SUPERINTENDENCIA GENERAL DE ENTIDADES FINANCIERAS

Certificada con ISO-9001/2000

Basilea II y Gobierno de TI

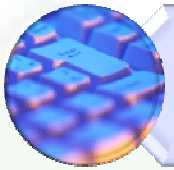
19 de agosto del 2009

Osvaldo Sánchez

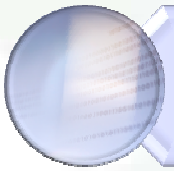
Contenido

Introducción

Basilea II y el Riesgo Operativo



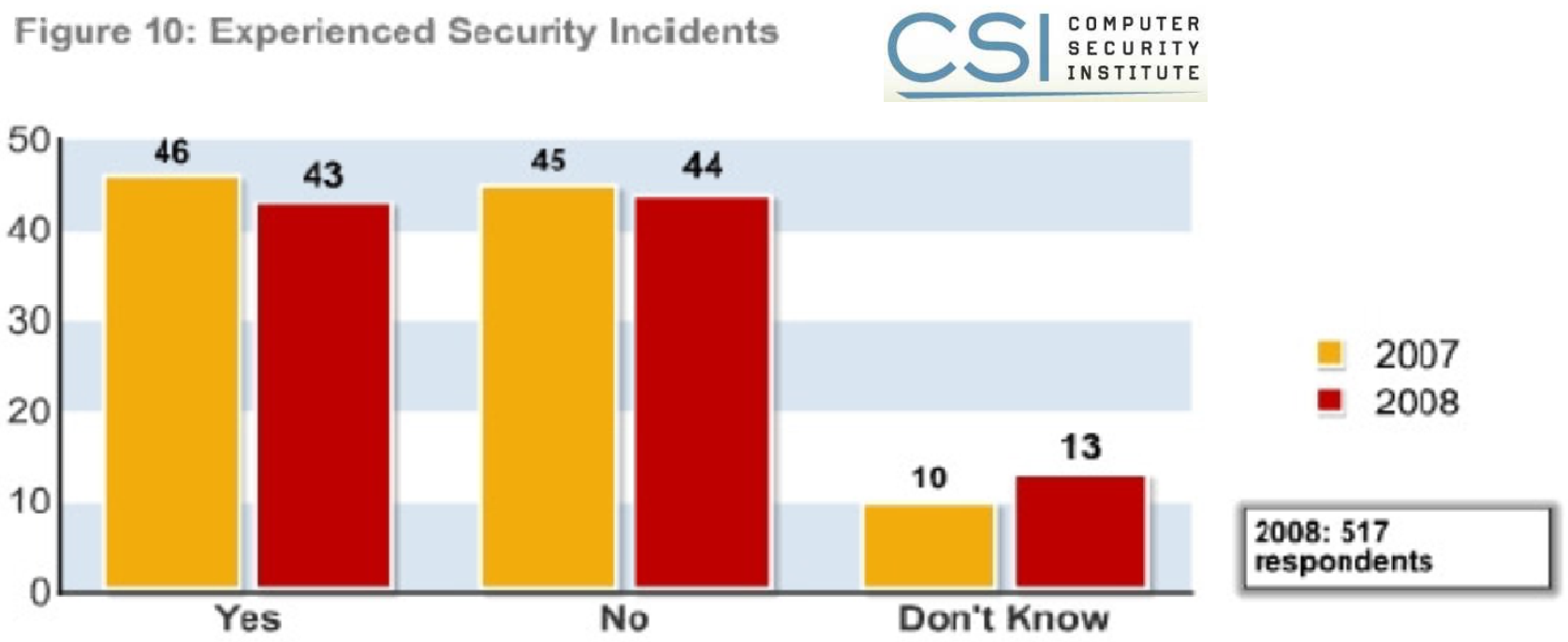
COBIT



Combinando Basilea II con COBIT

Normativa 14-09

Algunas estadísticas (USA)



