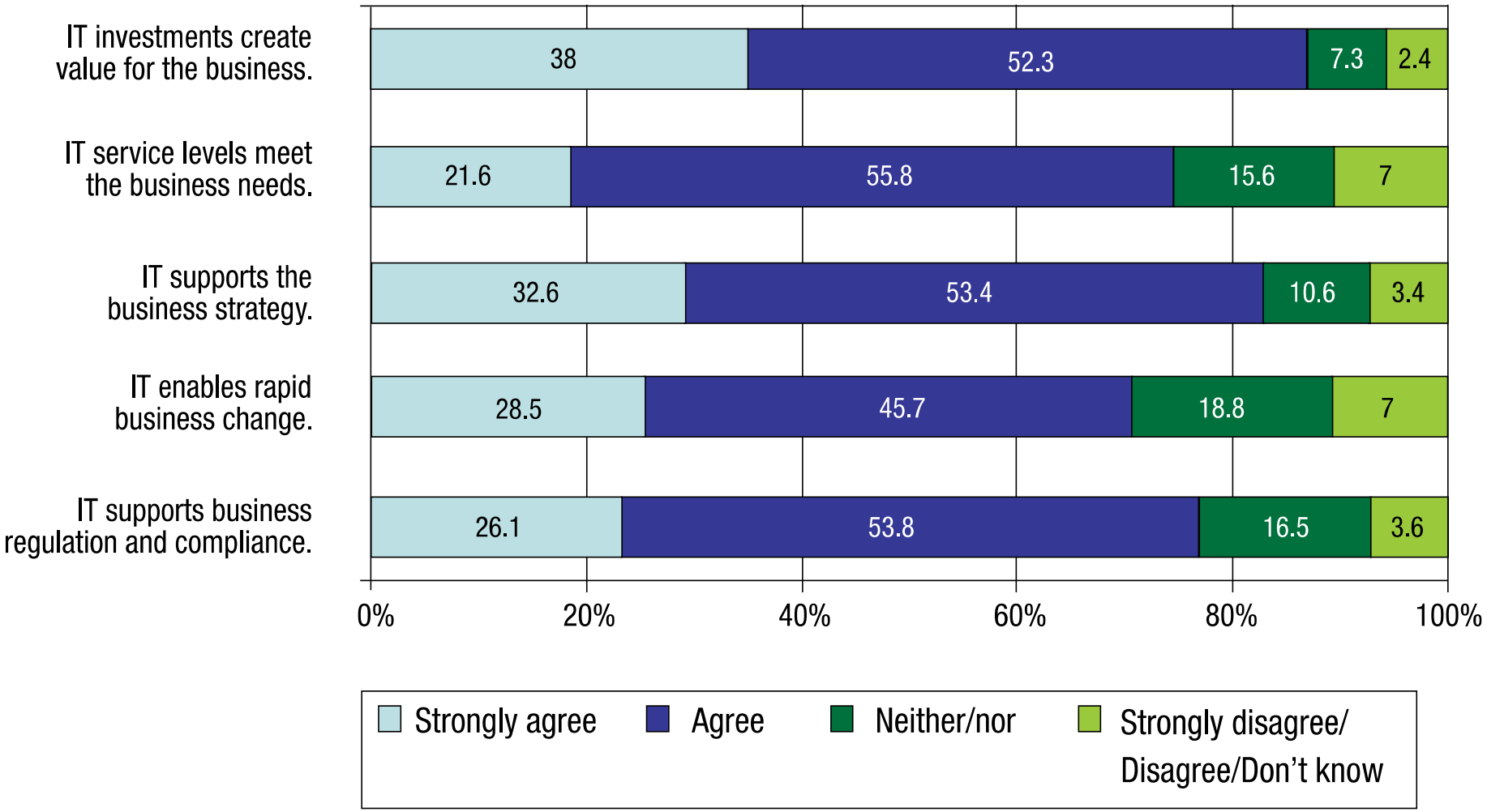
AGENDA

- INTRODUCCION
- CARACTERISTICAS DE UPTC
- CONCEPTOS
- GOBERNANZA Y MARCOS DE REFERENCIA
- AVANCES EN EL MODELO DE IMPLEMENTACION PROPUESTO

