



Certificación BS 7799

Barcelona, 13 de febrero de 2006

- Introducción al BS7799
- Fases de implementación
 - Desarrollo del SGSI
 - Implantación de controles
- Preguntas

- **Introducción al BS7799**
- Fases de implementación
 - Desarrollo del SGSI
 - Implantación de controles
- Preguntas

- El estándar se compone de dos partes:
 - BS7799-1:2000 (ISO/IEC 17799:2005)
 - 133 mejores prácticas de seguridad (controles)
 - NO CERTIFICABLE
 - Únicamente guía de referencia
 - BS7799-2:2002 (ISO/IEC 27001:2005)
 - Especificaciones para la gestión de la seguridad de la información: creación de un Sistema de gestión de la seguridad (ISMS).
 - CERTIFICABLE
 - Describe un modelo de gestión basado en una metodología PDCA (Plan – Do – Check – Act) para la mejora continua
 - Exige la implantación de algunos controles de la primera parte del estándar.
- Se ha establecido un periodo de transición para que todas las entidades certificadas en BS7799 parte 2 se adapten a la ISO27001. Este periodo es de 18 meses desde enero de 2006.

- ❖ El **ISO/IEC 17799** establece una selección de controles, incluyendo las mejores prácticas con respecto a la seguridad de la información.
- ❖ Estructurado en **11 secciones**:



- ❖ Dentro de estas secciones, existen **39 objetivos de control** y **133 controles específicos**.

❖ Controles legales y regulatorios:

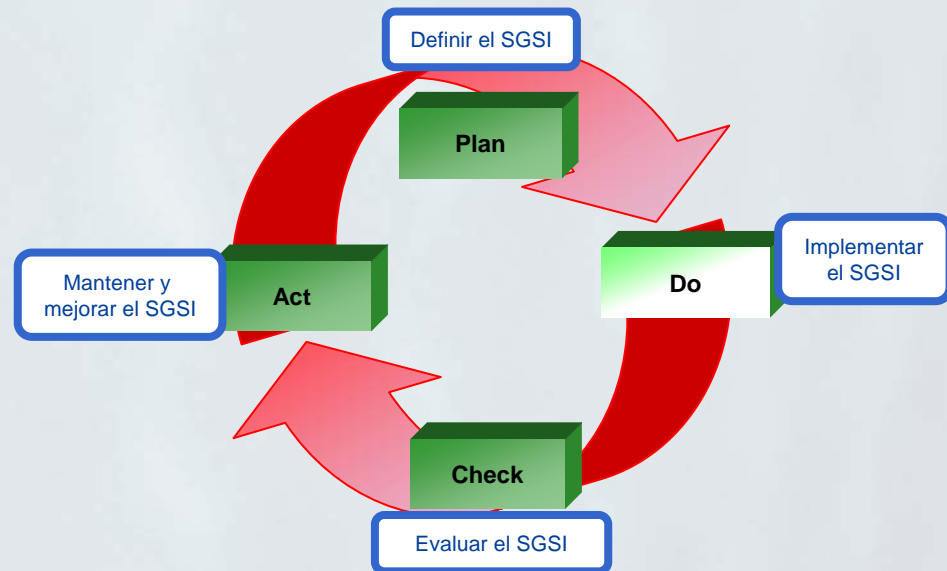
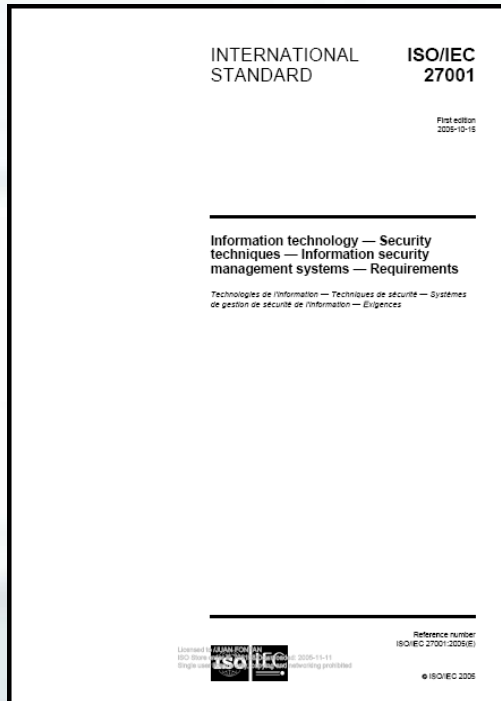
- ☑ Cumplimiento de derechos de copia (Copyrights)
- ☑ Protección de registros de la organización
- ☑ Protección de datos personales y privacidad de información privada

