

BEST PRACTICES FOR SECURITY



BEST PRACTICES (ITIL, COBIT, ISO 17799)

The effective adoption of best practices can provide many benefits, especially in the area of advanced technology.

These include:

- Avoiding re-inventing wheels
- Reducing dependency on technology experts
- Increasing the potential to utilise less-experienced staff if properly trained
- Making it easier to leverage external assistance
- Overcoming vertical silos and nonconforming behaviour
- Reducing risks and errors
- Improving quality
- Improving the ability to manage and monitor
- Increasing standardisation leading to cost reduction
- Improving trust and confidence from management and partners
- Creating respect from regulators and other external reviewers
- Safeguarding and proving value

IT mgmt

Figure 1—Stakeholders in IT Management Issues				
Top Management Issues Addressed by Standards and Best Practices (Based on the COBIT Framework)	Who Has a Primary Interest?			
	Board/ Executive	Business Management	IT Management	Audit/ Compliance
Plan and Organise				
Are IT and the business strategy in alignment?	✓	✓	✓	
Is the enterprise achieving optimum use of its resources?	✓	✓	✓	✓
Does everyone in the organisation understand the IT objectives?	✓	✓	✓	✓
Are IT risks understood and managed?		✓	✓	✓
Is the quality of IT systems appropriate for business needs?		✓	✓	
Acquire and Implement				
Are new projects likely to deliver solutions that meet business needs?		✓	✓	
Are new projects likely to deliver on time and within budget?		✓	✓	
Will the new systems work properly when implemented?		✓	✓	
Will changes be made without upsetting the current business operation?		✓	✓	
Deliver and Support				
Are IT services being delivered in line with business requirements and priorities?		✓	✓	
Are IT costs optimised?	✓	✓	✓	
Is the workforce able to use the IT systems productively and safely?		✓	✓	
Are adequate confidentiality, integrity and availability in place?		✓	✓	✓
Monitor				
Can IT's performance be measured, and can problems be detected before it is too late?	✓	✓	✓	
Is independent assurance needed to ensure that critical areas are operating as intended?	✓			✓

Mejores prácticas

- ITIL, COBIT, ISO 17799, ISO 9002, Capability Maturity Model (CMM®), Project in Controlled Environments (PRINCE), Managing Successful Programmes (MSP), Management of Risk (M_o_R®) and Project Management Body of Knowledge (PMBOK®)

ITIL

- The processes of service support described in ITIL are:
 - Incident management
 - Problem management
 - Configuration management
 - Change management
 - Release management
 - Service desk function

ITIL

- The processes of service delivery described in ITIL are:
 - Capacity management
 - Availability management
 - Financial management for IT services
 - Service level management
 - IT service continuity management



COBIT

- COBIT's management guidelines are generic and action-oriented for the purpose of answering the following types of management questions:
 - How far should we go and is the cost justified by the benefit? What are the indicators of good performance?
 - What are the critical success factors? What are the risks of not achieving our objectives? What do others do?
 - How do we measure and compare?