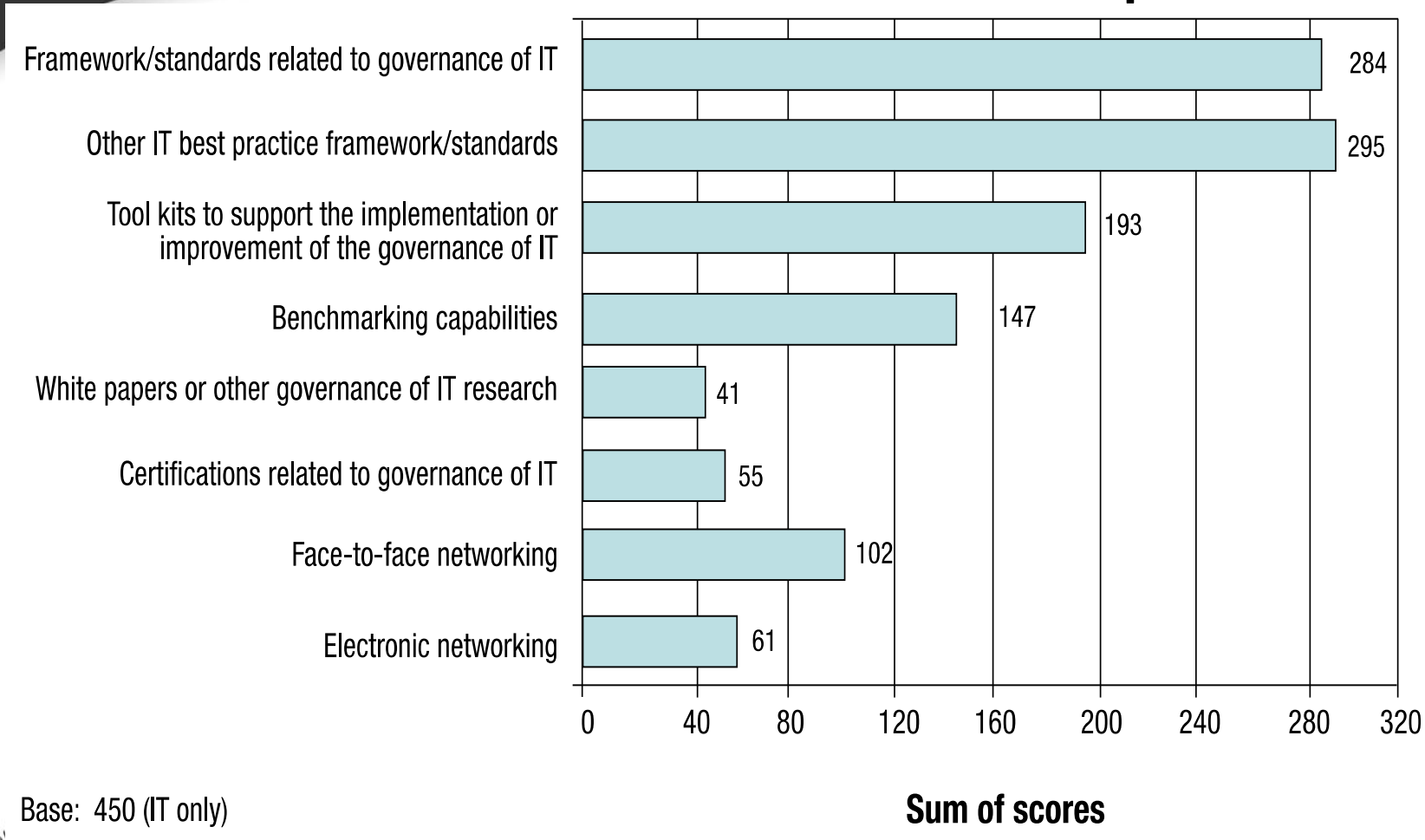
GOBERNANZA Y MARCOS DE REFERENCIA.

- En el año 2011 se adelanto por parte de Instituto para la Gobernanza de IT. Conocido como IT institute Governance, el survey acerca de la gobernanza empresarial de TI.
- Se presentan los resultados de algunas preguntas que permiten evidenciar el estado de la Gobernanza Empresarial del TI.
- Fuente: http://www.itgi.org

Contribución de TI al negocio:

