

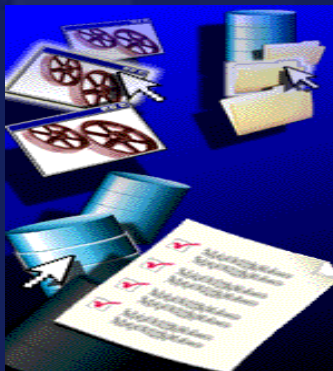
BS ISO/IEC 27001:2005 – SGSI SISTEMAS DE GESTION DE LA SEGURIDAD DE LA INFORMACION

Junio de 2008

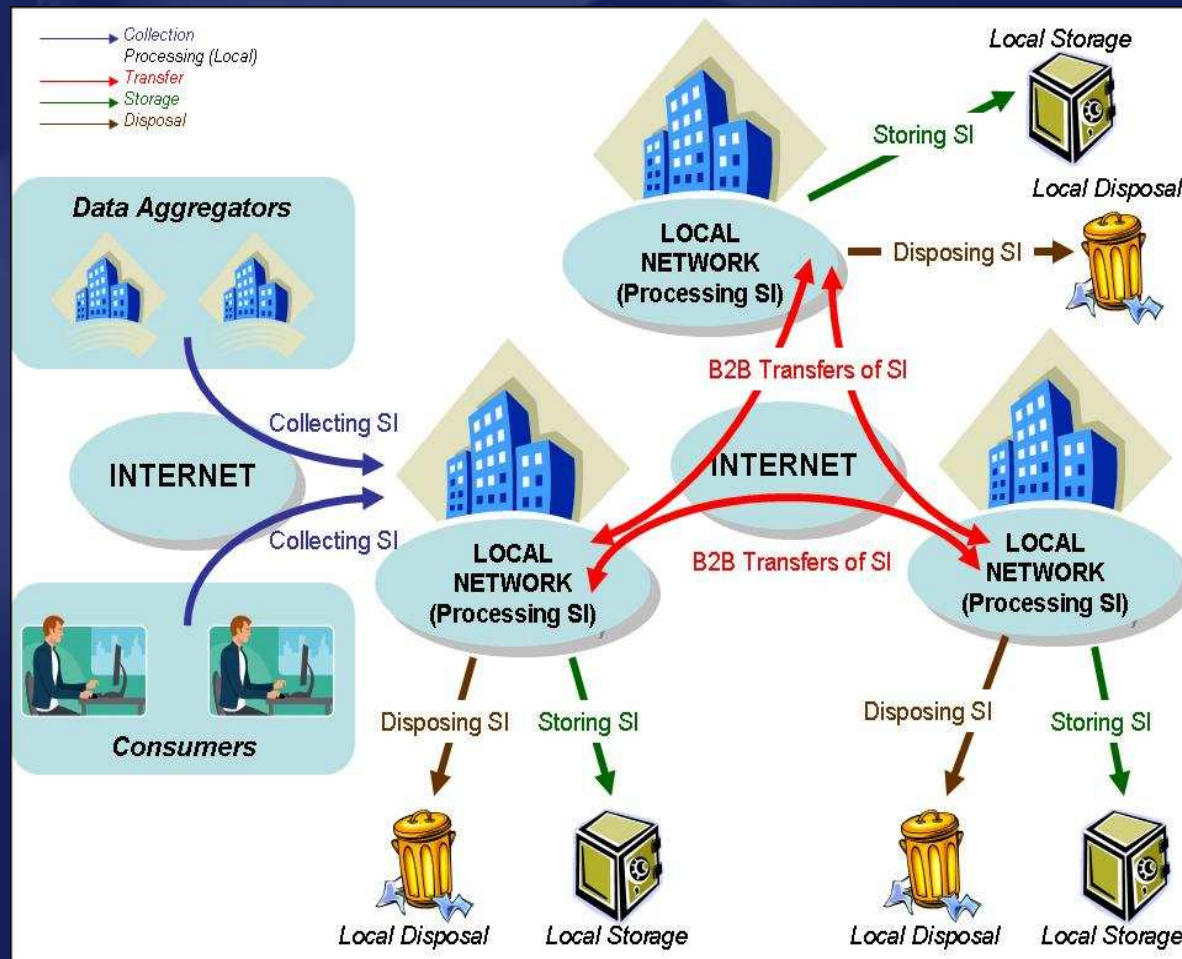
Falta de Seguridad de la Información

- ✓ Compartir passwords
- ✓ Acceso a sitios no autorizados
- ✓ Uso indebido de equipo de cómputo
- ✓ Equipos desatendidos
- ✓ Documentos perdidos
- ✓ Robo
- ✓ Bases de datos destruídas
- ✓ Mantenimiento no controlado
- ✓ Backups / Restores inservibles
- ✓ Redes de comunicación caídas
- ✓ Aplicaciones mal diseñadas
- ✓ Cambios no planeados/autorizados
- ✓ Destrucción/disposición inadecuadas
- ✓ USB's sin control
- ✓ Separación de funciones
- ✓ Infraestructura del centro de cómputo
- ✓ Expuestos a amenazas
- ✓ Personal no controlado
- ✓ Terceros / outsourcing sin control
- ✓ Viabilidad del negocio
- ✓ Incumplimiento de requerimientos legales/contractuales

Tipos de información



Ciclo de la información



- Genera-Captura
- Procesamiento
- Transferencia
- Almacenamiento
- Disposición

Importancia de la información

- *Activo vital en una organización.*
- *Me da una ventaja competitiva*
- *Permite mantener la operatividad de la empresa*
- *Asociada al flujo de efectivo y rentabilidad de la empresa*
- *Permite cumplir requerimientos legales y contractuales*
- *Me permite proyectar una imagen pública y comercial*



Ventajas de la gestión de la seguridad de la información

- *Organizacional*
- *Legal*
- *Operativa*
- *Comercial*
- *Financiera*
- *Recursos Humanos*



”Seguridad de la Información”

Es la preservación de la:

Confidencialidad

Acceden quienes están autorizados



Integridad

Es precisa, confiable y completa

Disponibilidad

Está disponible cuando se necesita

Gestión del Riesgo



Evaluación del Riesgo

Amenazas:

Terrorismo
Manifestaciones
Terremoto
Fuego
Inundación
Falla de HW/SW
Robo
Acceso no autorizado
Errores
Fraude
Huracán
Uso ilegal del SW
Falla de energía
Fuga de información
Errores Humanos
Cambios fallidos
Responsabilidad legal o contractual
Falla de la red



Activos

Información
Procesos
Servicios
Software
Hardware
Infraestructura
Personal
Imagen, etc.