2008
CSI Computer Crime & Security Survey

Tipos de incidentes en los últimos 12 meses

Tipo de ataque	%	Monto de la pérdida $
Abuso de la red interna	59	2,889,700
Virus	52	8,391,800
Robo de dispositivos móviles (PC)	50	3,881,150
Ataque de Phising	26	2,752,000
Uso indebido de MSM	25	200,700
Negación de servicio	25	2,888,600
Acceso no autorizado a la información	25	1,042,700
Robo de información de clientes o empleados	17	5,685,000
Abuso de las redes inalambricas	17	542,850
Sistema vulnerados	13	6,875,000
Fraude financiero	12	21,124,750
Obtención de claves de acceso	10	1,042,700
Desconfiguración del Web site	10	725,300
Robo de la propiedad intelectual - información	5	2,345,000
Sabotaje	4	1,056,000

CSI COMPUTER SECURITY INSTITUTE 2007

Algunas estadísticas (USA)

The most expensive computer security incidents were those involving financial fraud…

…with an average reported cost of close to $500,000 (for those who experienced financial fraud). The second-most expensive, on average, was dealing with "bot" computers within the organization's network, reported to cost an average of nearly $350,000 per respondent. The overall average annual loss reported was just under $300,000.

CSI COMPUTER SECURITY INSTITUTE

2008
CSI Computer Crime & Security Survey

Algunos incidentes (CR)

LA REPUBLICA.NET
EL DIARIO DE NEGOCIOS

Viernes 7 de Agosto, 2009

Clientes han denunciado 150 estafas que se han realizado a través de las páginas de Internet de las instituciones locales

Bancos intentan blindarse contra fraude electrónico

> Los delitos han sido cometidos por un mal uso o descuido de la información por parte de los clientes, argumentan entidades financieras
> Nuevos dispositivos de seguridad son incorporados en el país para aumentar la confiabilidad de las transacciones electrónicas realizadas a través de los sitios web

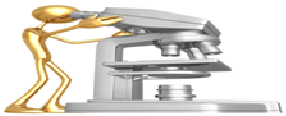
Preocupaciones del regulador

El uso creciente de tecnologías de información

Una mayor importancia de la integración de tecnologías informáticas y servicios compartidos entre entidades

El crecimiento del comercio electrónico

Las adquisiciones, fusiones y consolidaciones



La complejidad creciente de productos y servicios

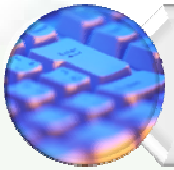
La creciente utilización de acuerdos de "*outsourcing*"