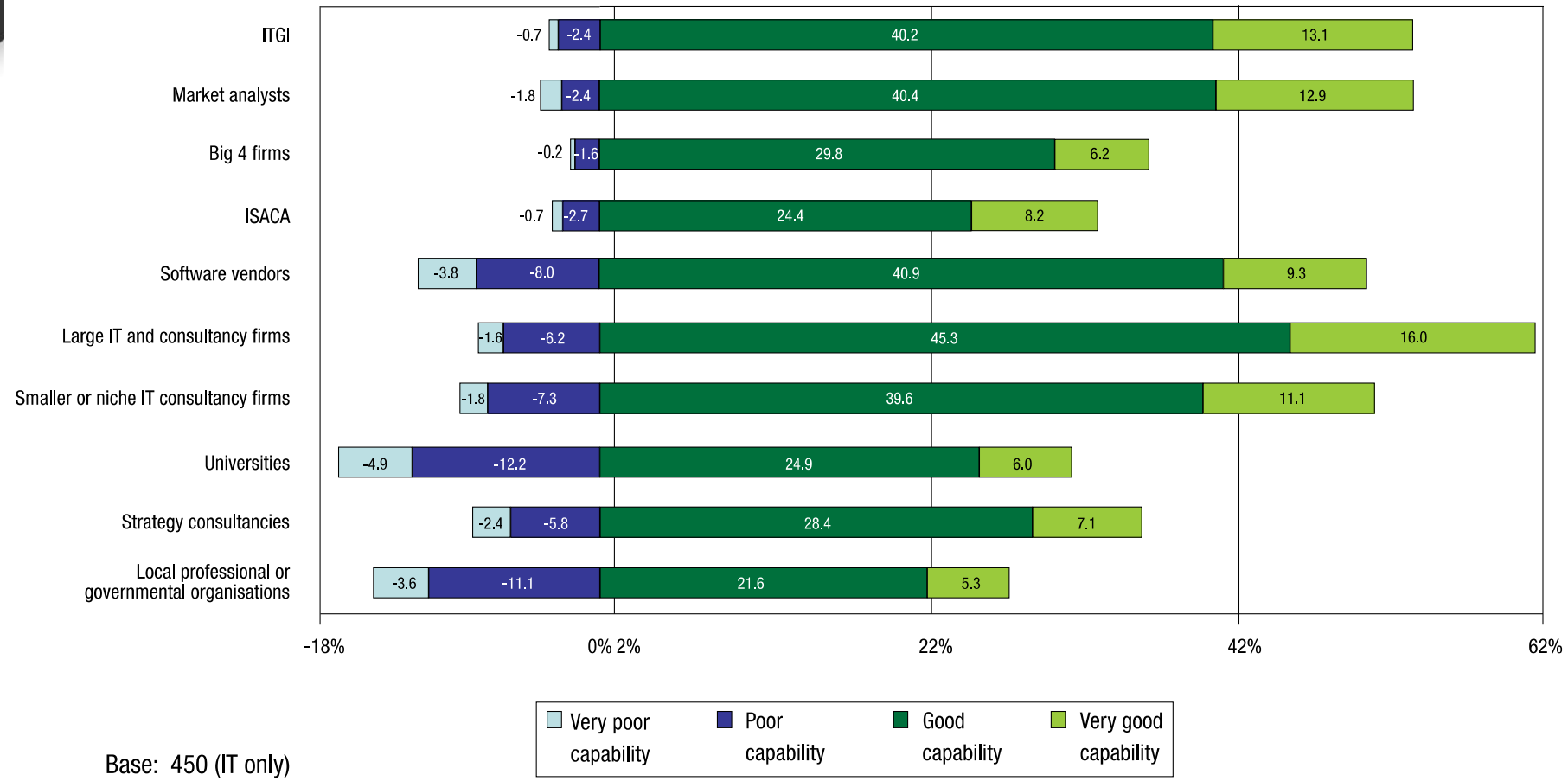


Madurez para la implementación de Modelos de Gobernanza Empresarial



Base: 450 (IT only)

Capacidad de las Organizaciones para Proveer o implementar modelos de Gobernanza Empresarial