Evaluación del Riesgo

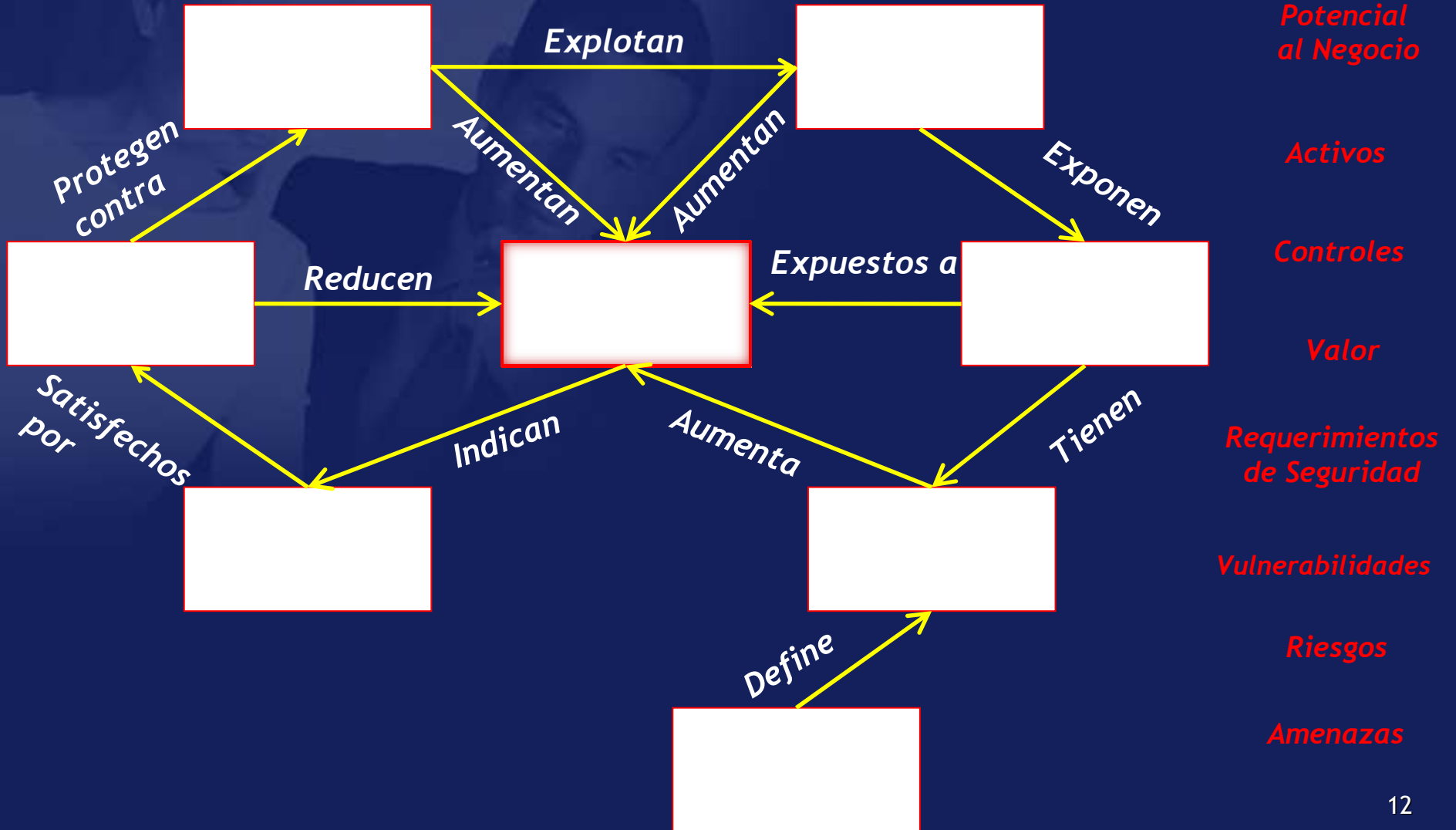
Vulnerabilidades

- Falta de entrenamiento
- Personal molesto
- Falta de protección física
- Falta de mantenimiento
- Ubicación inadecuada de instalaciones
- Aplicaciones complicadas
- Falta de control de cambios
- Inadecuada separación de funciones
- Puertos de servicio no controlados
- Pruebas inadecuadas a las aplicaciones
- Falta de control de los datos de prueba
- Falta de monitoreo
- Falta de políticas
- Falta de procedimientos
- Falta de un plan de continuidad
- Falta de supervisión de proveedores

Evaluación del Riesgo




Ejercicio



Ventajas de utilizar ISO27001



- Provee mejores prácticas
 - Permite implementar en una forma eficaz, completa y ordenada
 - Genera confianza entre organizaciones
 - Establece la mejora continua
 - Es certificable
- 
- A photograph showing two hands, one from a person in a white shirt and one from a person in a blue shirt, shaking over a document. The background is a blurred industrial or office setting.
- Aplicable a cualquier tipo de organización, sin importar: tipo, tamaño, y riesgos asociados
 - Aplicable a cualquier tipo de información
 - Compatible con otros estándares
 - Establece requisitos mínimos

