Seguridad de la Información Tendencias, Estándares y Apoyo Forense

Yuri Marroquin

Plus Technologies & Innovations, Inc.

ymarroquin@plus-ti.com

Seguridad de la Información

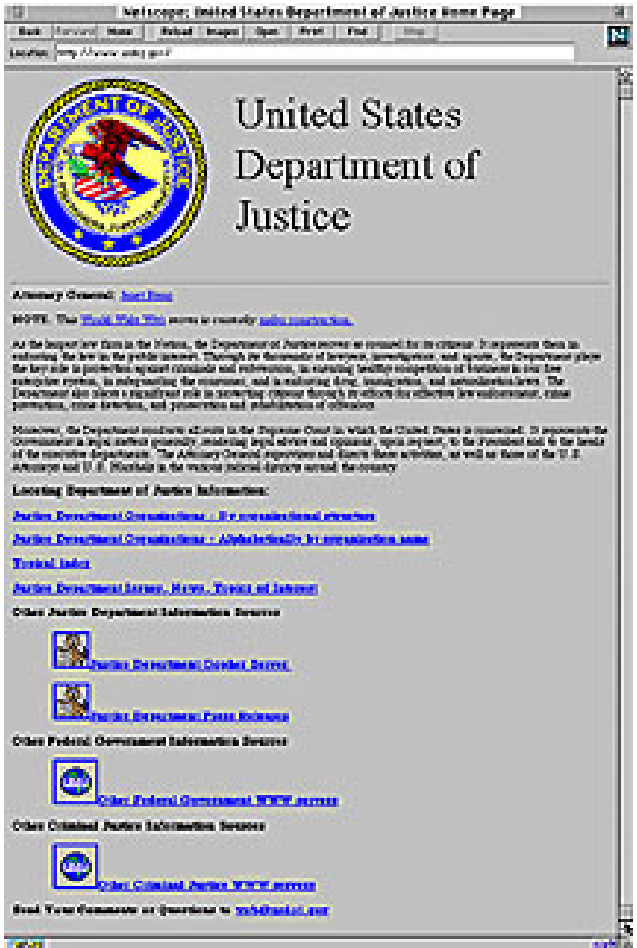
"dos de cada cinco empresas que enfrentan ataques o daños en sus sistemas dejan de existir ",

Fuente: Gartner Group

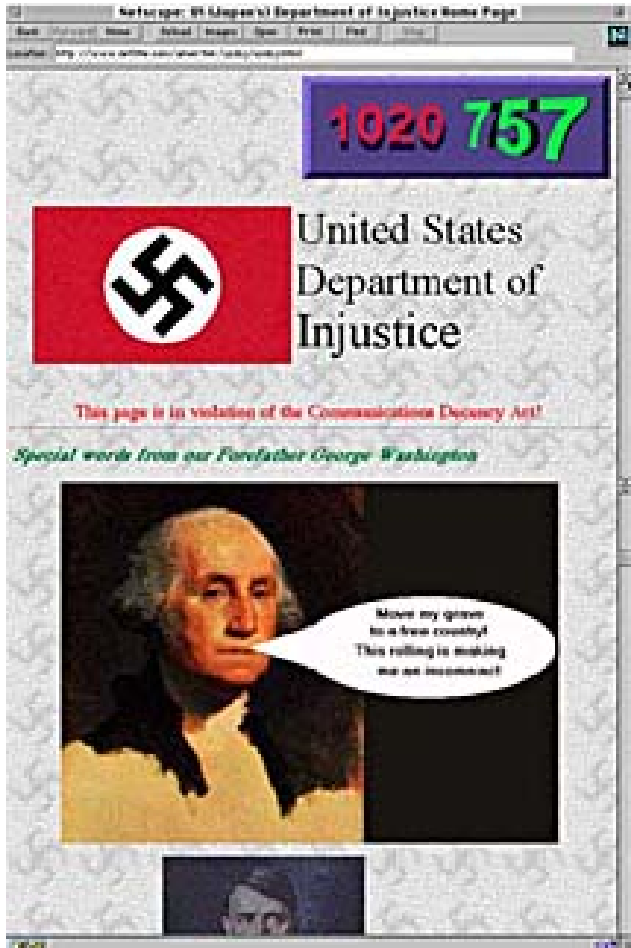
Cual podría ser la consecuencia de una mala práctica de seguridad y protección de la información..

Hacking de la pagina web??..

official site



hacked site



Department of Justice
Hack date: August 1996
Hackers broke into the Justice Department's Web site, adding swastikas, obscenities and a picture of Adolf Hitler to the page.
Justice officials said the hackers did not gain access to criminal files.

Acceso indebido a datos de clientes??..
Perdidas Económicas??

Credit Card Fraud - The Main Motive For Identity Theft

Purpose	Percentage
To obtain/take over a credit card account	53%
To acquire telecommunications services	27%
To obtain/take over a checking account	17%
To obtain a loan	11%

Source: The Federal Trade Commission

Violación a la confidencialidad de la información??..