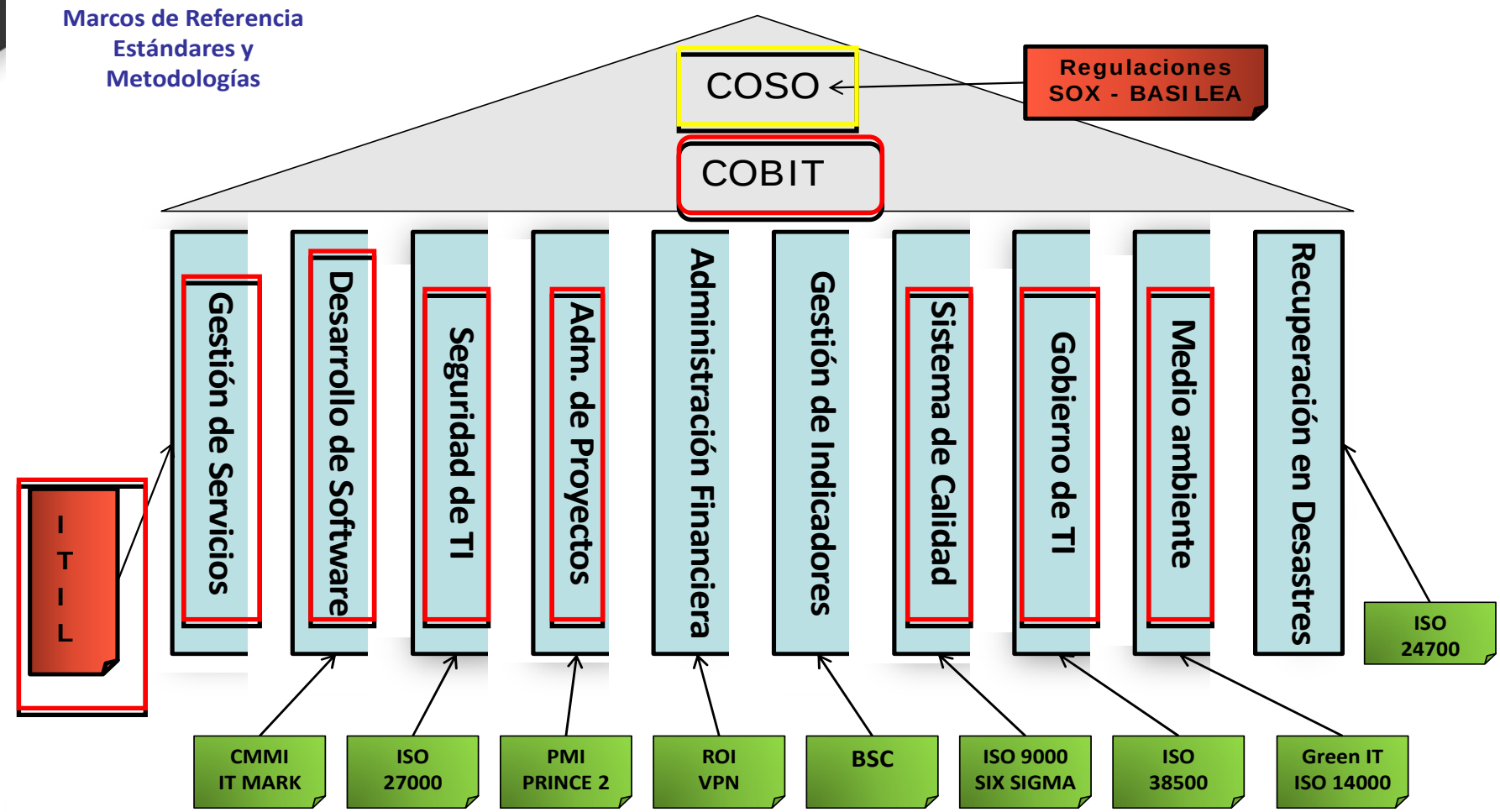


Base: 450 (IT only)

Uptc
Universidad Pedagógica y Tecnológica de Colombia

POR EL RESPETO, LA EXCELENCIA Y EL COMPROMISO SOCIAL
UPETECISTA

Modelo de Gobernabilidad y marcos de Referencia.



Modelo de Gobernabilidad. Fuente: Juan Guillermo Leruga CEO Grupo TekNe Argentina

COSO (*Committee of Sponsoring Organizations of the Treadway Commission*)

- Ha sido reconocido como un marco apropiado y exhaustivo para el control interno.
- C.O.S.O. es un comité (Comité de Organizaciones Patrocinadoras de la Comisión Treadway) que redactó un informe que orienta a las organizaciones y gobiernos sobre control interno, gestión del riesgo, fraudes, ética empresarial, entre otras. Dicho documento es conocido como “Informe C.O.S.O.” y ha establecido un modelo común de control interno con el cual las organizaciones pueden evaluar sus sistemas de control.

COBIT (Control Objectives for Information and Related Technology).

- Es un marco de referencia para el gobierno y la gestión de TI (34 objetivos de control). La versión 5 agrega una visión integral sobre Gobierno, negocio y gestión. La misión de COBIT es Investigar, desarrollar, publicar y promover un marco de referencia de gobierno y gestión de TI con autoridad, actualizado y aceptado internacionalmente para su adopción por empresas y utilizado por los directores de negocio, profesionales de TI y auditores de calidad.
- COBIT Soporta el gobierno de TI bajo cinco principios:
- • Satisfacer las necesidades de las partes interesadas.
- • Cubrir la organización de extremo a extremo.
- • Aplicar un marco de referencia único integrado.
- • Hacer posible un enfoque holístico, amplio e integrador.
- • Separar el Gobierno de la Gestión.

ITIL, (Information Technology Infrastructure Library)

- En la Gestión de servicios se utiliza un marco de referencia como ITIL, es un conjunto de buenas prácticas destinadas a facilitar la gestión del ciclo de vida de servicios de tecnologías de la información (TI). ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. ITIL da soporte a más del 50% de los objetivos de Control de COBIT.

ISO 20000

- ISO/IEC 20000 La serie fue normalizada y publicada por las organizaciones ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), es el estándar reconocido internacionalmente para la certificación de calidad en la gestión de servicios de TI (Tecnologías de la Información). La versión vigente es del año 2011 y amplia la cobertura a cualquier servicio.

ISO 9000

- Es un conjunto de normas sobre calidad y gestión continua de la calidad, establecidas por la Organización Internacional para la Estandarización . Se puede aplicar a cualquier tipo de organización o actividad orientada a la producción de bienes o servicios. La ISO 9000 especifica la manera de implementar un Sistema de Gestión de Calidad.

CMMI

- (Capability Maturity Model Integration)
- Es un modelo para la mejora y evaluación de procesos para el desarrollo, mantenimiento y operación de sistemas de software. Está compuesto por CMMI-DEV o CMMI for Development, CMMI-ACQ o CMMI for Acquisition y CMMI-SVC o CMMI for Services.

ISO 27001

- Esta norma proporciona los requisitos del sistema de gestión de seguridad de la información. para garantizar que las organizaciones preservan la confidencialidad, disponibilidad e Integridad de la Información, Es la norma con la cual se certifican por auditores externos los Sistemas de Gestión de la Seguridad de la Información de las organizaciones.

PMI

- (Project Management Institute), Este conjunto de mejores prácticas proporciona las herramientas que permiten gestionar en forma eficiente todo tipo de proyectos. Tiene su origen en USA y actualmente tiene representación en 180 países con más de 400.000 profesionales certificados. La irrupción de la ISO 21.500 ha dado a la gestión de proyectos una norma que le permita certificar la gestión de proyectos.
- PRINCE2 es otro estándar de PM reconocido mundialmente.