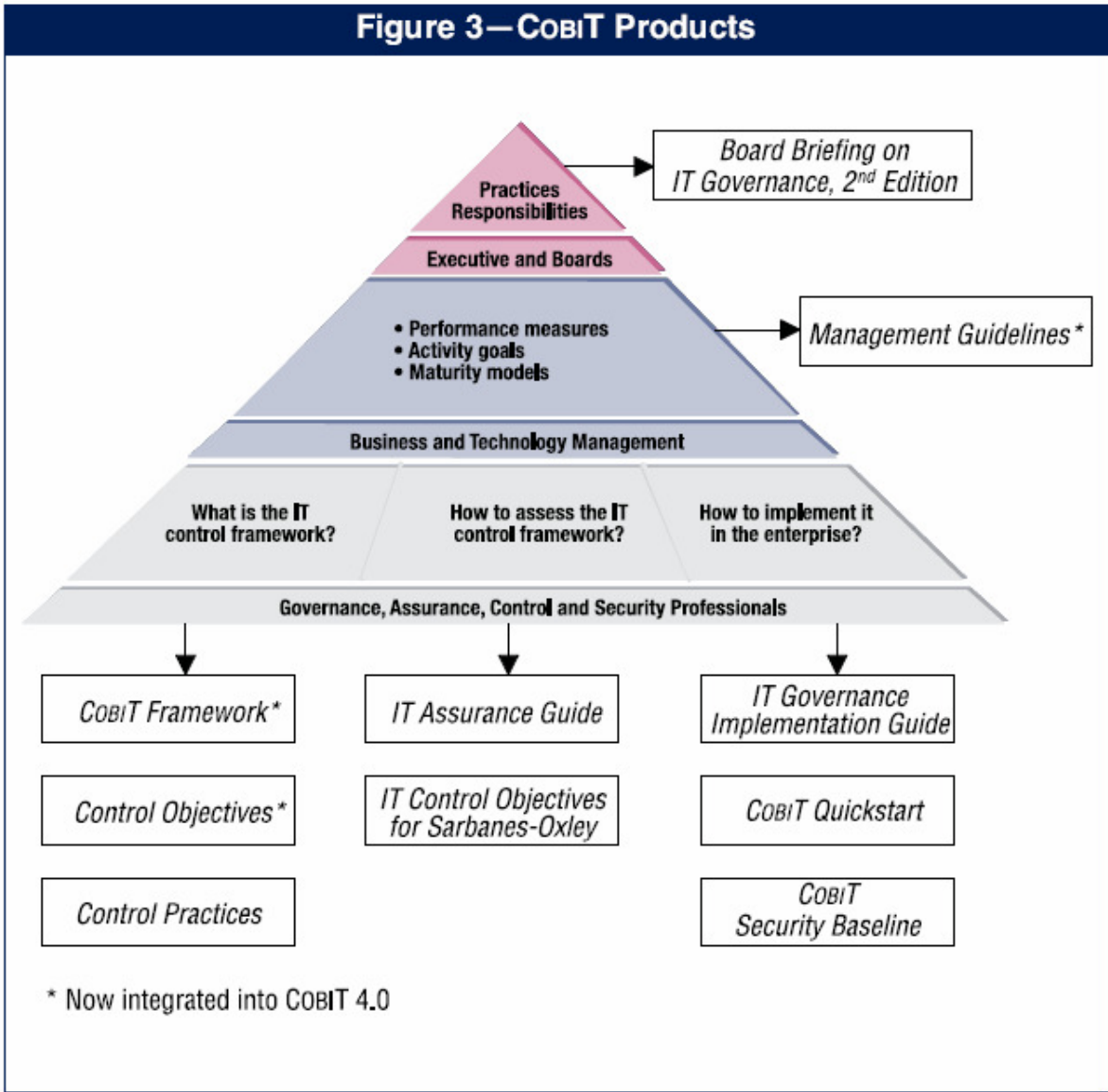
COBIT

Figure 2—IT Governance Focus Areas



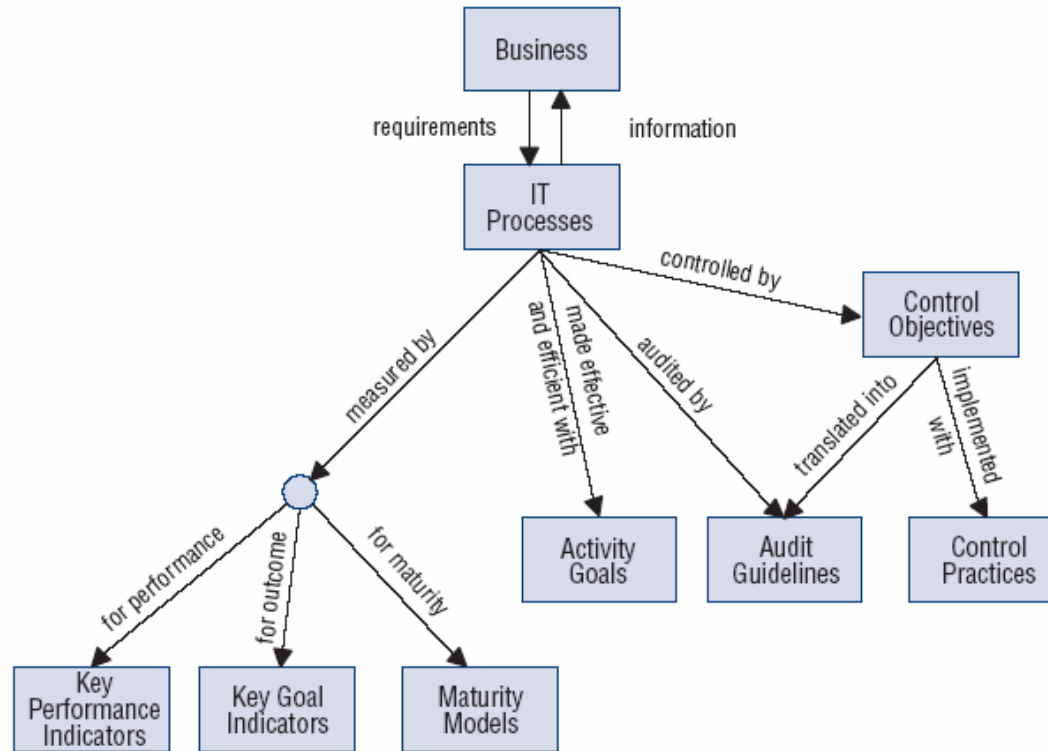
- **Strategic alignment** focuses on ensuring the linkage of business and IT plans; on defining, maintaining and validating the IT value proposition; and on aligning IT operations with enterprise operations.
- **Value delivery** is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimising costs and proving the intrinsic value of IT.
- **Resource management** is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimisation of knowledge and infrastructure.
- **Risk management** requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise, and embedding of risk management responsibilities into the organisation.
- **Performance measurement** tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.