La mayor participación en los sistemas de compensación y liquidación

Contenido

Introducción

Basilea II y el Riesgo Operativo



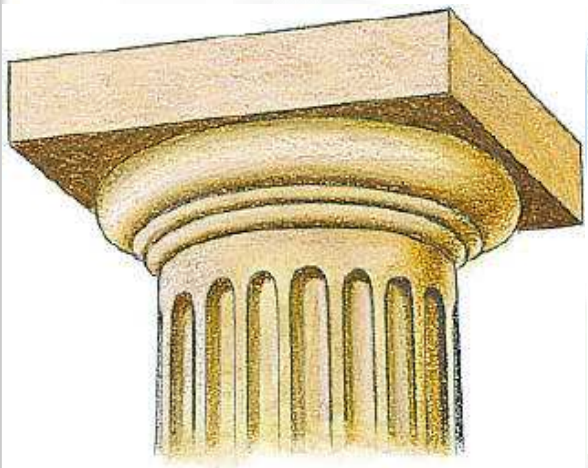
COBIT

Combinando Basilea II con COBIT

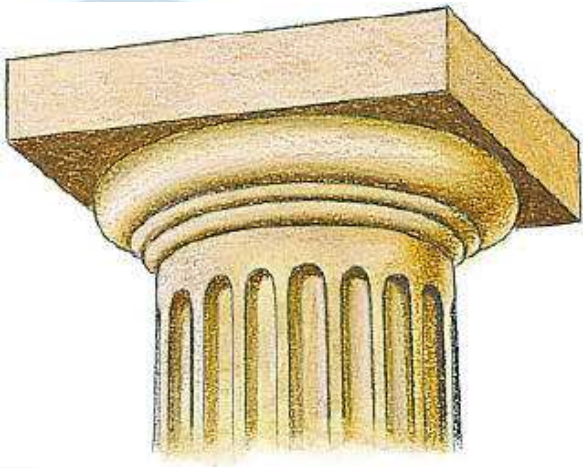
Normativa 14-09

Pilares Basilea II

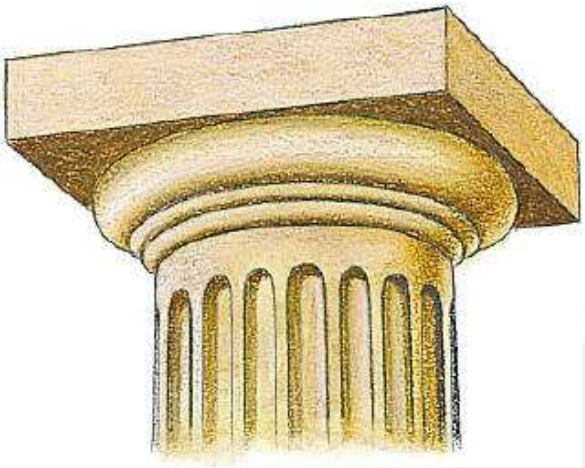
Primer Pilar: Requisitos de Capital Mínimo



Segundo Pilar: Revisión del Supervisor

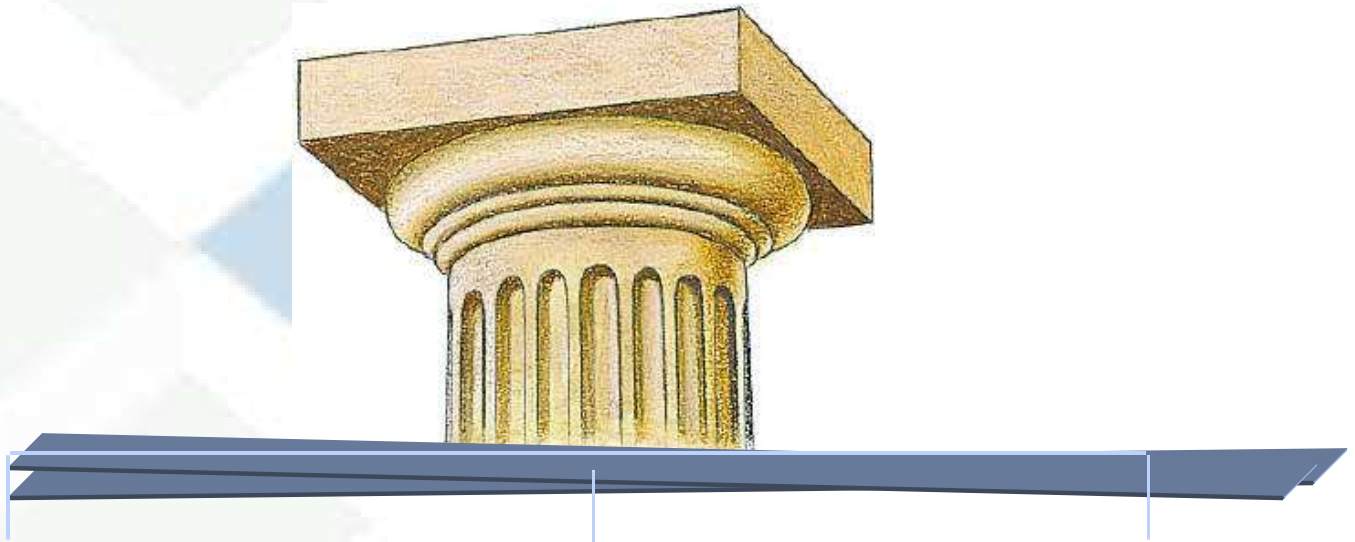


Tercer Pilar: Disciplina de Mercado



Pilares Basilea II

Primer Pilar: Requisitos de Capital Mínimo



- Riesgo de mercado
- Riesgo crediticio
- Riesgo operacional

Riesgo operativo

"Riesgo de pérdida debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos"