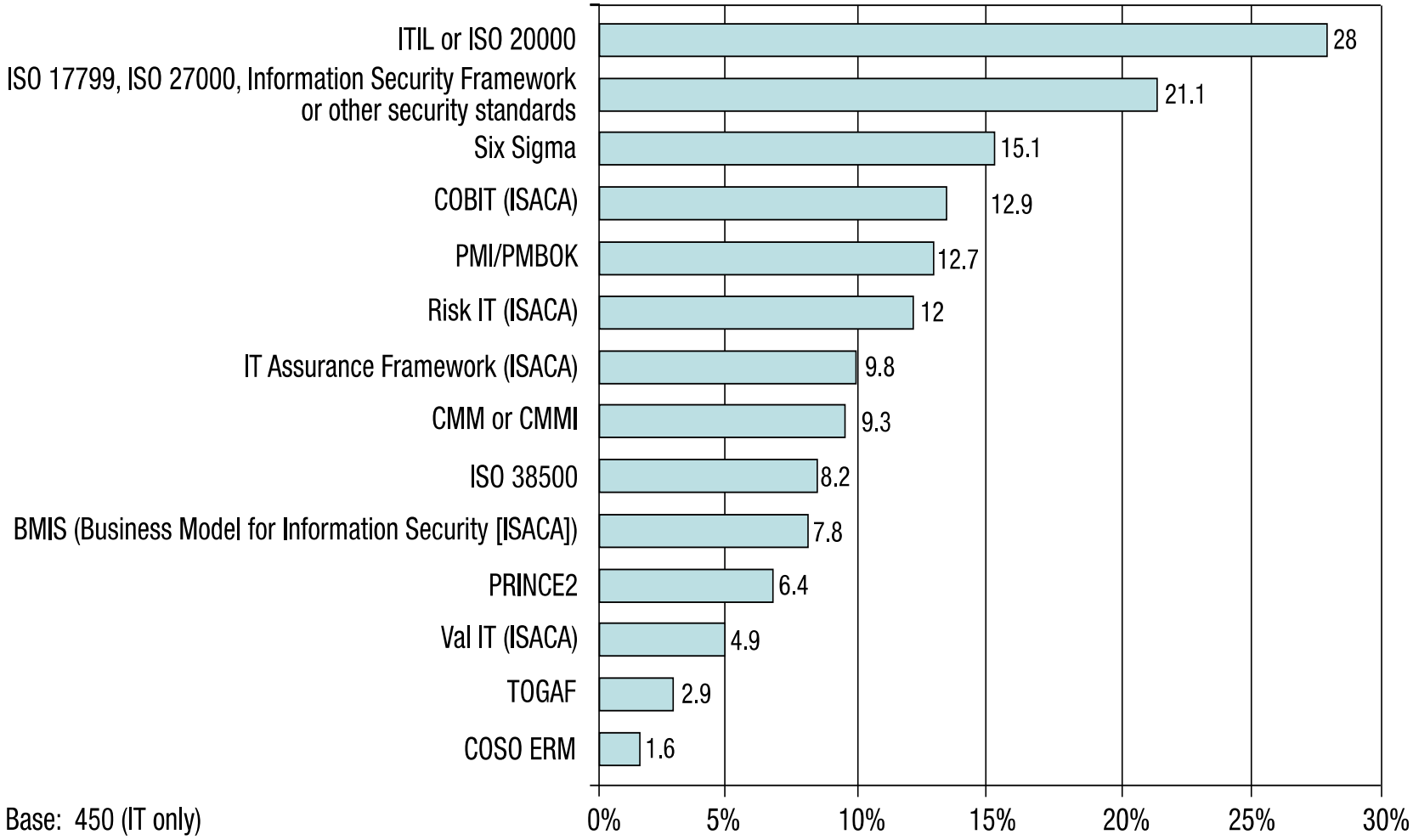
ISO 14000 – GREEN IT

- Es una norma especialmente diseñada para regular el "Sistema de Administración del Medio Ambiente (Environment Management System)". Sirve para controlar y minimizar los efectos dañinos que son causados en el medio ambiente por las diferentes actividades que desarrollan las organizaciones.
- Certifica a las organizaciones en el cumplimiento del manejo y buen uso de los recursos ambientales y la preparación para preservarlos.
- Green IT o traducido al español como Tecnologías Verdes se refiere al uso eficiente de los recursos computacionales minimizando el impacto ambiental, maximizando su viabilidad económica y asegurando deberes sociales

ISO 38500

- Esta nueva norma fija los estándares para un buen gobierno de los procesos y decisiones empresariales relacionados con los servicios de información y comunicación que, suelen estar gestionados tanto por especialistas en TIC internos o ubicados en otras unidades de negocio de la organización, como por proveedores de servicios externos.
- En esencia, todo lo que esta norma propone puede resumirse en tres propósitos fundamentales:
  - Asegurar que, si la norma es seguida de manera adecuada, las partes implicadas (directivos, consultores, ingenieros, proveedores de hardware, auditores, etc.), puedan confiar en el gobierno corporativo de TIC.
  - Informar y orientar a los directores que controlan el uso de las TIC en su organización.
  - Proporcionar una base para la evaluación objetiva por parte de la alta dirección en el gobierno de las TIC.

Frameworks mas implementados.



Base: 450 (IT only)

AGENDA

- INTRODUCCION
- CARACTERISTICAS DE UPTC
- CONCEPTOS
- GOBERNANZA Y MARCOS DE REFERENCIA
- AVANCES EN EL MODELO DE IMPLEMENTACION PROPUESTO

AVANCES EN EL MODELO DE IMPLEMENTACION PROPUESTO.