DENVER BUSINESS JOURNAL

LATEST NEWS
December 19, 2002

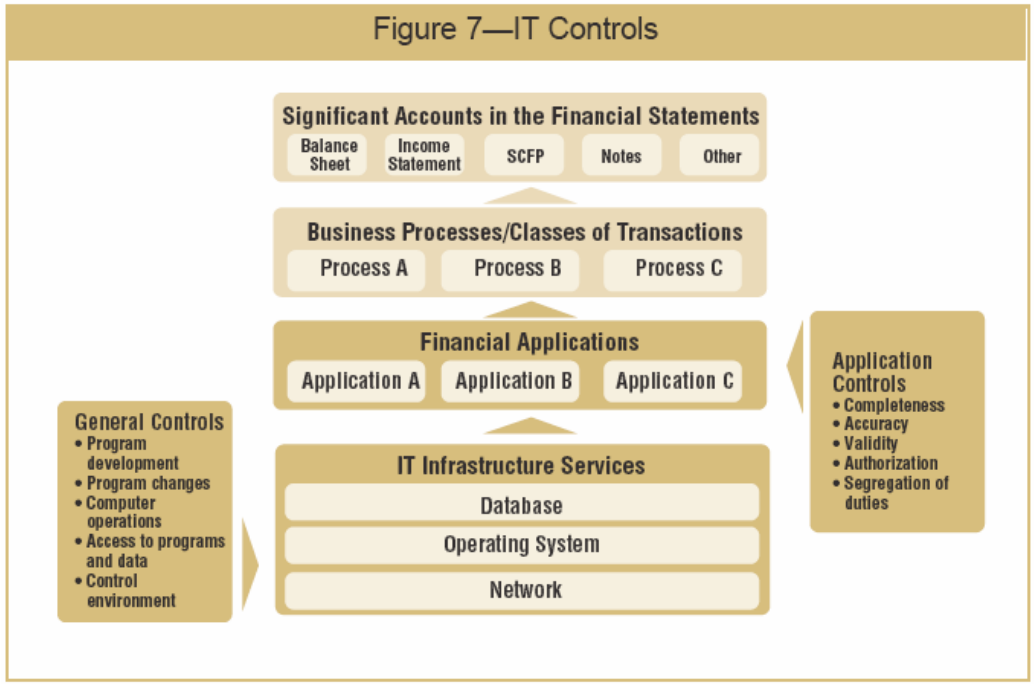
Western Union to pay $8M for N.Y. violation

Western Union Financial Services Inc. reached a settlement on Dec. 18 with the New York State Banking Department for violating the federal Bank Secrecy act in that state.

Without admitting wrongdoing, Western Union agreed to pay the banking department $8 million, Some of those deficiencies supposedly occurred because of a cumbersome compliance system and problems converting it to a more automated system, the SEC filing said. Centralizing Western Union's compliance system, as part of the system change, also has been troublesome.

Incumplimiento de Regulaciones??..

Por ahora, la seguridad es un componente primario en la mayoría de regulaciones, desde las mas generales hasta las mas especificas. Últimamente, la infraestructura es de los mas valiosos activos de la organización, al tratarse de cumplimiento, ya sea para proteger la información del cliente, accionistas o la propiedad intelectual de la empresa.



TEOREMA 1:

Cualquiera que sea la consecuencia,
La información es un ACTIVO
con intrínseca VULNERABILIDAD
a las potenciales AMENAZAS.

TEOREMA 1:

Cualquiera que sea la consecuencia, La información es un ACTIVO

con intrínseca VULNERABILIDAD

a las potenciales AMENAZAS

Seguridad de la Información

ACTIVO

Confidencialidad
Integridad
Disponibilidad

más

Autenticidad
Auditabilidad
Protección a la duplicación
No repudio
Legalidad
Confiabilidad de la información

AMENAZAS

Ingeniería Social
Man-in-the-middle
Phishing
Defacement
Spoofing
Backdoors
Escaneo de puertos
Catástrofe
Trashing
Código malicioso
Robo
Fraude informático
Eavesdropping
Exploits

COROLARIO 1:

No existe la Absoluta Seguridad de la Información, pero las organizaciones deben entender los Riesgos y adoptar una estrategia para reducirlos a niveles aceptables (mitigar).

Un enfoque holístico debe asegurar que las amenazas a activos de información crítica sean efectivamente Administrados.

No se trata sólo de antivirus y de firewalls !!.

DEFINICION 1:

SEGURIDAD DE INFORMACION : Se refiere a la PROTECCION de activos de IT contra riesgos de pérdida, mal uso no intencional y deliberado, exposición o daño.