❖ Controles basados en buenas prácticas:

- ☑ Política de Seguridad
- ☑ Establecimiento de responsabilidades de Seguridad de la Información
- ☑ Concienciación y formación en Seguridad
- ☑ Gestión de incidentes de Seguridad
- ☑ Gestión de la continuidad de negocio



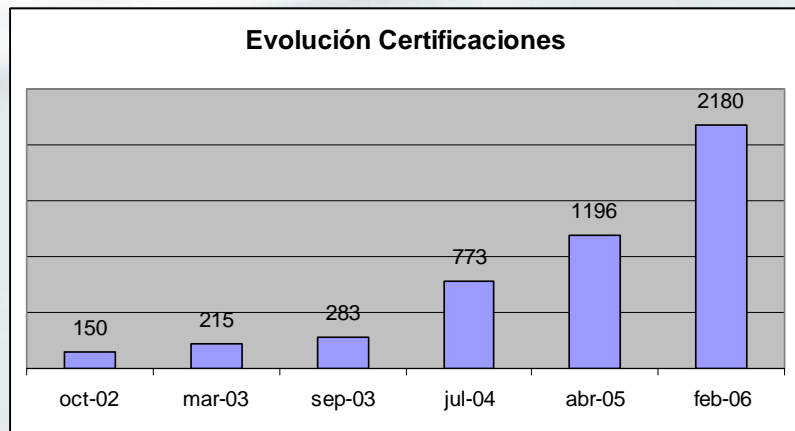
- ❖ El estándar internacional ISO/IEC 27001 contiene las especificaciones para establecer, operar, y mejorar el Sistema de Gestión de la Seguridad de la Información (SGSI)
- ❖ Marco de referencia para la certificación.
- ❖ La metodología aplicada para la implementación del estándar es un modelo **Plan - Do - Check - Act (PDCA)**.
 - ❑ Establece las bases para la mejora continua del SGSI.



- ❖ Los clientes perciben a la organización como un proveedor de “**servicios confiables**” con valor añadido desde un punto de vista de negocio, garantizado por una entidad certificadora internacional.
- ❖ La seguridad en los sistemas de información se gestiona como un **proceso**, no como un **estado**:
 - ❑ La seguridad se focaliza en la **gestión de riesgos** de los sistemas de la información que soportan el negocio.
 - ❑ Se garantiza la **calidad** en cuanto a la gestión de la seguridad.
 - ❑ El enfoque del modelo facilita la **mejora continua**, incrementando progresivamente la madurez y eficiencia de la gestión de la seguridad.
- ❖ Ofrece un marco ideal para la adaptación a requisitos legales, regulatorios, etc.

A Febrero de 2006, se han emitido **2.180** certificados en **60** países

Name of Organization	Certification Body	BS 7799-2:2002 or ISO/IEC 27001:2005
Caja Madrid	BSI	BS 7799-2:2002
ERICSSON ESPA A S.A.	BSI	BS 7799-2:2002
Nextel S.A	BSI	BS 7799-2:2002
Oficina De Armonizacion Del Mercado Interior	BSI	BS 7799-2:2002
T-Systems ITC Services Espana S.A.U	DQS GMBH	BS 7799-2:2002



Argentina	3	Hungary	24	Philippines	4
Armenia	1	Iceland	4	Poland	8
Australia	18	India	151	Qatar	1
Austria	9	Ireland	11	Romania	1
Bahrain	1	Isle of Man	2	Russian Federation	1
Belgium	2	Italy	42	Saudi Arabia	4
Brazil	5	Japan	1271	Serbia and Montenegro	1
Canada	2	Korea	37	Singapore	11
Chile	1	Kuwait	3	Slovak Republic	2
China	25	Lebanon	1	Slovenia	1
Colombia	2	Lithuania	1	South Africa	2
Croatia	4	Luxemburg	1	Spain	5
Czech Republic	6	Macau	2	Sweden	7
Denmark	2	Macedonia	1	Switzerland	13
Egypt	1	Malaysia	2	Taiwan	76
Finland	15	Mexico	3	Thailand	1
France	2	Morocco	1	Turkey	6
Germany	54	Netherlands	27	UAE	3
Greece	5	New Zealand	1	UK	225
Hong Kong	20	Norway	13	USA	32