SISTEMA INTEGRADO DE GESTION SIG

El Sistema Integrado de Gestión SIG de la UPTC integra las normas:

NTC GP 1000:2009: Norma Técnica de Calidad en la Gestión Publica.

NTC-ISO 9001:2008: Norma Internacional para los Sistemas de Gestión de Calidad.

MECI 1000:2005: Modelo Estándar de Control Interno.

GTC 180: Responsabilidad Social.

SISTEDA: Sistema de Desarrollo Administrativo.

NTC OHSAS 18001:2007: Sistemas de Gestión en Seguridad y Salud Ocupacional.

NTC ISO 14001:2004: Sistemas de Gestión Ambiental.

NTC-ISO/IEC 17025:2005: Requisitos Generales para la Competencia de los laboratorios de ensayo y calibración.

ISO 27001:2005: Sistema de Gestión de Seguridad de la Información SGSI.

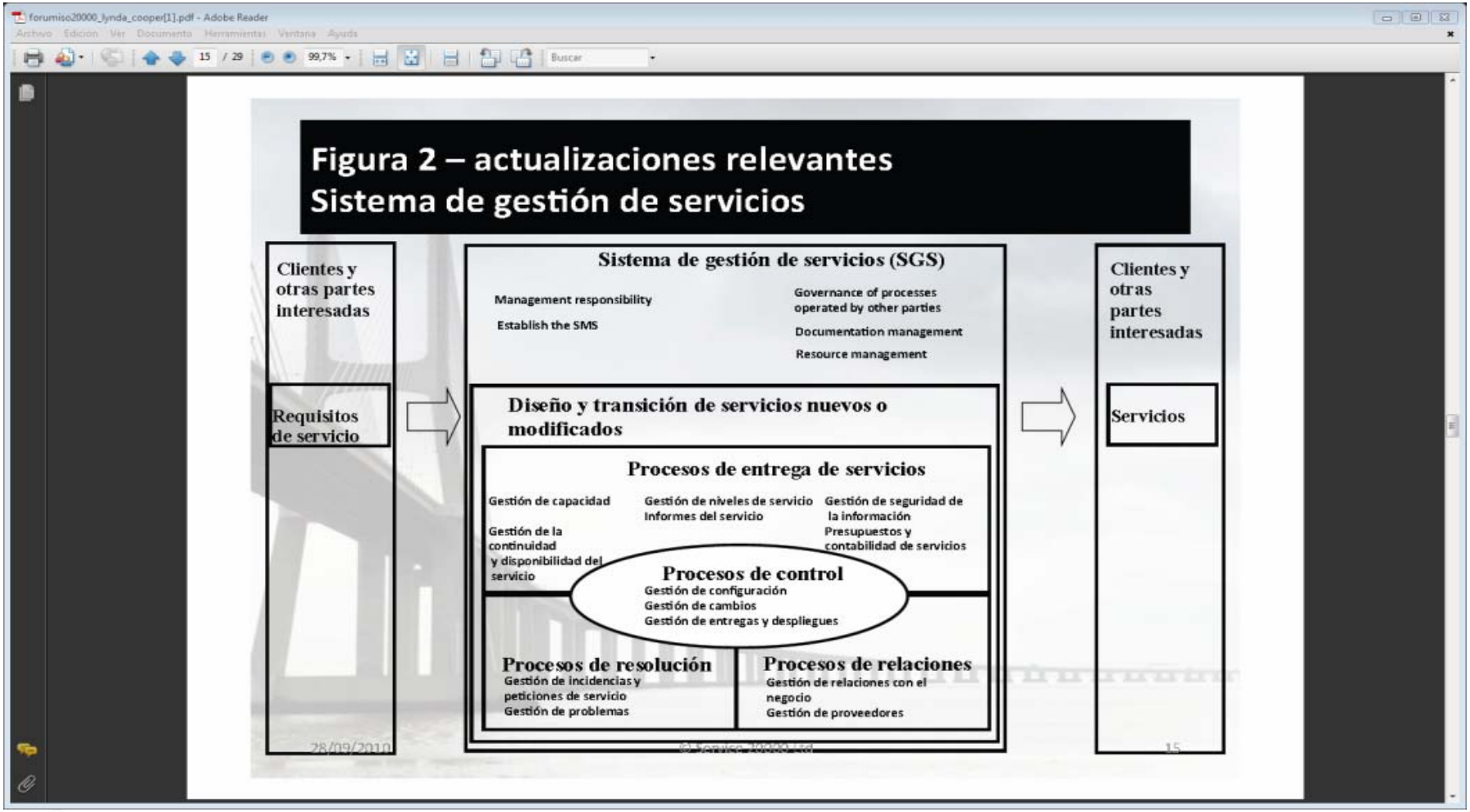
ISO 20000:2008: Sistema de Gestión de Servicios de Tecnología e Información SGSTI.

Proceso Gestión de Recursos Informáticos.