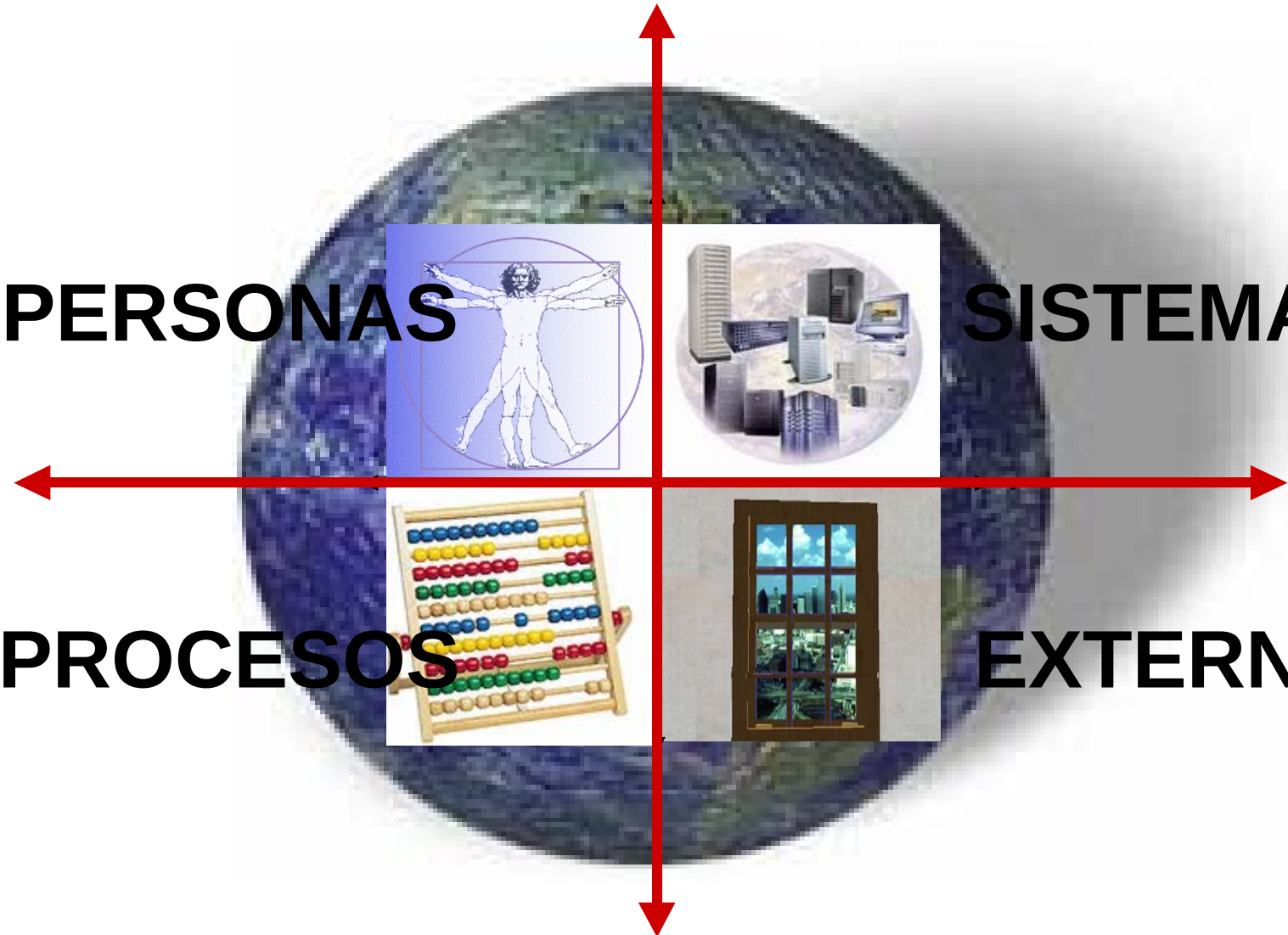
ADMINISTRACION DE LA SEGURIDAD DE INFORMACION: define los controles que la organización necesita implementar para asegurar que hay una sensibilidad al tratamiento de los riesgos en todo momento.

Riesgos de la Información

"Los reguladores financieros instruyen a la industria bancaria en enfocarse en el Riesgo Operacional, que comprende a la Seguridad de la Tecnologia de Informacion ",

Fuente: IT Governance Institute

Cobertura del Riesgo Operacional (Basilea II) como Referencia de Tendencias Internacionales:



Análisis de Riesgo para la Seguridad de la Información (AS/NZS 4360 –Risk Management Process)

Los objetivos del Análisis de Riesgos..(AS/NZS 4360)

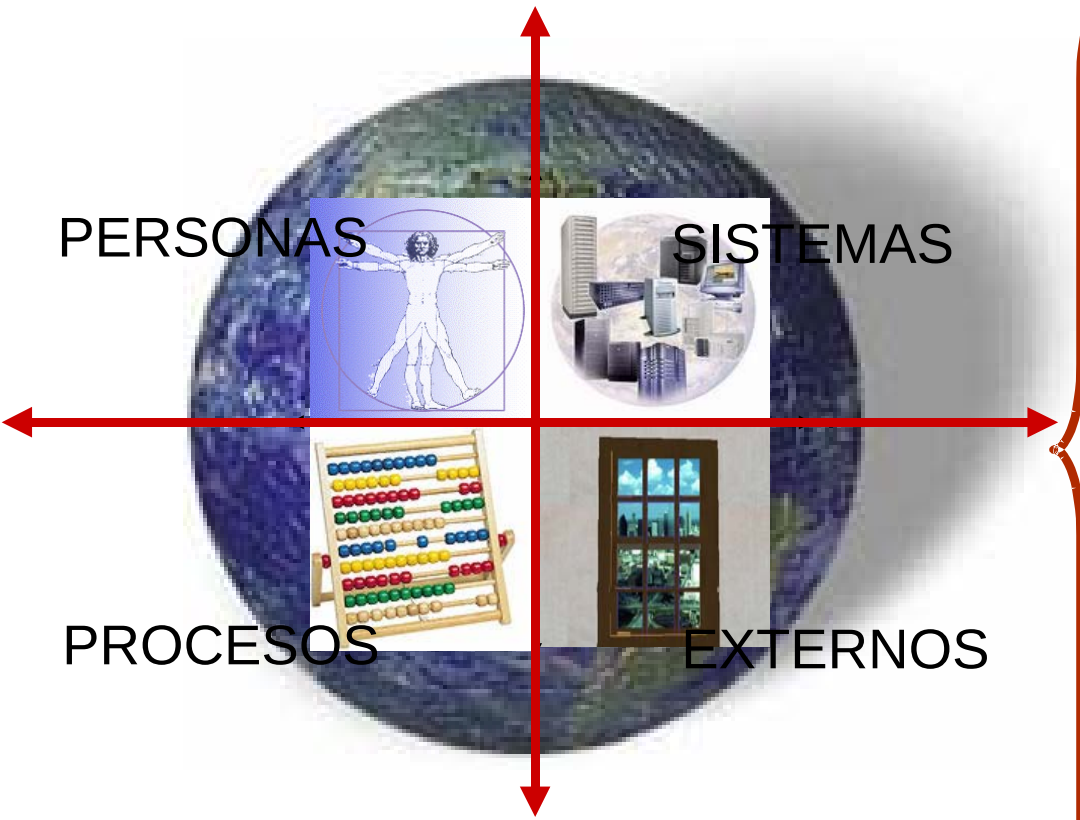
- Identificar los activos de información critica mas valiosos para la organización
- Identificar las amenazas asociadas con esos activos
- Analizar y cuantificar los riesgos que dichas amenazas representan y categorizarlos
- Evaluar opciones para su tratamiento, sea eliminar o mitigar los riesgos
- Definir proceso continuo de monitoreo y revisión

Este paso preliminar permite a la organización enfrentar de una manera estructurada la administración del riesgo, asegurando que los recursos de personal y financiero se enfoquen en las áreas de mayor riesgo al inicio.