Implica una Administración del Riesgo Operativo a nivel Institucional

Principales Eventos

Los principales *eventos de RO que ha identificado el BCBS, en conjunto con la banca, como posibles causantes de pérdidas sustanciales son:*

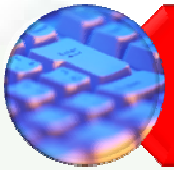
- Fraude interno
- Fraude externo
- Relaciones laborales y seguridad en el puesto de trabajo
- Prácticas con los clientes, productos y negocios
- Daños a activos materiales
- Alteraciones en la actividad y fallos en los sistemas
- Ejecución, entrega y procesamiento

BCBS Comité de Supervisión Bancaria de Basilea

Contenido

Introducción

Basilea II y el Riesgo Operativo



COBIT

Combinando Basilea II con COBIT

Normativa 14-09

Incluye 41 referencias de estándares

COSO
OCDE
DTI
ISO 9000-3
NIST SP 800-12
ITIL
IBAG
NSW
DCB
EDPAF/Monográfico 7
PCIE
JISAS
EDPAF/Objetivos de Control

CISA
IFAC
NIST SP 500-153
GAO/GAS
SPICE
ISAA (Dinamarca)
DRI International
IIA/SAC
IIA/PPP 97-1
E&Y/TRS
C&L/Audit Guide SAP R/3
ISO IEC JTC1-SC27
ISO IEC JTC1-SC7

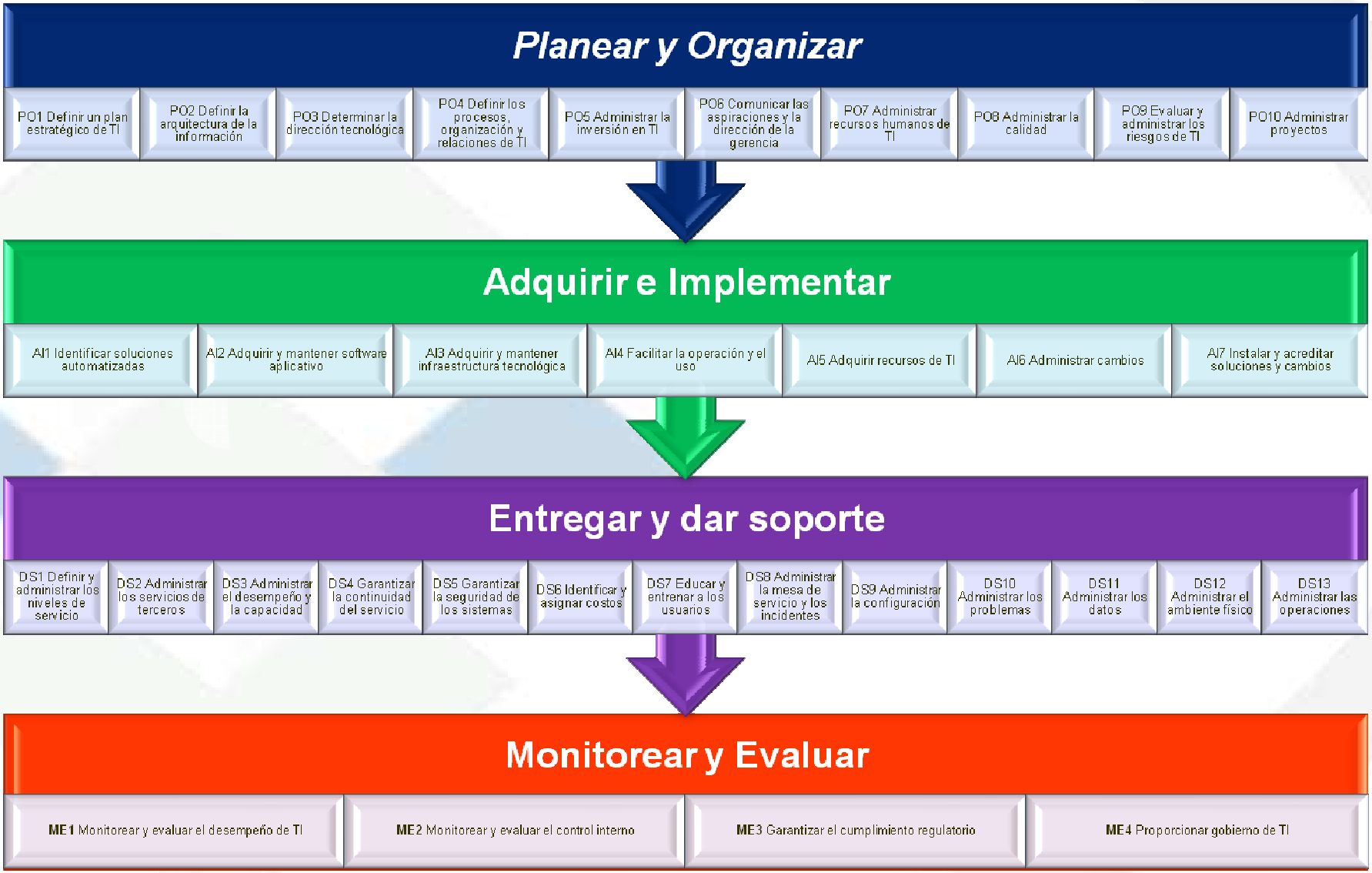
ISO TC68-SC2-WG4
Criterios Comunes
EDIFACT
TickIT
ESF/Comunicaciones
ESF/Microordenadores
EDPAF/CISAM
GAO/AIMD-00-21.3.1
NIST SP 800-18
GAO/FISCAM
BS7799
CICA
ISO IEC 13335-n (1..5)
SysTrust™