COBIT



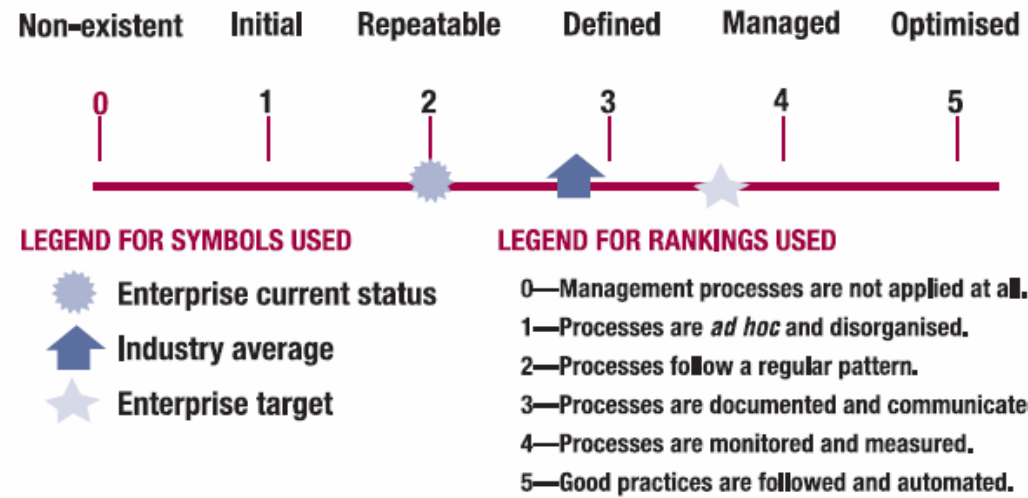
COBIT

Figure 4—Interrelationships of COBIT Components



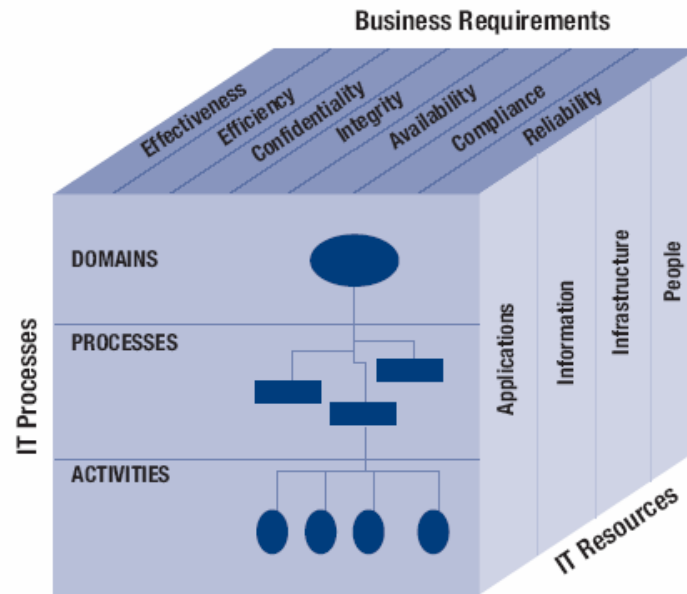
CMM

Figure 9—Graphic Representation of Maturity Models



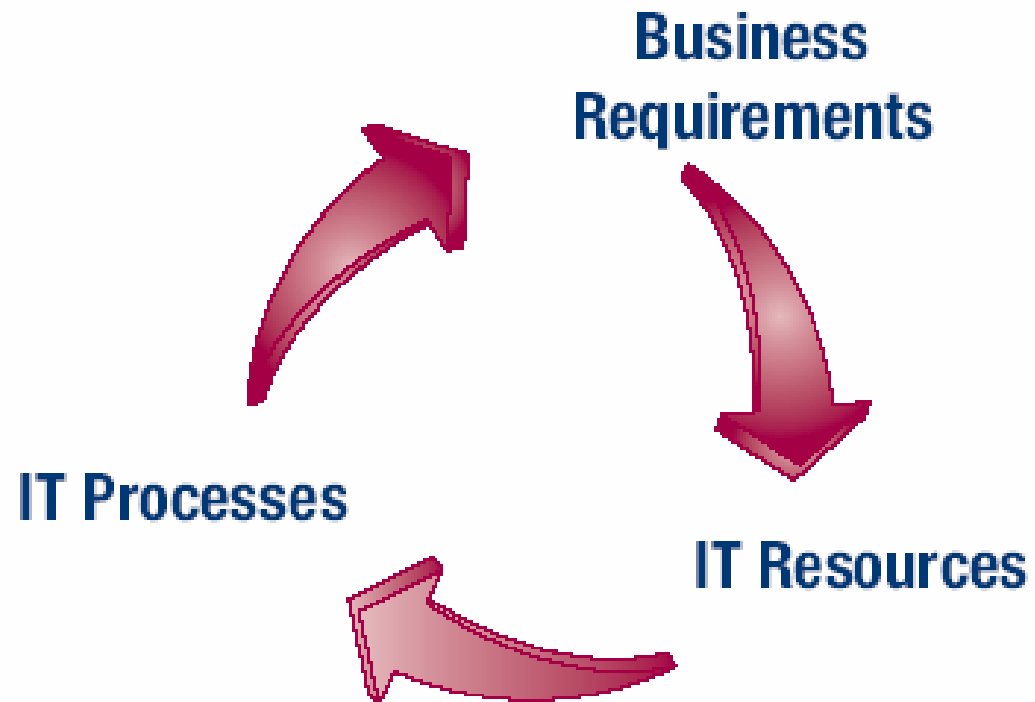
COBIT

Figure 15—The COBIT Cube



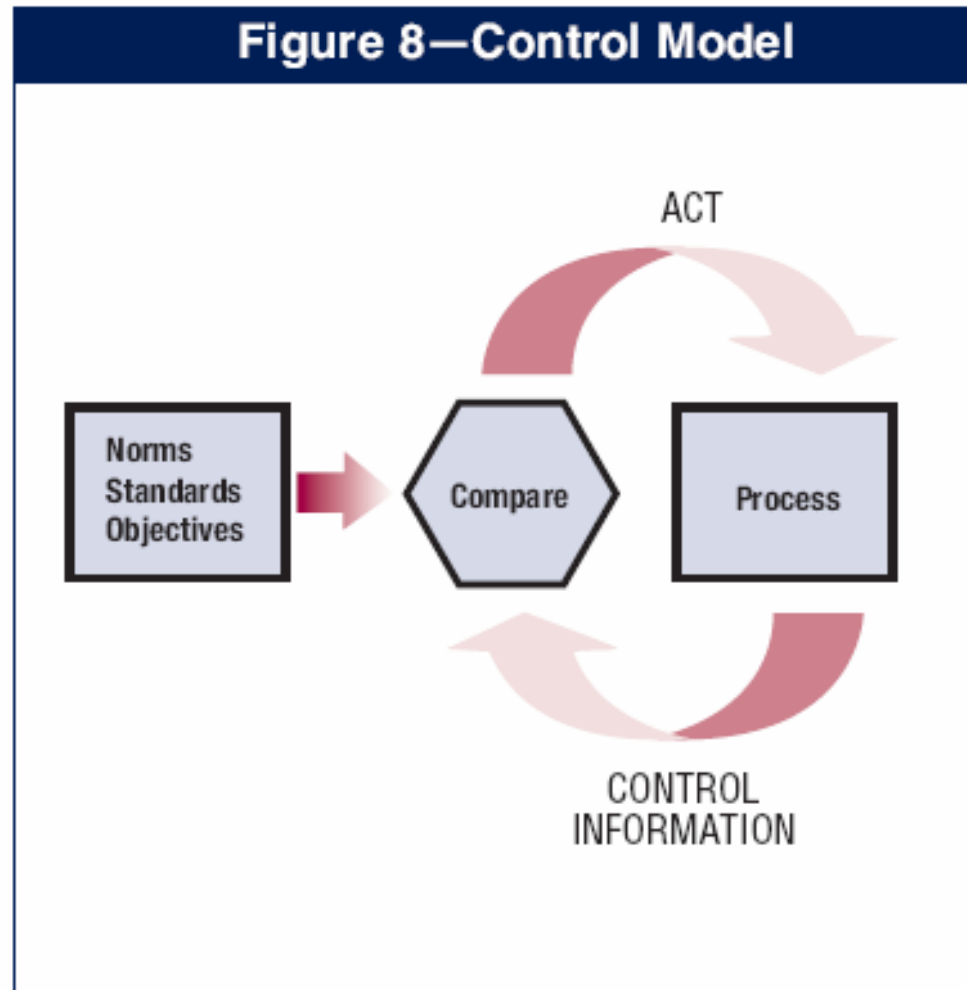
COBIT

Figure 5—Basic COBIT Principle



COBIT

Figure 8—Control Model



SAP

RELIABILITY = AVAILABILITY + PERFORMANCE + SECURITY

ISO

- ❑ ISO: The International Organization for Standardization.
- ❑ IEC: International Electrotechnical Commission)

Qué es el **BS 7799/ISO 17799**

- ❖ Conjunto de controles basado en las mejores prácticas en seguridad de la información
- ❖ ISO/IEC 17799 fue preparado por el British Standard Institution.
- ❖ Estándar internacional el cual genera recomendaciones sobre aspectos de la seguridad de la información tales como:
 - *Equipos*
 - *Políticas administrativas*
 - *Recursos Humanos*
 - *Aspectos legales.*

Definiciones y/o Conceptos

- ❖ La información es un activo.
- ❖ La seguridad de la información protege de un amplio espectro de amenazas, tendientes a garantizar la continuidad del negocio, minimizar danos, y mejor el retorno de las inversiones y oportunidades de negocio.
- ❖ La información existe en múltiples formas.
- ❖ Confidencialidad, Integridad, Disponibilidad.
- ❖ Se logra por el uso adecuado de Controles, Políticas, procedimientos, Estructura Organizacional.

Por qué se necesita?

- ❖ La información, sistemas, redes son activos importantes del negocio.