Total: 2.180

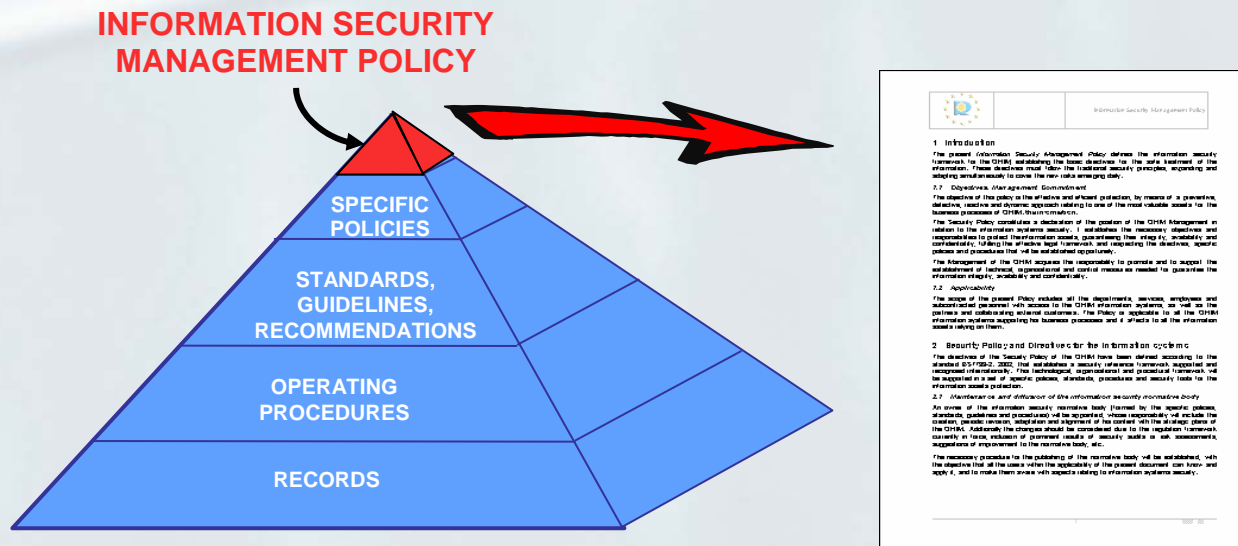
- Introducción al BS7799
- **Fases de implementación**
 - Desarrollo del SGSI
 - Implantación de controles
- Preguntas