Qué es COBIT

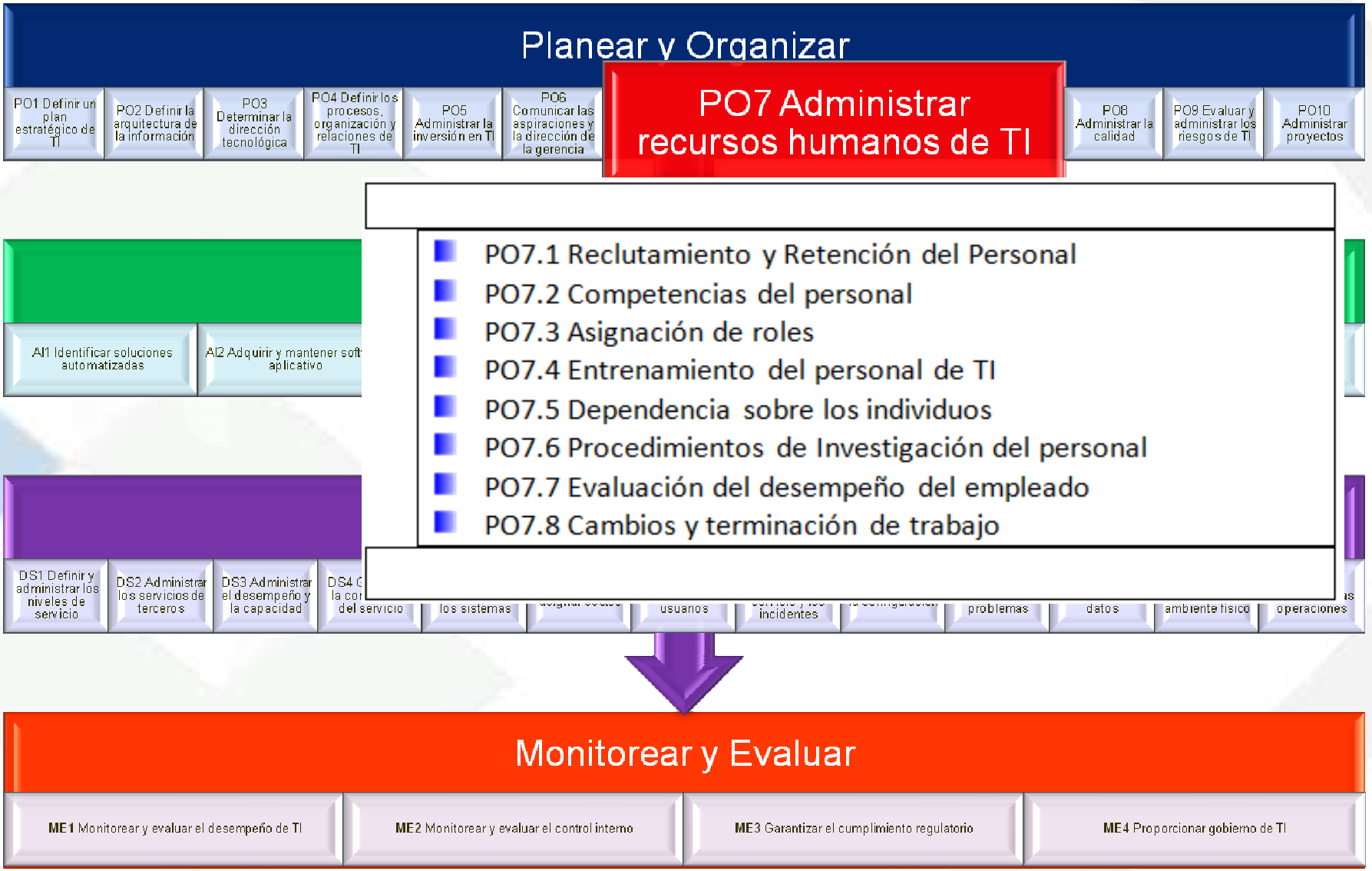
Un conjunto de mejores prácticas para la implementación de un Gobierno de TI, abarcando todos los procesos que podría tener el área de TI, agrupándolas en 4 grandes bloques (dominios)