- ❖ Las amenazas continúan aumentando y cada vez con mayor impacto de tipo financiero.
- ❖ La dependencia es creciente.
- ❖ La mayoría de sistemas de información no se diseñaron pensando en que fueran seguros.
- ❖ No solo aplica a los empleados, sino a proveedores, clientes y accionistas por ejemplo.
- ❖ Los controles son considerablemente más económicos si se establecen en la fase de diseño y no al final.

Cada cuanto?

- Considerar cambios en los requerimientos del negocio y sus respectivas prioridades.
- Considerar nuevas amenazas y vulnerabilidades.
- Confirmar que el control continua siendo efectivo y apropiado.



Beneficios

How implementing the Standard can help

ISF Members agree that, in general, implementing the Standard helps organisations to:

- move towards international best practice
- manage the breadth and depth of information risk
- build confidence in third parties that information security is being addressed in a professional manner
- reduce the likelihood of disruption from major incidents
- fight the growing threats of cybercrime
- comply with legal and regulatory requirements
- maintain business integrity.

Historia

- ❑ En 1995 el British Standard Institute publica la norma BS7799, un código de buenas prácticas para la gestión de la seguridad de la información.
- ❑ En 1998, también el BSI publica la norma BS 7799-2, especificaciones para los sistemas de gestión de la seguridad de la información; se revisa en 2002.

Definición ISO 17799

ISO 17799 es un Estándar internacional que ofrece **recomendaciones** para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