Administración de Riesgos de Información

A Diferencia de las tendencias de Basilea II y Riesgo Operacional, la Administración de Riesgos de Información excluye a los factores Externos.

Amenazas reconocidas por tendencias Internacionales que afectan la Seguridad de la Información:



- Globalización
- Crecimiento de los medios electrónicos
- Fusiones y Adquisiciones a gran escala
- Mayor automatización tecnológica
- Mayor oferta en proveedores de servicios
- Incremento del Outsourcing
- Complejidad y cobertura de productos
- Crecimiento de los volúmenes de negocio
- Regulaciones y Normativas
- Crimen Casual u Organizado

Comunes a Basilea II (Riesgo Operacional) Y Administración de Riesgos de Información

Consecuencias Directas de Inadecuada Administración de Riesgos de Información:

- Robo, daño o perdida de Activos físicos o lógicos de información
- Robo, explotación y exposición deliberada de información sensible
- Exposición accidental de información privilegiada por alusión irresponsable (Soc. Eng)
- Poco control de información documental o registro de información.
- Destrucción o corrupción de información deliberadamente o accidentalmente.
- Señalamiento por incumplimiento de legislaciones o normativas..
- Ataques a redes (hacking) o danos a la infraestructura IT organizacional, o alteración de contenidos e información.

Consecuencias Indirectas de Inadecuada Administración de Riesgos de Información:

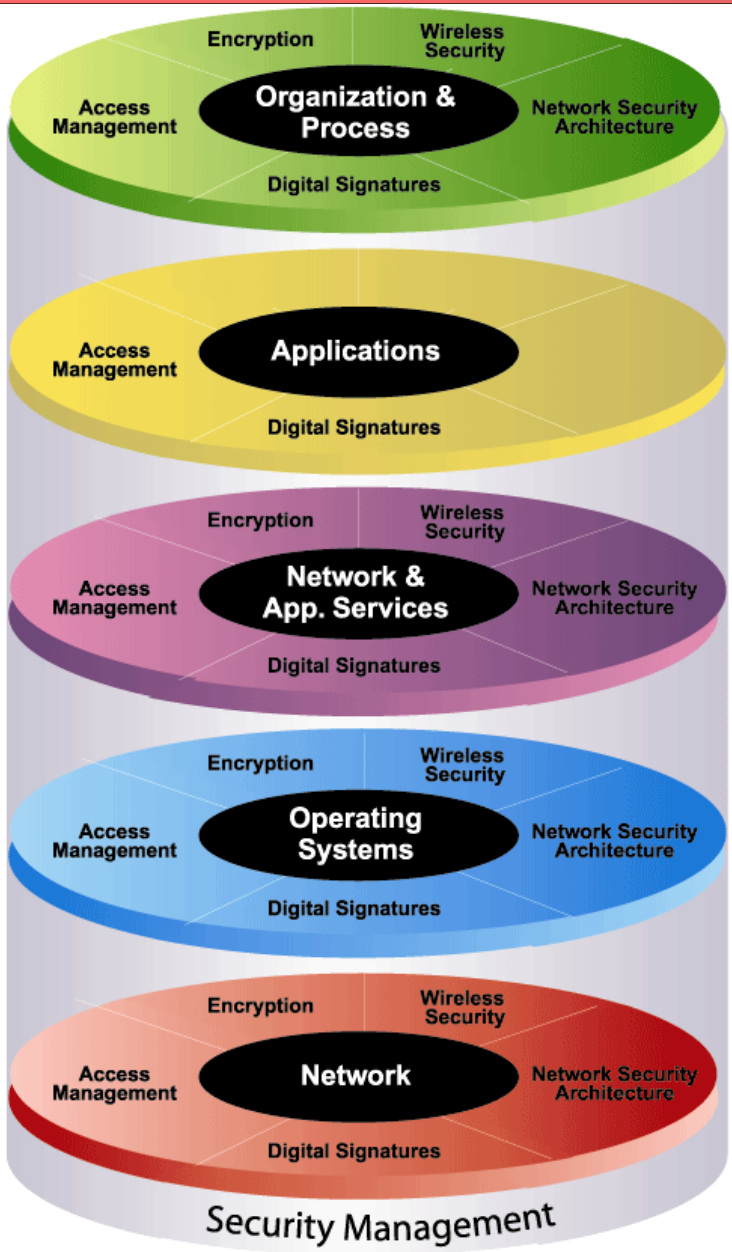
- Incremento en las primas de seguros.
- Inclusión de cláusulas de penalización y exigencias de Evaluación de Vulnerabilidad
- Agencias o Medios de Financiamiento o Socios Comerciales requerirán Evaluaciones de Seguridad de la información como condición contractual.

TEOREMA 2:

La identificación de Riesgos a través de la Administración de Riesgos de Información, dictara las prioridades y los riesgos críticos a ser atendidos, mostrando las áreas donde se requiere desarrollar políticas de seguridad y protección de la información.

COROLARIO 2:

Es indispensable que la organización establezca una estrategia que profundice en las capas que conforman la organización a fin de identificar y Mitigar los riesgos, en estricta interacción con Auditoria.



The Organisation & Process Layer comprises the policies, processes and governance framework required to direct and guide the organisation towards effective security. Everyone within and associated with the organisation must understand their role.