- ***Planear y organizar***
- ***Adquirir e implementar***
- ***Entregar y dar soporte***
- ***Monitorear y evaluar***

Procesos de los dominios



Procesos de los Dominios



Modelo de madurez

Va del nivel 0 (no existente) hasta el nivel 5 (optimizado)

Se deriva del modelo del Software Engineering Institute

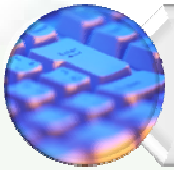
Busca

- El desempeño real de la empresa—Dónde se encuentra la empresa hoy
- El estatus actual de la industria—La comparación
- El objetivo de mejora de la empresa—Dónde desea estar la empresa
- El crecimiento requerido entre “como es” y “como será”

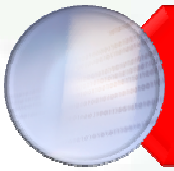
Contenido

Introducción

Basilea II y el Riesgo Operativo



COBIT



Combinando Basilea II con COBIT

Normativa 14-09

"Sound Practices for the Management and Supervision of Operational Risk", Feb 2003 - BCBS

Normativa de TI SUGEF

Principales Eventos

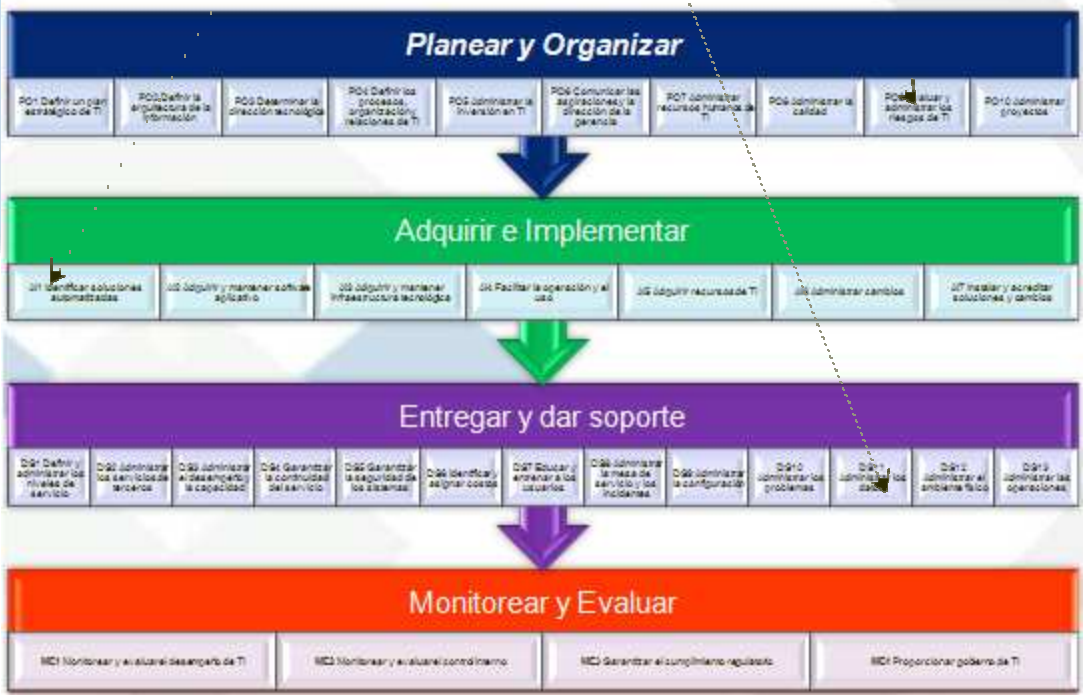
Los principales *eventos de RO que ha identificado el BCBS, en conjunto con la banca, como posibles causantes de pérdidas sustanciales son:*

- Fraude interno
- Fraude externo
- Relaciones laborales y seguridad en el puesto de trabajo
- Prácticas con los clientes, productos y negocios
- Daños a activos materiales
- Alteraciones en la actividad y fallos en los sistemas
- Ejecución, entrega y procesamiento

BCBS Comité de Supervisión Bancaria de Basilea

Cómo ligar Basilea II con COBIT

Procesos de los Dominios



Fraude Interno

Errores intencionados en la información sobre posiciones	Robos por parte de empleados	Utilización de información confidencial en beneficio de la cuenta del empleado