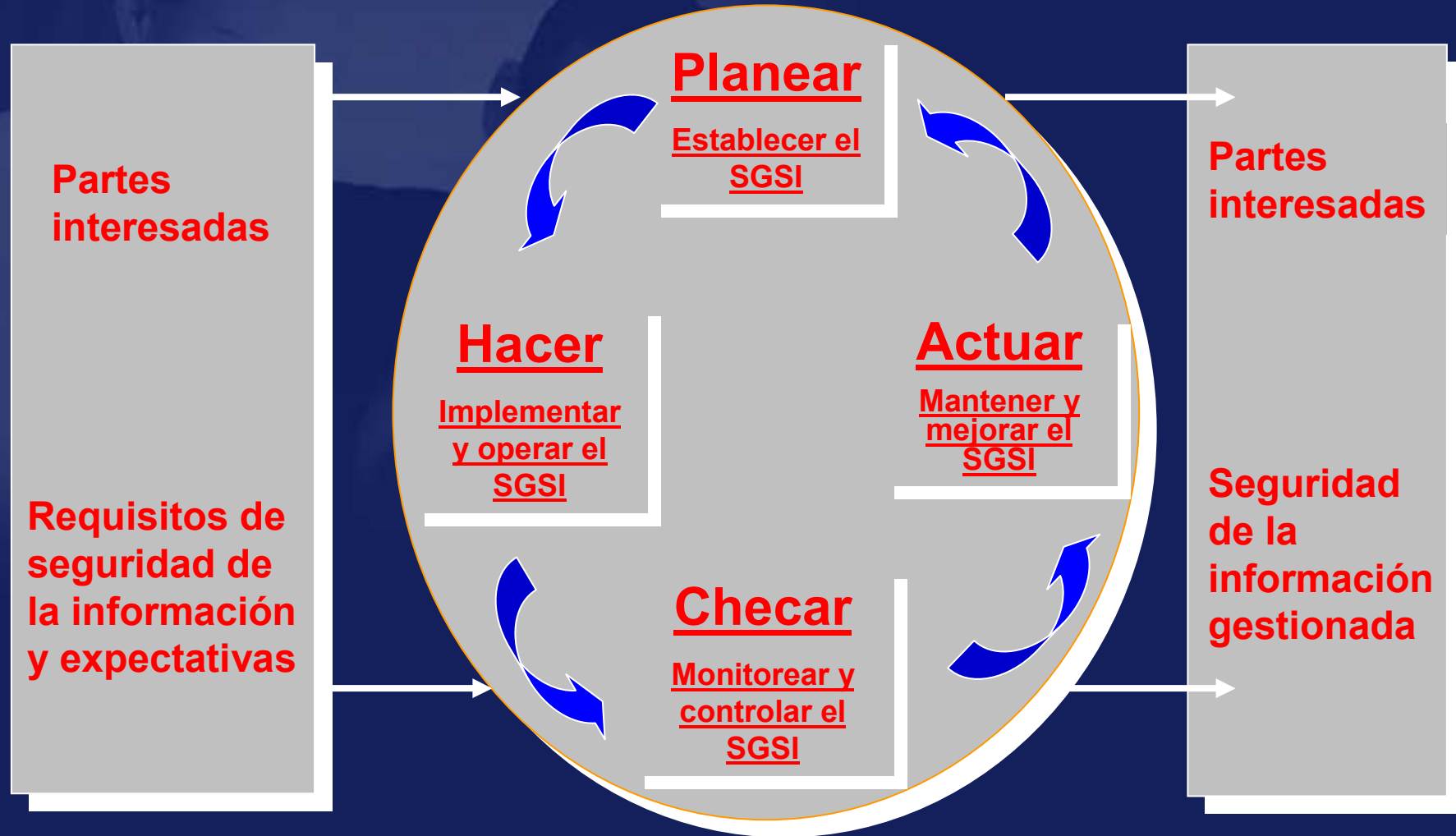
ISO27001: Historia

- 1990 – El Departamento de comercio e industria del Reino Unido apoyó su desarrollo
- 1995 – Por primera vez se adopta como norma inglesa (BSI)
- 1998 – Se lanzan los requisitos para su certificación
- 1999 – Se emite una segunda edición de la norma
- 2000 – Fue aprobada como la parte 1 de ISO17799
- 2002 – BS7799-2 se publicó el 5 de septiembre: en esta revisión se adoptó el “modelo de proceso” con el fin de alinearla con ISO9001 e ISO14001
- 2004 – A finales del 2004, cerca de 950 compañías se habían certificado en BS 7799-2
- 2005 – Se publica ISO/IEC17799:2005 en Junio y la ISO27001:2005 en Octubre.
- 2007 – Se publica ISO27002:2005 (se renombra ISO/IEC17799:2005)
- 2007 – Se publica ISO27006:2007, requisitos para org. certificadores