The **Application Layer** comprisesend-user applications such as MS Office, Peoplesoft and the web browser.

The **Network and Application Services Layer** comprises supporting libraries and packages such as databases and middleware.

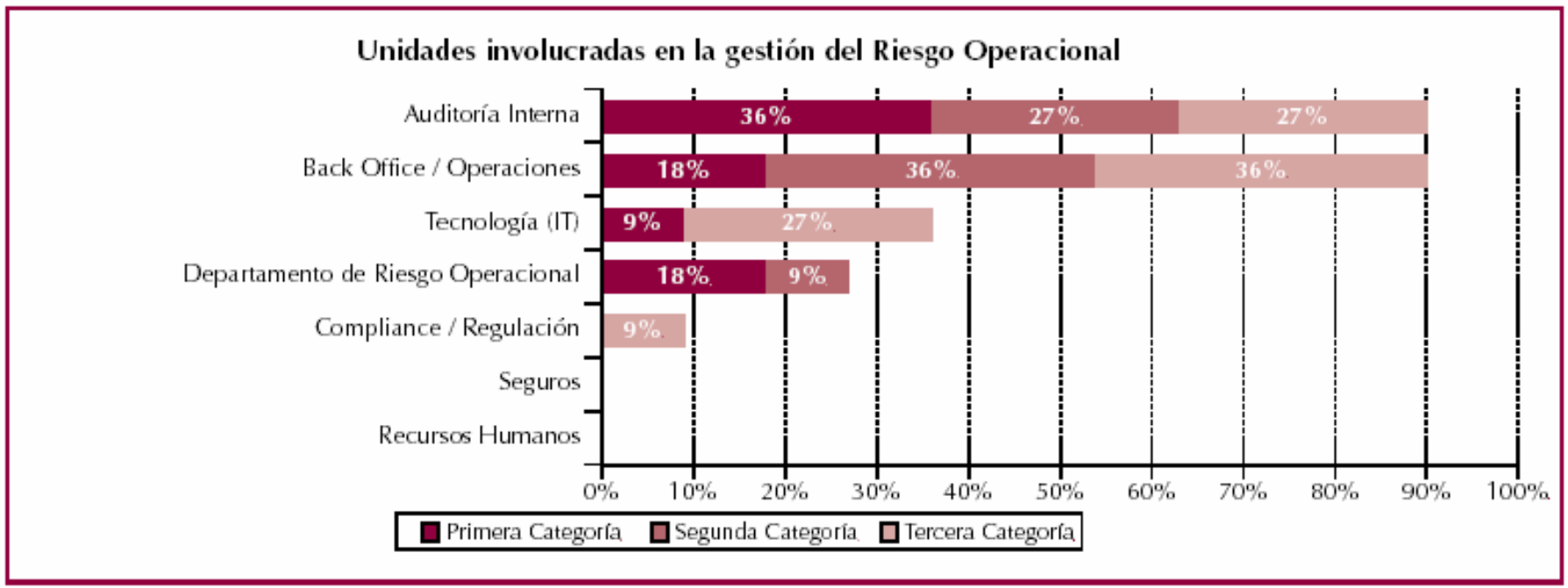
The **Operating Systems Layer** comprises the computer and network operating system such as Windows NT/2000, Solaris and Linux.

The **Network Layer** comprisesthe physical network hardware and software such as Firewalls, Ethernets, ATM networks, Routers and Switches.

Correlación entre Gestión de Riesgos y Auditoria Interna

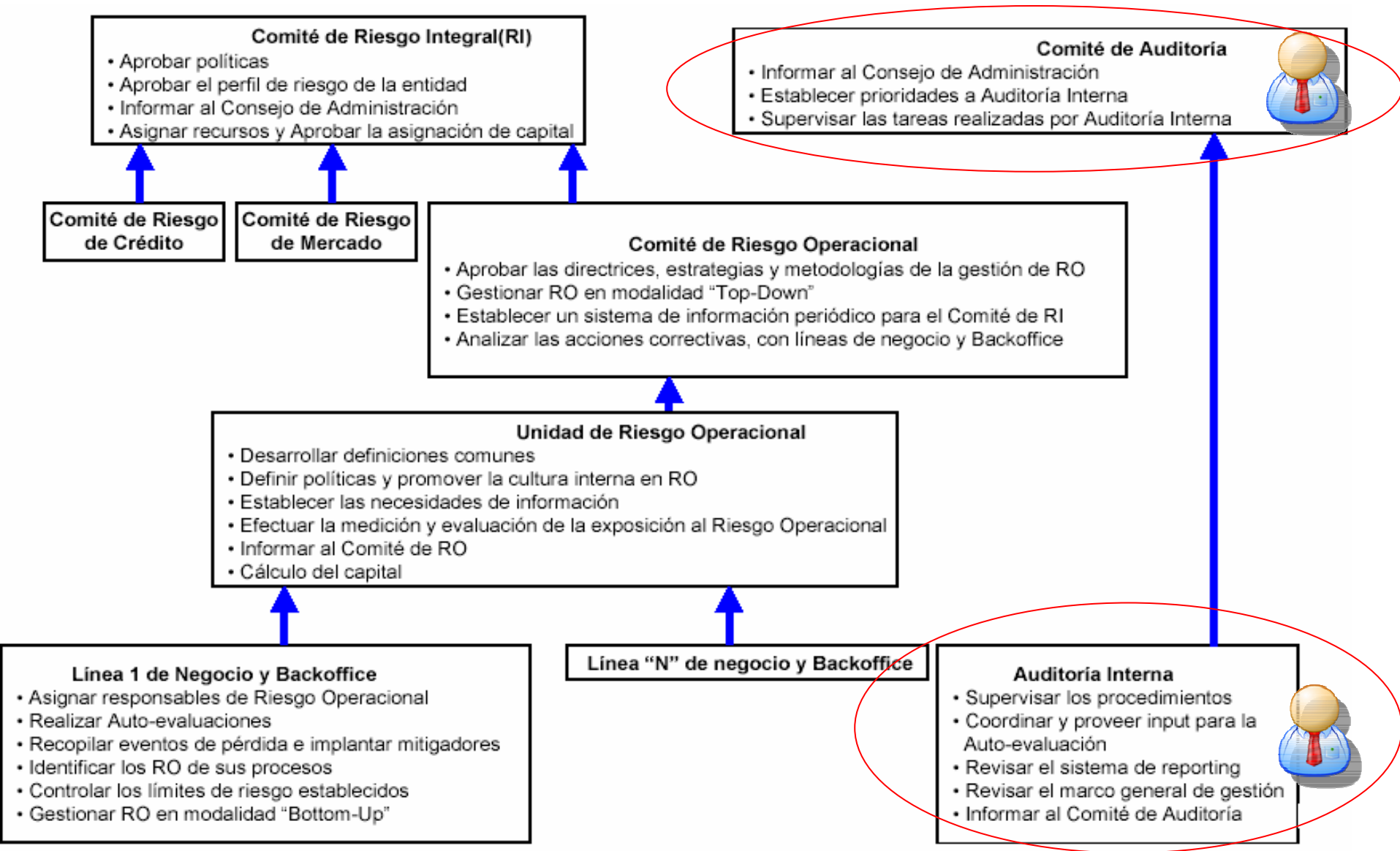
Auditoría, Operaciones y Sistemas..