- 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"*
- *Contiene 4 procedimientos.*

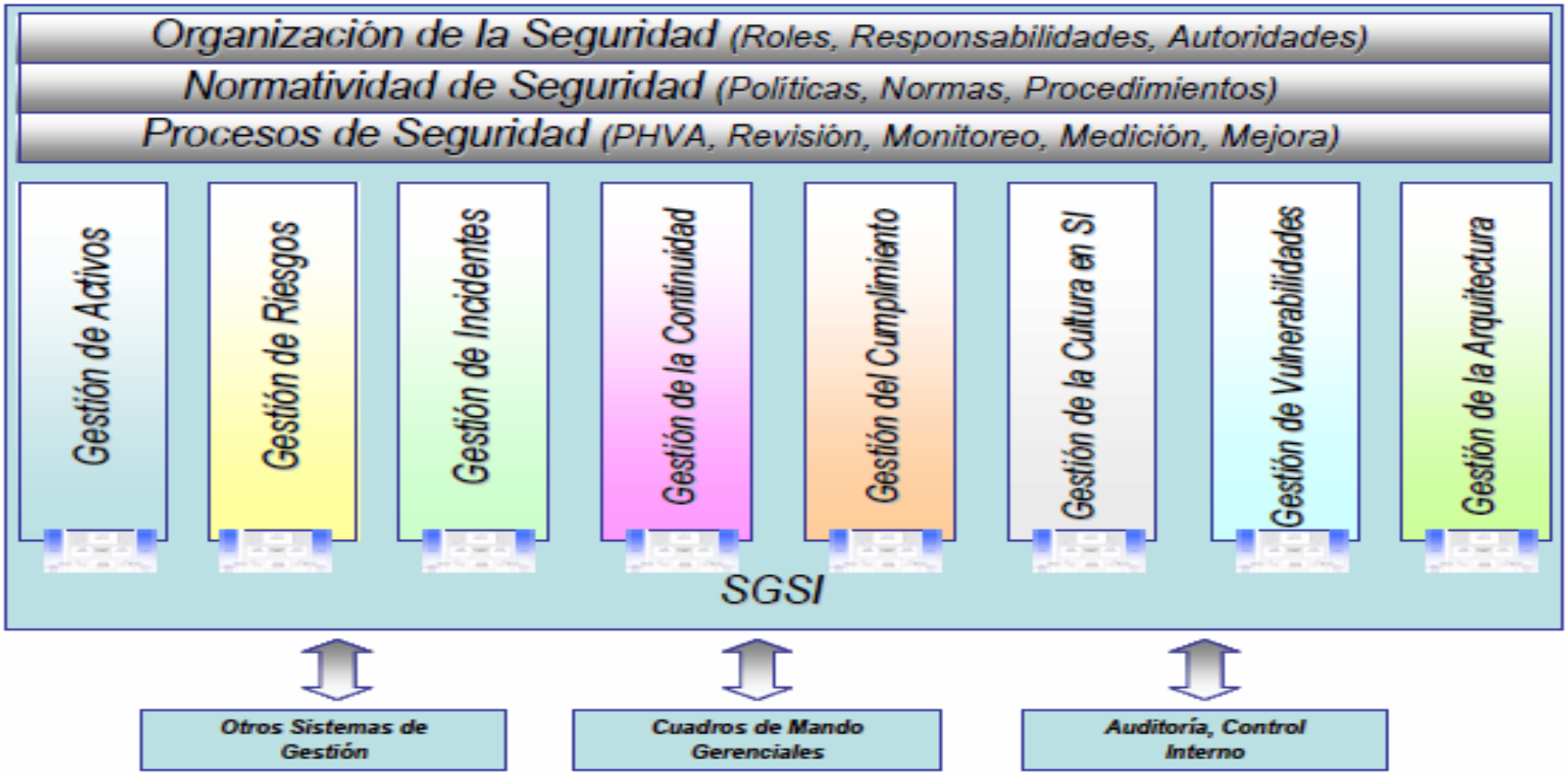
1. *Procedimiento para la Incorporación de los Sistemas de Información.*
2. *Soporte y Administración de Recursos Informáticos.*
3. *Seguridad de la Información*
4. *Administración de Aulas de Informática.*

Procesos de ISO 20000



ISO 27001

- Componentes de un modelo de ISO 27001



MODELO PROPUESTO

Fase 0
- **Diagnóstico Inicial. Revisión del Sistema. Identificación de Procesos Comunes**

Fase 1
- Verificar procesos comunes exigidos por las normas, Control de Documentos, Control de Registros, Auditorias Internas, revisión por la Dirección

Fase 2
- .ISO 27001: Gestión de Activos y Gestión de Riesgos.
- ISO 20000: Gestión de la Configuración, Gestión de Incidentes, Gestión de Problemas.

Fase 3
- ISO 27001: Gestión de la Cultura y Gestión de Cumplimiento.
- ISO 20000: Gestión de Cambios, Gestión de la Capacidad, Gestión de nivel del servicio, Presentación de Informes.

Fase 4
- ISO 27001: Gestión de la Arquitectura, Gestión de la continuidad y Gestión de Vulnerabilidad..
- ISO 20000: Gestión de versiones y entrega, 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.