Fraude Interno

Errores intencionados en la información sobre posiciones	Robos por parte de empleados	Utilización de información confidencial en beneficio de la cuenta del empleado

- Manipulación deliberada de programas (código)
- Uso no autorizado de las funciones de modificaciones
- Manipulación deliberada del hardware
- Cambios mal intencionados a las aplicaciones con técnicas de hackeo
- Copia de Software o licencias no autorizadas
- Evadir los privilegios de acceso

→ PO6 Comunicar las aspiraciones y la dirección de la gerencia

→ DS5 Garantizar la Seguridad de los sistemas

→ DS9 Administrar la configuración

Fraude Externo

Atraco	Falsificación	Circulación de cheques en descubierto	Daños por intrusión en los sistemas informáticos

Fraude Externo

Atraco	Falsificación	Circulación de cheques en descubierto	Daños por intrusión en los sistemas informáticos

- Cambios mal intencionados a las aplicaciones con técnicas de hackeo
- Obtención de documentos confidenciales
- Eludiendo los controles de acceso
- Intercepción de la comunicación
- Claves comprometidas
- Virus

→ DS5 Garantizar la Seguridad de los sistemas

Relaciones laborales y seguridad en el puesto de trabajo

Solicitud de indemnizaciones por parte de los empleados	Infracción de las normas laborales de seguridad e higiene	Organización de actividades laborales	Acusaciones de discriminación	Responsabilidades generales

Relaciones labores y seguridad en el puesto de trabajo

- Uso indebido de los recursos de TI
- Falta de respuestas adecuadas ante incidentes de seguridad

→ PO6 Comunicar las aspiraciones y la dirección de la gerencia