Auditoría Interna tiene el papel de verificar el cumplimiento de los procesos de gestión del riesgo, pero no de la ejecución propia del mismo.



Fuente PWC -2002

Marco de Gestión Integral de Riesgos



Políticas de Seguridad de la Información

"Actualmente las Entidades Financieras están desarrollando programas y políticas de protección de la información metódicos encaminados a ser liderados por las áreas de negocio. ",

Fuente: IBM Consulting Services

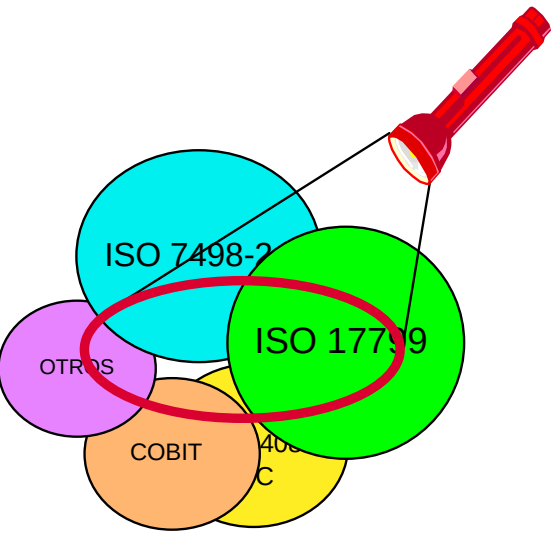
Los programas de Protección de la Información han ido evolucionando área por área hacia un manejo de riesgo integral, basados en códigos de práctica de Seguridad de la Información

Código de Práctica Utilizado

- Identificación y Autenticación
- Control de Acceso
- Integridad
- Confidencialidad
- Disponibilidad
- No repudio
- Monitoreo
- Manejo de Riesgo
- Política

Inicio

Que complementados con requerimientos legales y del negocio han sido el fundamento para la creación de la Política de Seguridad de la Información