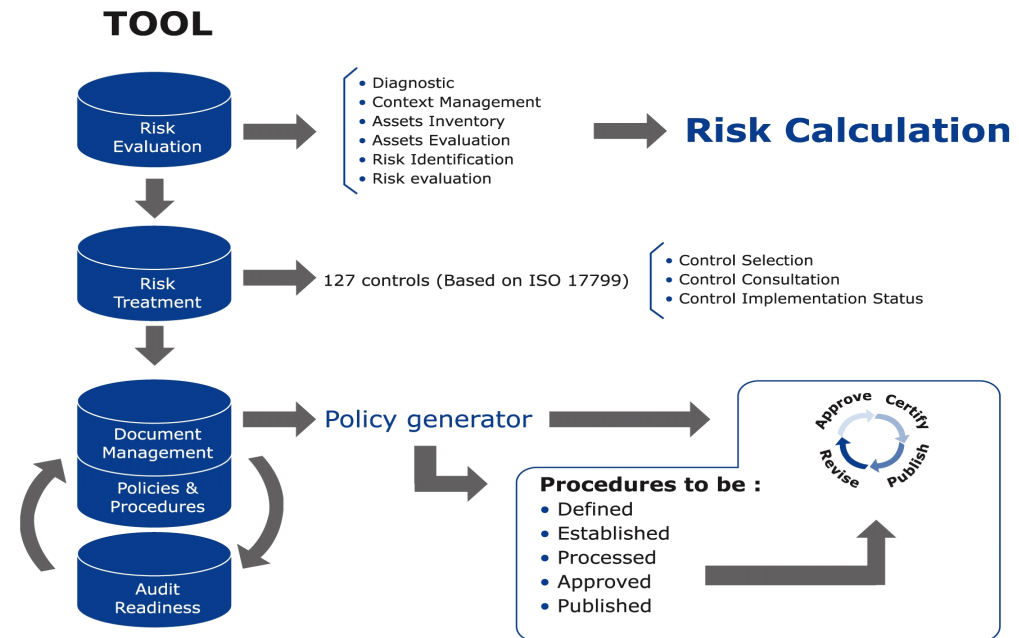
ISO 17799

ISO 17799 define la **información** como un activo que posee valor para la organización y requiere por tanto de una protección adecuada.

El objetivo de la **seguridad de la información** es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

Características de BS 7799 / ISO 17799

- ✓ Probado
- ✓ Público
- ✓ Internacional
- ✓ Asociado con el concepto de calidad
- ✓ Evolución y flexibilidad



Consideración sobre el ISO 17799

- La alta dirección debe definir una **política** que refleje las líneas directrices de la organización en materia de seguridad, aprobarla y publicitarla de la forma adecuada a todo el personal implicado en la seguridad de la información.
- Las políticas, se constituyen en la base de todo el sistema de seguridad de la información.
- La alta dirección debe **apoyar visiblemente** la seguridad de la información en la compañía.