ISO27001: Futuro

- ISO27000 - Términos y Definiciones
- ISO27001 - Requisitos (Certificable) (BS7799-2)
- ISO27002 - Código de Práctica (ISO/IEC 17799:2005 BS7799-1:2005)
- ISO27003 - Guía de Implementación
- ISO27004 - Métricas y Mediciones
- ISO27005 - Guía para la Gestión de Riesgos de Seguridad de la Información (BS7799-3:2006)Guía de Implementación
- ISO27006 - Requisitos para los organismos que certifican y registran un SGSI (ISO27001).
- ISO27007 - Guía de Auditoría para un SGSI (ISO19011)
- ISO27008 - Guía para la Gestión de la Continuidad del Negocio (BS25999-1:2006 Business Continuity Guide)
- ISO27009 - Telecomunicaciones
- ISO27010 - Industria Automotriz

Ciclo de Mejora Continua



Establecer el SGSI:

1. Definir el alcance del SGSI
2. Definir una política para el SGSI
3. Definir la metodología de evaluación de riesgos
4. Criterio de aceptación de riesgos
5. Identificar los riesgos
6. Analizar y evaluar los riesgos
7. Identificar y evaluar opciones para el tratamiento de los riesgos
8. Seleccionar objetivos de control y controles
9. Obtener aprobación gerencial de los riesgos residuales
10. Obtener aprobación gerencial del SGSI
11. Preparar el Documento de Aplicabilidad (SOA vs Anexo A)

Implementar y operar el SGSI.

1. Formular el Plan de Tratamiento de Riesgos
2. Implementar el Plan de Tratamiento de Riesgos
3. Implementar los controles seleccionados
4. Definir como medir la eficacia de los controles
5. Implementar un plan de entrenamiento y sensibilización
6. Gestionar las operaciones del SGSI
7. Gestionar los recursos SGSI
8. Implementar procedimientos para detectar/responder a eventos e incidentes de seguridad

Monitorear y Revisar el SGSI

1. Ejecutar procedimientos de monitoreo y revisión
2. Efectuar revisiones regulares de la eficacia del SGSI
3. Medir la eficacia de los controles
4. Revisar, de acuerdo a un plan, la evaluación de riesgos, el nivel de riesgos residuales y aceptables, considerando los cambios en el ambiente.
5. Conducir auditorías internas del SGSI de acuerdo a un plan
6. Revisión periódica por la dirección
7. Actualizar planes de seguridad en función de las actividades de monitoreo y revisión
8. Registrar acciones y eventos que afecten la eficacia del SGSI.

Actuar

Mantener y Mejorar el SGSI.

1. Implementar las mejoras identificadas
2. Tomar acciones preventivas/correctivas. Aplicar lecciones aprendidas
3. Comunicar los resultados a las partes interesadas
4. Asegurar que las mejoras logran los objetivos esperados.

ISO27001:2005 Estructura

0. Introducción
1. Alcance
2. Normas de referencia
3. Términos y definiciones
4. Sistema de Gestión de Seguridad de la Información
5. Responsabilidad de la Dirección
6. Auditorías Internas del SGSI
7. Revisión Gerencial del SGSI
8. Mejora del SGSI

Anexo A. Objetivos de Control y Controles

11 Cláusulas, 39 objetivos de control y 133 controles

Anexo B. Principios de la OCDE y este estándar internacional

Anexo C. Correspondencia entre ISO9001:2000, ISO14001:2004 y este estándar internacional

Documentación SGSI

1. Política y objetivos del SGSI
2. Alcance del SGSI
3. Procedimientos y controles en soporte al SGSI
4. Descripción de la metodología de Evaluación de Riesgos
5. Reporte de la Evaluación de Riesgos
6. Plan de Tratamiento de Riesgos
7. Procedimientos documentados de la organización para la efectiva planeación, operación y control de los procesos de seguridad de la información y de la forma de medir la eficacia de los controles.
8. Registros requeridos por el estándar
9. Documento de aplicabilidad (SOA)

Documentación SGSI

Procedimientos documentados requeridos:

1. Control de Documentos
2. Control de Registros (recomendado)
3. Auditorías Internas
4. Acciones Correctivas
5. Acciones Preventivas

BS ISO/IEC 27001: 2005

Anexo A: Objetivos de Control y Controles

Junio de 2008

Objetivos de Control y Controles