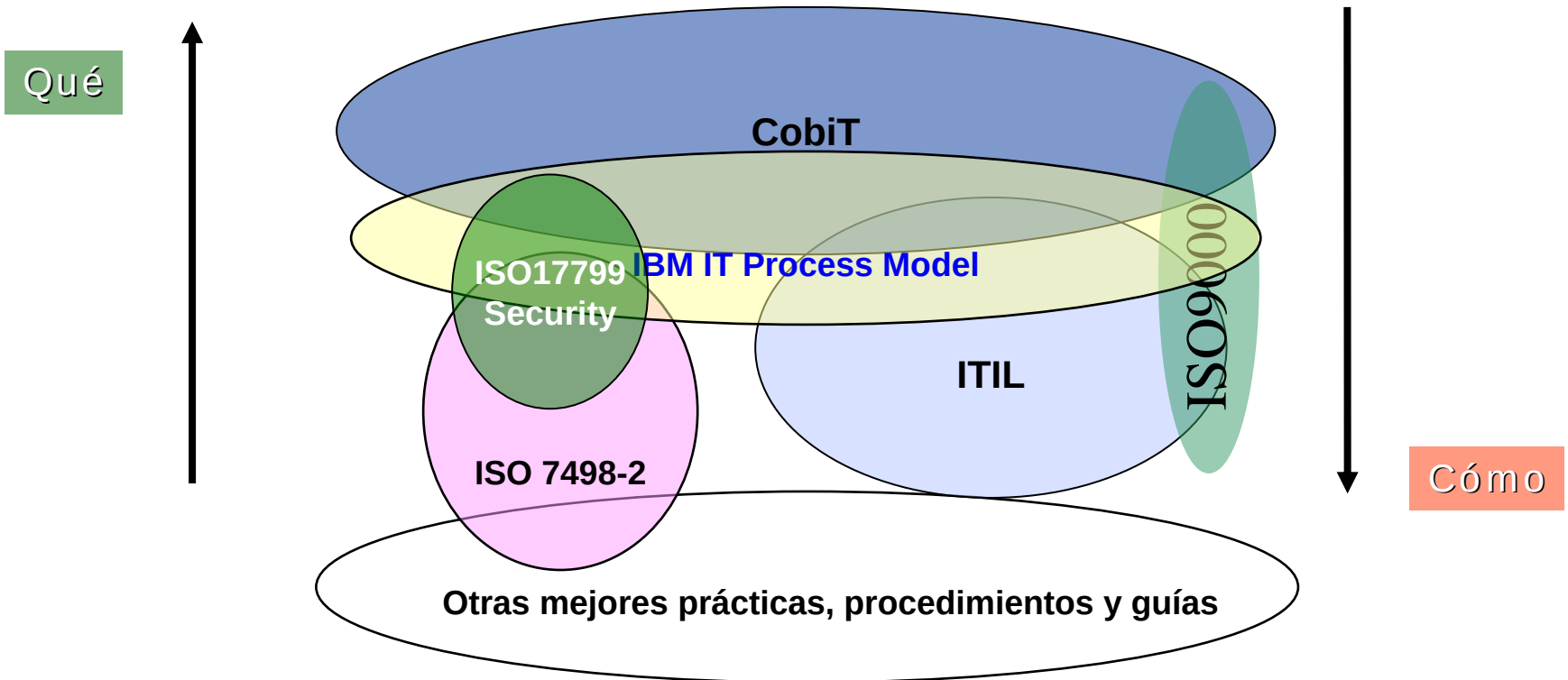
+

Requerimientos
-Negocio
-Legales (Sarbanes & Oxley, Basilea II)
-Riesgo

=

En la selección de los códigos de práctica, base para generar la Política de Seguridad de la Información, se han utilizado los reconocidos por el mercado

En general todos buscan los mismos objetivos pero a diferentes niveles de abstracción



El Standard ISO/IEC 17799
(Code of Practice for Information Security Management)

La Norma ISO 17799

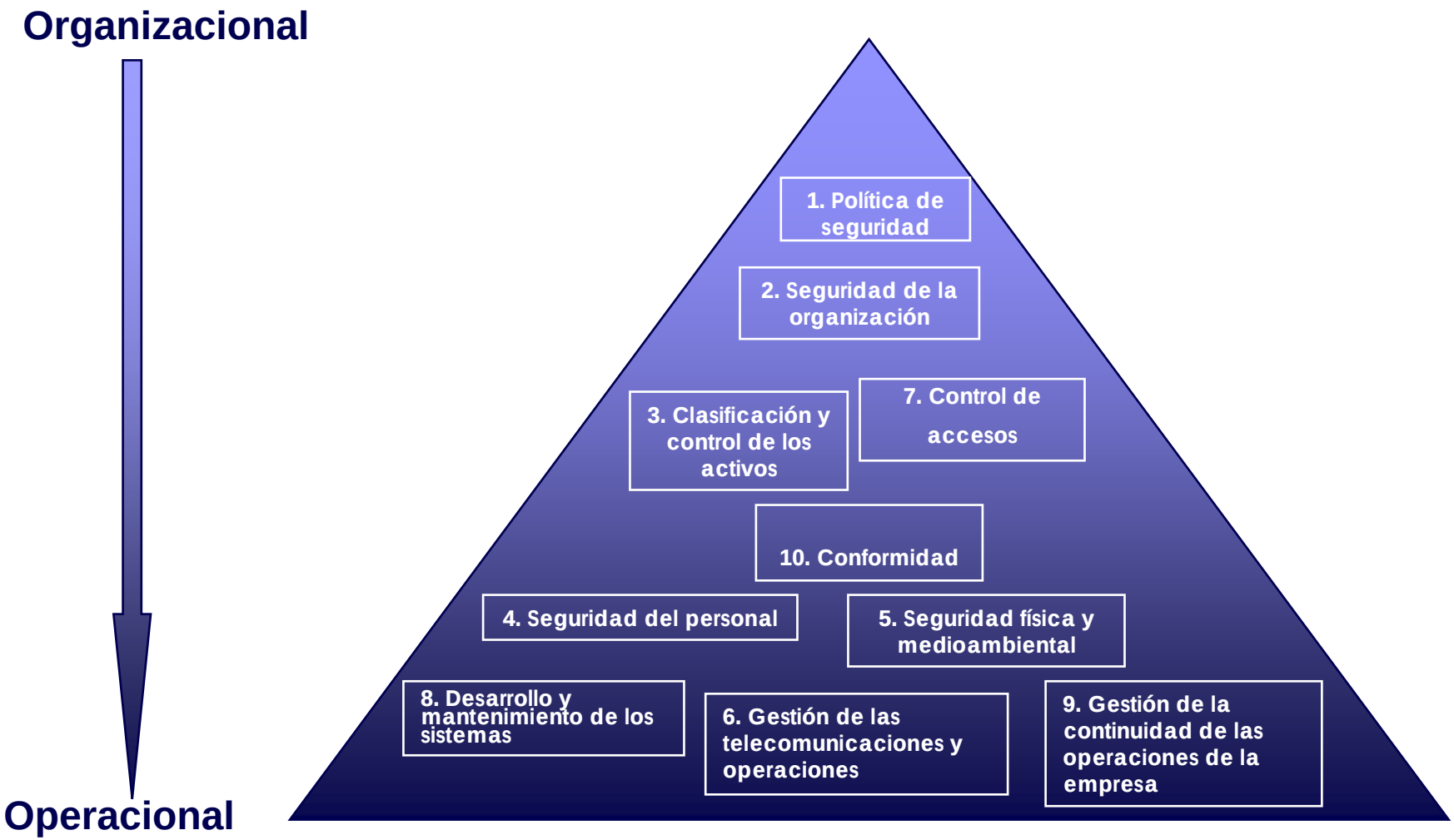
ISO 17799 en la actualidad es un compendio de recomendaciones y prácticas exitosas de seguridad que toda organización puede aplicar independientemente de su tamaño o sector.