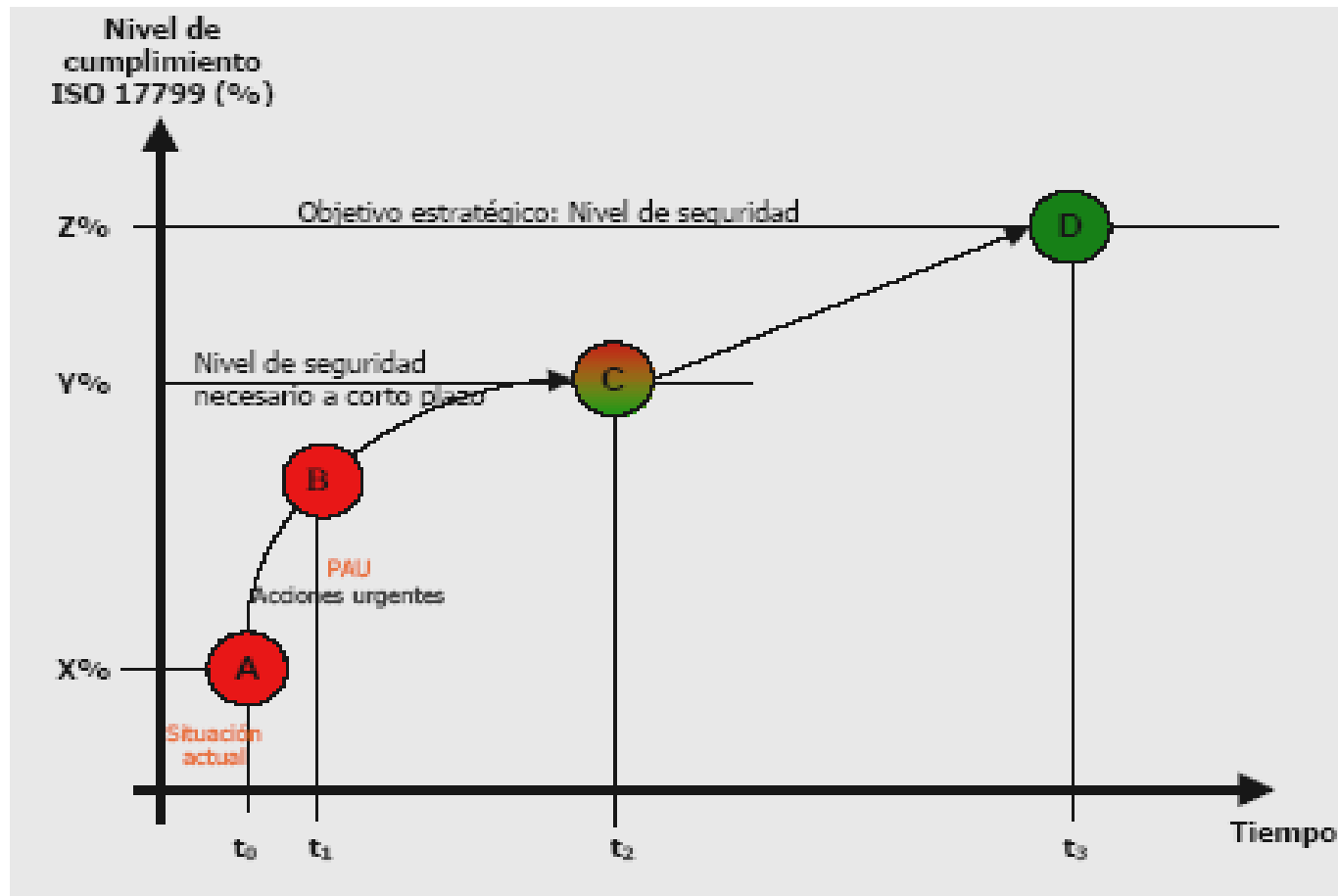
ISO 17799



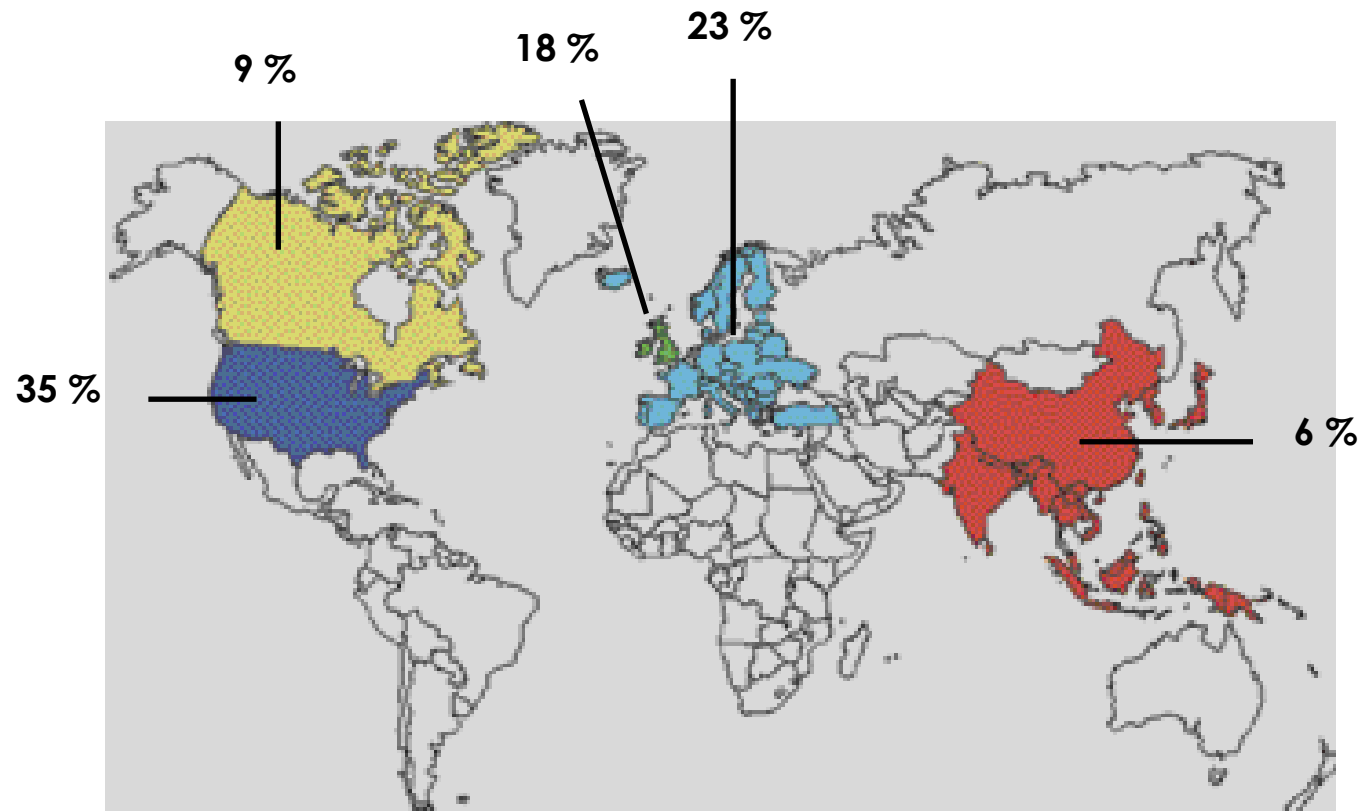
Objetivos Basicos.



Proceso Continuo



Compras en línea del ISO 17799

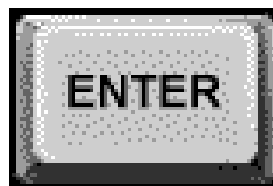


Otros : 9 %



Beneficios

- Procedimientos en línea con disposiciones de tipo gubernamental.(reconocimiento internacional)
- Mejor protección a la confidencialidad, integridad y disponibilidad de la información.
- Mitigar riesgo a diferentes ataques
- Rápida y eficiente forma de recuperarse ante posibles amenazas.
- Cumplimiento con disposiciones legales.



Cont.

- ❖ Aumento de la **seguridad efectiva** de los sistemas de información.
- ❖ Correcta **planificación** y gestión de la seguridad.
- ❖ Garantías de **continuidad del negocio**.
- ❖ **Mejora continua** a través del proceso de auditoría interna.
- ❖ Incremento de los niveles de **confianza** de nuestros clientes y *partners*.
- ❖ Aumento del **valor comercial** y mejora de la **imagen** de la organización.

Factores Críticos de Éxito

- ✓ Alineamiento con la organización.
- ✓ Consistente con la cultura de la org.
- ✓ Soporte visible y compromiso de las directivas.
- ✓ Buen entendimiento de los requerimientos de seguridad (risk assessment and risk management)
- ✓ Educación
- ✓ Indicadores de Gestión.

Seguridad en la Organización



Introducción

- ❑ La administración de la seguridad, define los roles y responsabilidades dentro de la organización, con el objetivo de mantener e implementar el Sistema de Gestión de Seguridad de la información.
- ❑ Colaboración de directivos, usuarios, administradores, desarrolladores y personal de seguridad, así como también especialistas en el área de aseguramiento y manejo de riesgo.
- ❑ Visión multidisciplinaria a el tema de la seguridad de la información.
- ❑ Cooperación entre Usuarios, gerentes, administradores etc.

Definición de la Política.


- ✓ *“La seguridad de la información es una responsabilidad compartida por todos los miembros de la dirección. El Comité de Seguridad debe garantizar que las políticas cumplen con los requerimientos de negocio de la organización, y velar por el apoyo de la administración para su implementación.”*




Temas asociados a la Política.