DOCUMENTOS Y PROCEDIMIENTOS IMPLEMENTADOS

A-RI-M02	MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION
A-RI-L02	PLAN DE GESTION DEL SERVICIO
A-RI-P01	PROCEDIMIENTO PARA LA INCORPORACION DE SISTEMAS DE INFORMACION
A-RI-P02	SOPORTE Y ADMINISTRACION DE RECURSOS INFORMATICOS
A-RI-P03	COPIAS DE SEGURIDAD DE LA INFORMACION
A-RI-P04	ADMINISTRACION AULAS DE INFORMATICA
A-RI-P05	PROCEDIMIENTO GESTION DE LA DISPONIBILIDAD
A-RI-P06	PROCEDIMIENTO GESTION DE LA CONFIGURACION
A-RI-P07	PROCEDIMIENTO PARA LA GESTION DE INCIDENTES
A-RI-P08	PROCEDIMIENTO PARA LA GESTION DE PROBLEMAS
A-RI-P09	PROCEDIMIENTO INVENTARIO Y CLASIFICACION DE ACTIVOS DE INFORMACION
A-RI-P10	PROCEDIMIENTO PARA LA GESTION DE CAMBIOS Y ENTREGAS

DOCUMENTOS Y PROCEDIMIENTOS IMPLEMENTADOS

A-RI-P10	PROCEDIMIENTO PARA LA GESTION DE CAMBIOS Y ENTREGAS
A-RI-P11	PROCEDIMIENTO GESTION DEL RIESGO DE SEGURIDAD DE LA INFORMACION
A-RI-P12	PROCEDIMIENTO GESTION DE LA CAPACIDAD
A-RI-P13	PROCEDIMIENTO GESTION DE NIVEL DEL SERVICIO
A-RI-P14	GESTION DE SERVICIOS NUEVOS Y MODIFICADOS
A-RI-P15	GESTION DE INFORMES
A-RI-P16	GESTION DE LA CONTINUIDAD
A-RI-P17	GESTION DE SEGURIDAD DE LA INFORMACION
A-RI-P18	MEJORA CONTINUA SGS

CATALOGO DE SERVICIOS

- Además de implementar procedimientos, para el cumplimiento de ISO 20000 se estableció el catalogo de servicios del área los cuales son y de cada uno se suscribió ANS:
- Desarrollo de aplicaciones.
- Asistencia Técnica.
- Aulas de Informática.
- Infraestructura de Red y comunicaciones.
- Gestión de la seguridad informática.

POLITICAS

- Mejora Continua.
- Capacidad
- Configuración
- Disponibilidad
- Continuidad
- Entrega
- Ley de Protección de Datos Personales
- Terceros
- Propiedad de la Información
- Clasificación de activos de Información
- Uso de Recursos informáticos
- Relacionadas con el personal: Ingreso, confidencialidad, aceptación, desvinculación.
- Relacionadas con la seguridad Fisica: Condiciones eléctricas y ambientales, control de acceso a áreas de TI, control de acceso a instalaciones de la Universidad.
- Asignación de responsabilidades operativas.
- Control de cambios
- Protección software malicioso
- Almacenamiento y respaldo
- Uso de comunicaciones
- Acceso a Internet
- Uso de periféricos
- Auditorías a la plataforma tecnológica
- Cuentas de usuario
- Contraseñas.
- Acceso a sistemas operativos
- Redes de datos y sistemas de información.
- Cifrado de información.
- Desarrollo y soporte
- Administración de vulnerabilidades
- Contingencia
- Propiedad intelectual
- Privacidad de la Información
- Pirateria.

INDICADORES

- Satisfacción del Usuario
- Porcentaje de Disponibilidad
- Implementación de Mejoras
- Comunicación de Mejoras de los servicios
- Cumplimiento de los servicios
- Tratamiento de incidentes de seguridad de la información
- Efectividad del Plan de Riesgos
- Atención de incidentes.
- Formación del personal de TI

PARA FINALIZAR

- Aún es prematuro concluir todo el impacto del sistema, sin embargo para responder a la pregunta de si se logra evolucionar a un modelo de gobernanza, A partir del trabajo realizado y teniendo en cuenta la tendencia hacia las áreas de TI, se presentan algunas reflexiones, para lograrlo y algunas ideas de Leruga:
- Cuente con el apoyo de la Alta Dirección.
- Sin duda el avance hasta el momento, permite pensar en que se puede llegar a un modelo de gobernanza, y para ello se debería realizar una evaluación de madurez cuyo resultado nos brinde el GAP entre lo deseado y el estado actual

- Elaborar un proyecto de mejora en base a los objetivos organizacionales
- Definición de etapas y entregables por periodos
- Selección de las herramientas adecuadas
- Comenzar la Implantación
- Seguimiento y control

- El Gobierno de TI es parte de la Gobernabilidad Corporativa.
- La alineación de TI con los objetivos de Negocio es una herramienta fundamental para el logro de los mismos.
- El abanico de estándares existentes nos permiten mediante su implementación y combinación adecuada alcanzar los objetivos de mejora y el gobierno de la información.

- Las herramientas adecuadas son parte importante del proyecto de mejora
- La solución comprobada es la adopción de estándares en el marco de un proceso evolutivo de mejora de la calidad y la gobernabilidad.
- Más del 90% de las empresas encuestadas ITGI tiene en sus planes mejorar la gobernabilidad de TI.

GRACIAS