La norma técnica fue redactada intencionalmente para ser flexible y nunca indujo a las personas que la cumplían para que prefirieran una seguridad específica.

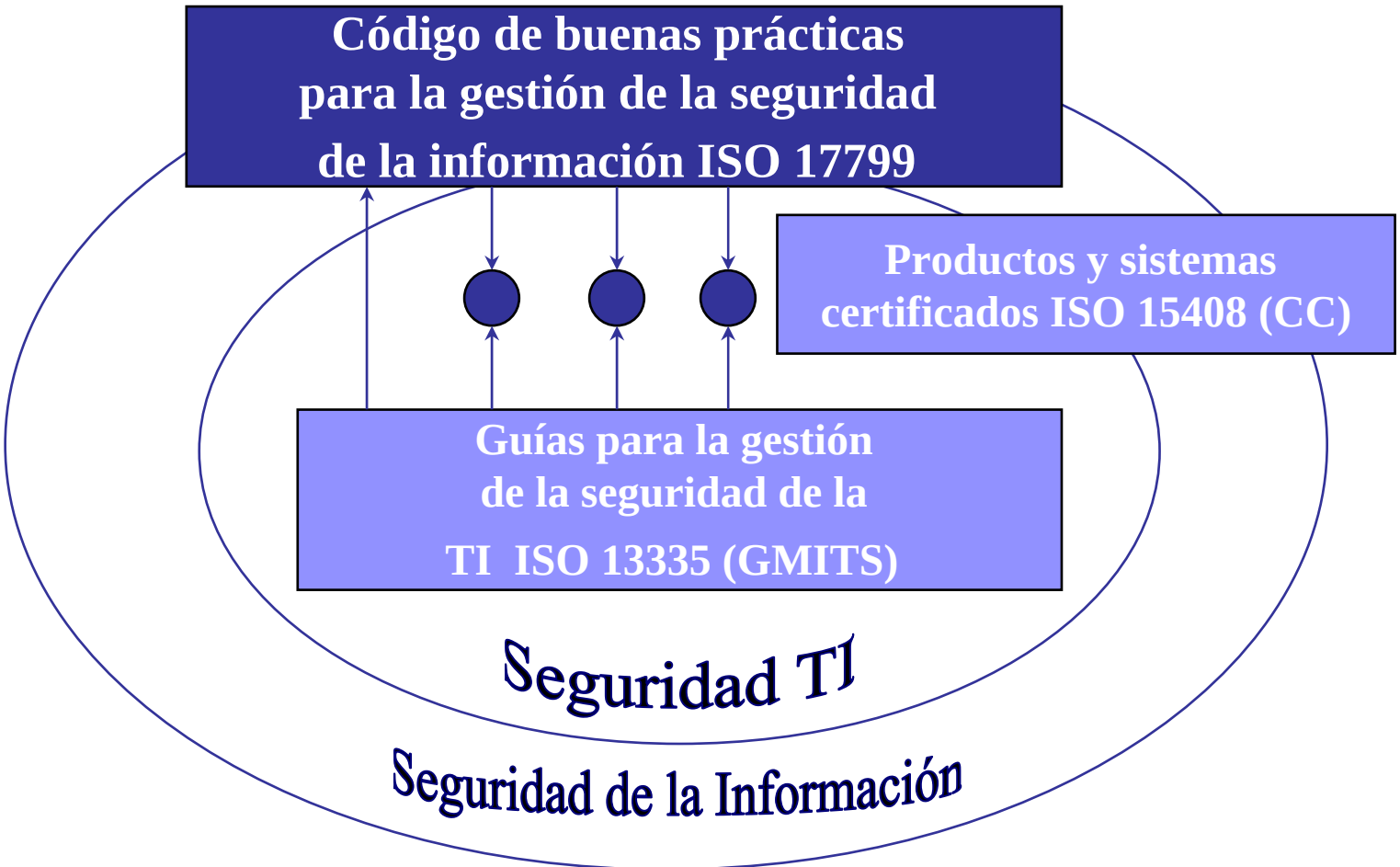
Las recomendaciones de la norma ISO 17799 son neutrales en cuanto a la tecnología y no ayudan a evaluar y entender las medidas de seguridad existentes.

Estructura de la Norma ISO/IEC 17799

Estructura de la Norma ISO/IEC 17799 en la Organización



Complementariedad con otros estándares ISO



Ventajas de la norma ISO 17799

Las organizaciones que hacen uso de la norma ISO 17799 experimentan ventajas competitivas que le permiten garantizar lo siguiente:

- Protección de los bienes de la empresa (información y actividades);
- Protección de la información en las comunicaciones y software;
- Protección ante accesos malintencionados;
- Prevención de alteraciones en las comunicaciones entre organizaciones; y
- Procesamiento seguro de la información.

Beneficios de la norma ISO 17799

Una empresa certificada con la norma técnica ISO 17799 puede ganar frente a sus competidores no certificados. Si un cliente potencial tiene que escoger entre empresas diferentes y la seguridad es un aspecto trascendente, por lo general optará por la certificada. Además una empresa certificada tendrá en cuenta lo sig:

- Mayor seguridad en la empresa;
- Planeación y manejo de la seguridad más efectivos;
- Alianzas comerciales y e-commerce más seguros;
- Mayor confianza en el cliente;
- Auditorías de seguridad más precisas y confiables; y
- Menor responsabilidad civil.

PLUS

TECHNOLOGIES
& INNOVATIONS

THANKS FOR YOUR TIME !