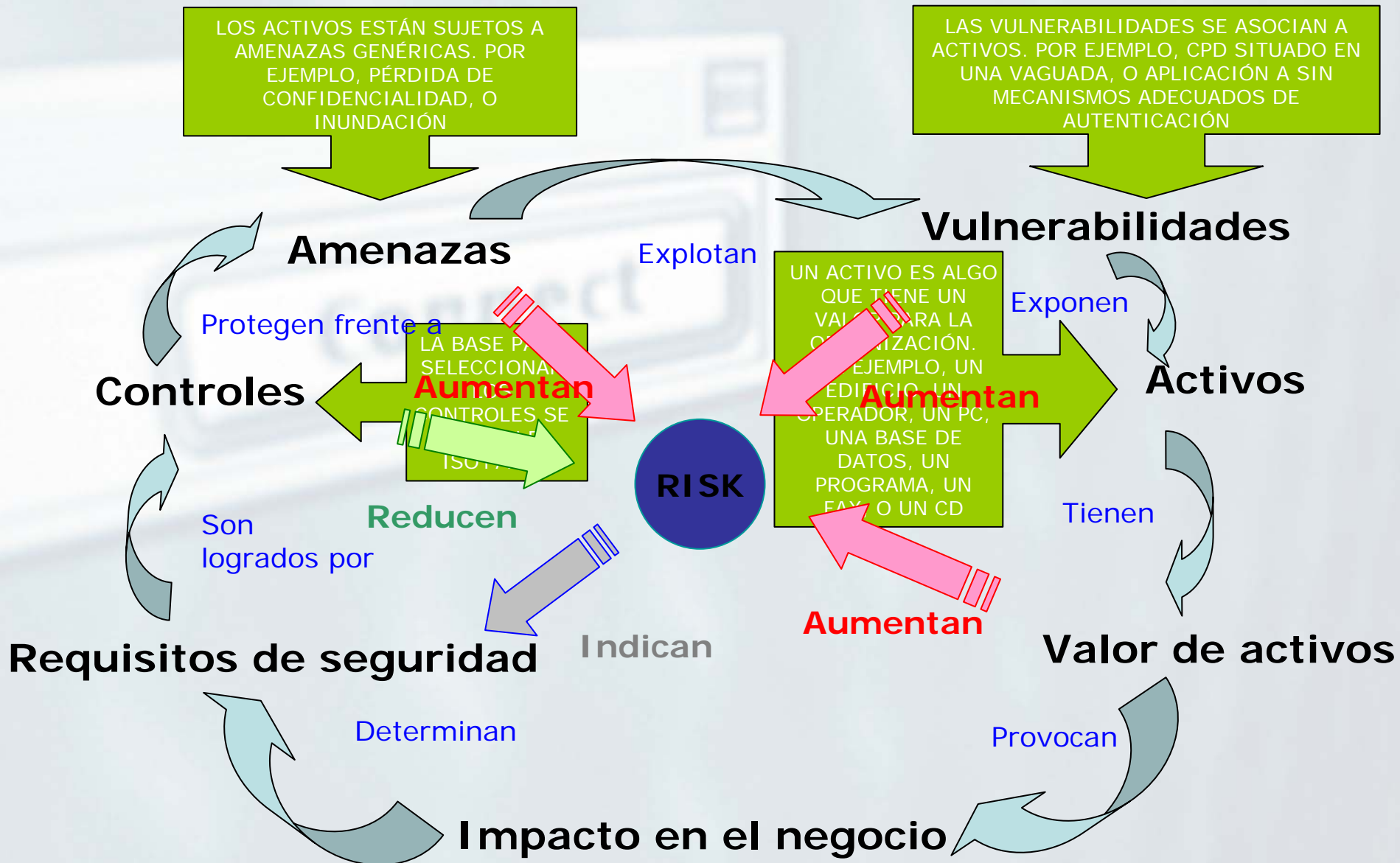


- El ISMS (Sistema de Gestión de Seguridad de la Información) de la OAMI (Oficina de Armonización del Mercado Interior) tiene como ámbito los siguientes procesos asociados al registro de diseños, tanto de entidades jurídicas como físicas:
 - recepción y archivo,
 - examen,
 - registro,
 - inspección pública (de un diseño previamente a su publicación),
 - custodia y publicación.
- En el futuro podrán certificarse otros procesos, o simplemente incluirlos en el sistema de gestión de seguridad (ISMS)

- La Política de Seguridad es el Documento que define el marco general de seguridad que rige en la entidad, estableciendo las directrices básicas para el tratamiento seguro de la información
- La Política de Seguridad debe ser aprobada formalmente por la Dirección, y obtener su respaldo
- De la Política de Seguridad emanarán las normativas y procedimientos de seguridad específicos.
- Security Policy Statement:

“The management and all the staff from the OHIM are committed to protect the Availability, Confidentiality and Integrity of the Information managed by its Business and Support Processes. Employees, contractors, and other parties related to the OHIM are required to actively support the management in the enforcement of this Security Policy Statement.”





Valor del Riesgo: probabilidad Muy Alta / impacto Muy Alto

7.6 Degradación del tiempo de respuesta

☒ 205. Sistema 1

5.45 Copia no controlada de documentos

☒ 801. Departamento 1

☒ 810. Departamento 2

2.14 Acceso no autorizado a salas

☒ 112. CPD 1

☒ 116. Sala 2

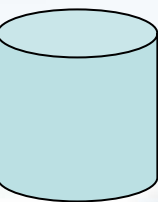
7.8 Fallo de Hardware

☒ 606. Servidor 1

☒ 607. Servidor 2

	V	40	25	15	4
	H	HL			
	M	ML	MM		
	L	LL	LM	LH	
		L	M	H	V

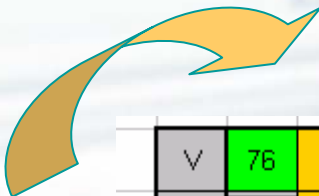
Risk Assessment Database



Total: 414 Detailed Risks

V	VL	VM	VH	VV
H	HL	HM	HH	HV
M	ML	MM	MH	MV
L	LL	LM	LH	LV
	L	M	H	V

Select and Prioritise



V	76			4
H	HL	81	24	
M	ML	MM		
L	LL	LM	LH	
	L	M	H	V

Category 1

Category 2

Category 3

Category 4

Total: 185 Selected and Prioritised Risks

Grouping



V	50	44	19	4
H	HL			
M	ML	MM		
L	LL	LM	LH	
	L	M	H	V

**Total:
117 grouped risks
to focus on**

(DATOS SIMULADOS)