- Roles y Responsabilidades de la administración de la seguridad.
- Auditorias externas.
- Seguridad en el acceso por parte de terceros.
- Compra y mantenimiento de software comercial.
- Outsourcing
- Asistencia de especialista en S.I.
- Revisión independiente de los Sistemas de Información.

Funciones del Comité de seguridad

- ❑ *Revisar y aprobar las políticas, procedimientos y estándares de seguridad.*
 - ❑ *Evaluar cambios significativos de la exposición de los activos de información a las amenazas de seguridad.*
 - ❑ *Seguimiento de incidentes de seguridad reportados por el Oficial de Seguridad.*
 - ❑ *Apoyar a la administración en la implementación del entrenamiento en seguridad de la información a los usuarios.*
 - ❑ *Evaluar los avances en los proyectos o iniciativas de seguridad.*
- 

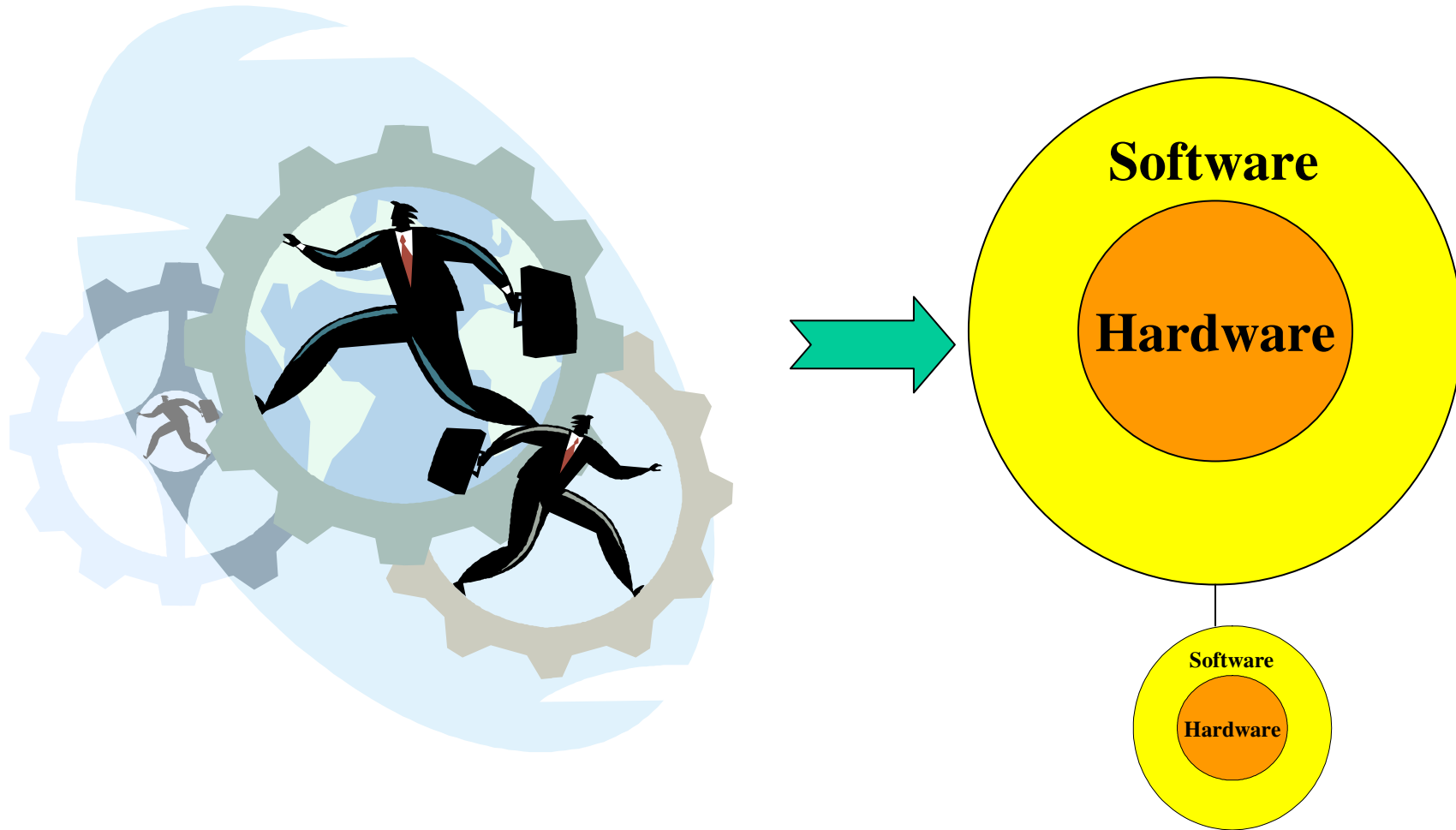
Funciones del Oficial de Seguridad

- ❑ *Desarrollar, implementar y administrar un programa de seguridad de la información.*
 - ❑ *Asesorar a la organización como incluir la seguridad de la información en las fases de inicio de todos los proyectos de tecnología de la información.*
 - ❑ *Revisar las políticas, procedimientos y estándares según lo estipulado y presentar los cambios para la aprobación del comité de seguridad.*
 - ❑ *Participar en la definición de los controles de seguridad para la plataforma tecnológica de la organización.*
 - ❑ *Evaluar, realizar el seguimiento y reportar los incidentes de seguridad relevantes al comité.*
 - ❑ *Asegurar que los planes de contingencia sean desarrollados, mantenidos y probados regularmente para su funcionamiento.*
 - ❑ *Asegurar que los controles de acceso de cada sistema de información estén de acuerdo con el nivel de riesgo evaluado.*
- 

Aspectos de la seguridad relacionados con el aspecto humano



Gestion de Redes



Introducción

- El recurso humano es uno de los elementos fundamentales dentro del modelo de seguridad de la organización.
- Las políticas, los procedimientos y estándares de seguridad, son llevados a cabo en el desarrollo diario de las actividades por el personal vinculado a la organización, y sin su compromiso, el modelo no sería exitoso.
- Evitar errores humanos, robo, fraude o uso inadecuado de los recursos.
- Debe empezar con el proceso de contratación.