OFFICE FOR HARMONIZATION IN THE INTERNAL MARKET
(TRADE MARKS AND DESIGNS)

Risk Assessment Report

Version: 4

Information Technologies and Facilities Management
Department

CLASSIFICATION

Confidential

APPROVAL

Name:

Date:

**Risk Assessment
Report**

Control	In Place	Policy	Procedure	Technical	Evidence	Compliance
7.1.1 Physical security perimeter	Yes	No	No	No	Yes	Partial
7.1.2 Physical entry controls	Yes	No	No	Yes	Yes	Partial
7.1.3 Securing offices, rooms and facilities	No					Null
7.1.4 Working in secure areas	Yes	Yes	Yes	N/A	Yes	Total
7.1.5 Isolated delivery and loading areas	N/A					Not Applicable
7.2.1 Equipment siting and protection	Yes	Yes	Yes	N/A	Yes	Total
7.2.2 Power supplies	Yes	No	No	Yes	Yes	Partial
7.2.3 Cabling security	Yes	No	No	N/A	Yes	Not Formal
7.2.4 Equipment maintenance	Yes	No	No	N/A	Yes	Not Formal
9.2.3 User password management	Yes	Yes	Yes	Yes	Yes	Total
9.2.4 Review of user access rights	Yes	No	Yes	N/A	No	Null
9.3.1 Password use	Yes	Yes	N/A	N/A	Yes	Total
9.3.2 Unattended user equipment	No					Null
9.4.1 Policy on use of network services	No					Null
9.7.2 Monitoring of system use	Yes	No	No	Yes	Yes	Partial

(DATOS SIMULADOS)

Valor del Riesgo: probabilidad V / impacto V

Riesgo 7.6 Degradación del tiempo de respuesta

Categoría: 1 (VV) Acción a realizar: **Mitigar** Categoría deseada: 3 (MV)

Controles seleccionados para mitigar el riesgo:

10.1.1 Análisis y especificación de requerimientos de seguridad

8.2.1 Capacity planning

8.2.2 Systems acceptance

Riesgo 5.45 Copia no controlada de documentos

Categoría: 1 (VV) Acción a realizar: **Asumir**

Riesgo 2.14 Acceso no autorizado a salas

Categoría: 1 (VV) Acción a realizar: **Mitigar** Categoría deseada: 4 (LV)

Controles seleccionados para mitigar el riesgo:

4.2.1 Identificación de riesgos del acceso de terceras partes

7.1.2 Controles de acceso físicos

- Agrupar controles a implantar en proyectos.
- Estimación de presupuesto planificado de proyectos
- Elaboración de la planificación de proyectos. Debe ser una planificación realista, pues su cumplimiento será auditado por BSI.

Proyecto 1 - Comunicación y Concienciación de usuarios

Duración: 3 semanas **Fecha Inicio:** 23/02/2004 **Inversión:** XX.XXX €

Prioridad: Corto plazo

Objetivo: Concienciar al personal acerca las políticas y procedimientos generales de seguridad.

Proyecto 2 - Mejora de los controles de acceso físico al CPD 1

Duración: 2 meses **Fecha Inicio:** 23/06/2005 **Inversión:** XX.XXX €

Prioridad: Medio plazo

Objetivo: Mejorar el control de acceso existente en el CPD 1 para garantizar que únicamente acceden usuarios autorizados.

Proyecto 3 - Nota legal del correo saliente

Duración: 1 día **Fecha Inicio:** 04/02/2004 **Inversión:** 0 €

Prioridad: Quick Win

Objetivo: Mostrar un aviso en el correo saliente indicando que es confidencial y que pertenece a la compañía.

- Es el documento en el que se identifican los controles ISO17799 que serán implantados, así como los controles que la entidad decida no implantar, junto con su justificación.
- El statement of applicability debe ser aprobado formalmente por la Dirección

- En base al Plan de Tratamiento del riesgo realizado, y a los controles a implantar aprobados por la dirección, se deben ir implantando las medidas seleccionadas.
- Revisar los resultados de los controles implantados.
- Determinar el nuevo nivel de riesgo.
- Comunicar los resultados obtenidos, validando que se alcanzan los resultados esperados.



Deloitte.