Seguridad en aspectos relacionados con el recurso humano.

- Soportar las políticas de seguridad de la compañía en el curso del trabajo normal.
- Minimizar el daño ocasionado por incidentes de seguridad y poder aprender de ellos.
- Entrenamiento y Concientización.
- Acuerdos de confidencialidad.
- Respuesta a incidentes de seguridad.
- Reportes de vulnerabilidades y funciones equivocadas del software.
- Procesos disciplinarios.



Clasificación y Control de Activos



Clasificación y Control de activos.

- El objetivo de esta sección es mantener una apropiada protección de los activos de la compañía y garantizar que los activos informáticos reciban un nivel apropiado de Seguridad.
- Para todos los activos se debe identificar un dueño y responsables para la implementación de los controles.
- Inventarios de activos.
- Clasificación de la información.(Labelling and Handling).



Beneficios

- Muestra el compromiso de la organización hacia la seguridad de la información.
- Ayuda a identificar que información es la más valiosa para la organización.
- Permite identificar que protecciones aplican a que información.

Ejemplo de Activos

- a) Information assets: databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, archived information;
- b) Software assets: application software, system software, development tools and utilities;
- c) Physical assets: computer equipment (processors, monitors, laptops, modems), communications equipment (routers, PABXs, fax machines, answering machines),
- d) Services: computing and communications services, general utilities, e.g. heating, lighting, power, air-conditioning.

Administración de operaciones

- Garantizar operaciones seguras en sitios de procesamiento de la información.
- Minimizar el riesgo de fallas de los sistemas usando por ejemplo segregación de las actividades o funciones.
- Proteger la integridad del software y la información.
- Mantener la integridad y la disponibilidad de los sistemas de información.
- Garantizar la protección de las redes y la infraestructura de soporte.
- Prevenir daños a los activos y fallas en la continuidad del negocio.
- Prevenir pérdida, modificaciones, o un mal uso de la información.
- Control de Cambios.



Administración de operaciones

Cont.

- Information Back up
- Operators logs
- Disposal of media
- Information Handling Procedures
- Seguridad de documentos
- Seguridad de los medios en transito.
- Seguridad en procesos de ecommerce.
- Seguridad en email
- Planeamiento futuro de capacidad.
- Protección contra software malicioso.



Continuidad del negocio

- El objetivo de esta sección es eliminar las posibles interrupciones a las actividades propias del negocio y procesos críticos, con el fin de evitar fallas o desastres.
- BCP
- DRP
- Planes de Contingencia.
- MTD
- BIA



Conformidad con leyes civiles, contractuales y legales.

- Los objetivos de esta sección son:
- Evitar actos criminales, civiles, regulatorios o de algunos de los requerimientos de seguridad.
- Garantizar cumplimiento de las políticas y estándares de seguridad.
- Maximizar la efectividad y minimizar la interferencia de los procesos de auditoría.



Sistemas de control de acceso

Los objetivos de esta sección:

- Controlar el acceso a la información.
- Prevenir el acceso no autorizado a los sistemas de información.(O.S)
- Protección de los servicios de redes.
- Detectar actividades no autorizadas.
- Garantizar seguridad con sistemas móviles o portátiles.
- Password use
- Equipos no atendidos.
- Políticas en el uso de la red.
- Enforced path.
- Authentication.
- Segregation of Networks.
- Monitoreo.



Desarrollo y mantenimiento de sistemas

- Garantizar seguridad en los sistemas operacionales.
- Prevenir pérdidas, modificaciones o mal uso de los datos de las aplicaciones.
- Proteger la confidencialidad, autenticidad e integridad de la información.
- Garantizar que los proyectos de IT son conducidos de una manera segura.
- Mantener la seguridad del software y sus respectivos datos.



Resultados Evaluación

Dominio	Cumplimiento
Política de Seguridad	
Desarrollo y Mantenimiento de Sistemas.	
Control de Acceso.	
Administración de Operaciones.	
Administración de la Continuidad del Negocio	
Seguridad en la Organización.	
Aspectos de Seguridad relacionados con el recurso humano.	
Control y Clasificación de Activos	
Conformidad con leyes civiles, contractuales y legales.	
Seguridad Física.	



Seguridad Física



Objetivo de la seguridad Física

- Entender la importancia de la seguridad física en la protección de activos valiosos de información para los negocios de la empresa.



Objetivo Cont.

- El objetivo fundamental de la seguridad física es garantizar un ambiente seguro para todos los activos e intereses de la organización, incluyendo los sistemas de información.
- Aspectos mecánicos, organizacionales, naturales (CPTED).

Centro de computo

(Mejores prácticas)

- No más que dos puertas, con seguros electrónicos.
- Control de acceso (Tarjeta mas un PIN)
 - No alimentos, bebidas, cigarrillos, combustibles, no trabajos de construcción sin autorización.
- Tomas eléctricas adicionales para equipos eléctricos de mantenimiento
- Paredes de altura completa
- Paredes, puertas y techo deben tener una adecuada resistencia al fuego.
- Redundancia en general.(HVAC, Potencia, Electricidad, etc)
- Teléfonos de emergencia y salidas de emergencia delimitadas.