



## Controles Generales

Barcelona, 16 de febrero de 2006



18:30 – 21:30

2 sesiones con descanso

### Aspectos generales de la Auditoría de seguridad

- Introducción a la Auditoría Informática
- Metodología

→ **Enfoques CISA  
y COBIT**

### Algunos trabajos

- Auditoría de Seguridad informática
  - Plataforma Internet
  - Seguridad física
  - Aplicaciones Web
- Auditoría de los requerimientos de seguridad estándares en el tratamiento de los PIN
- Auditoría del Reglamento de Medidas de Seguridad de la LOPD
- Sistema de alarmas automatizado

**Requerimientos  
y normativa  
externa**

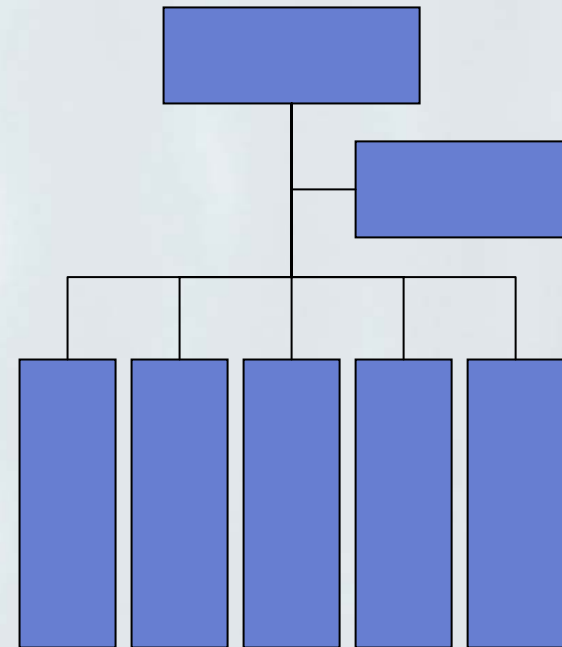
# Revisión de controles generales basada en el COBIT

### Objetivo / Alcance

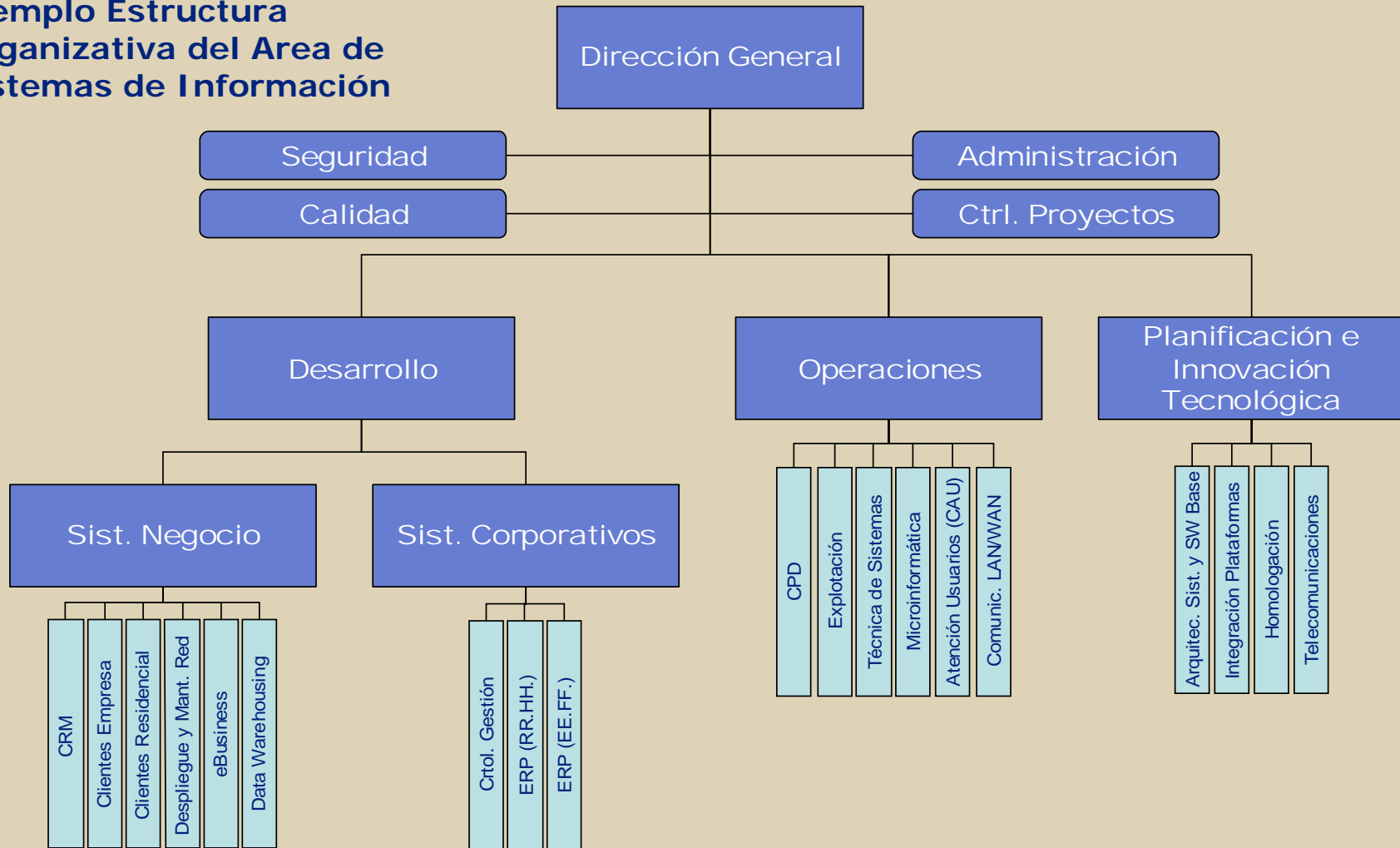
Verificar y evaluar el ambiente general de control imperante en el Área de Sistemas de la Compañía, con el propósito de efectuar un diagnóstico de las principales debilidades de control existentes y sus riesgos asociados.

Esta revisión alcanza las actividades realizadas por el Área de Sistemas en la administración y gestión del departamento e incluye:

- Estrategia y planificación de las fuentes de información
- Operaciones de los sistemas de información
- Relaciones con los proveedores de Outsourcing
- Seguridad de la información
- Planificación continuada del negocio
- Implantación y mantenimiento de los sistemas de la aplicación
- Implantación y soporte de las bases de datos
- Soporte de la red
- Soporte del software
- Soporte del hardware



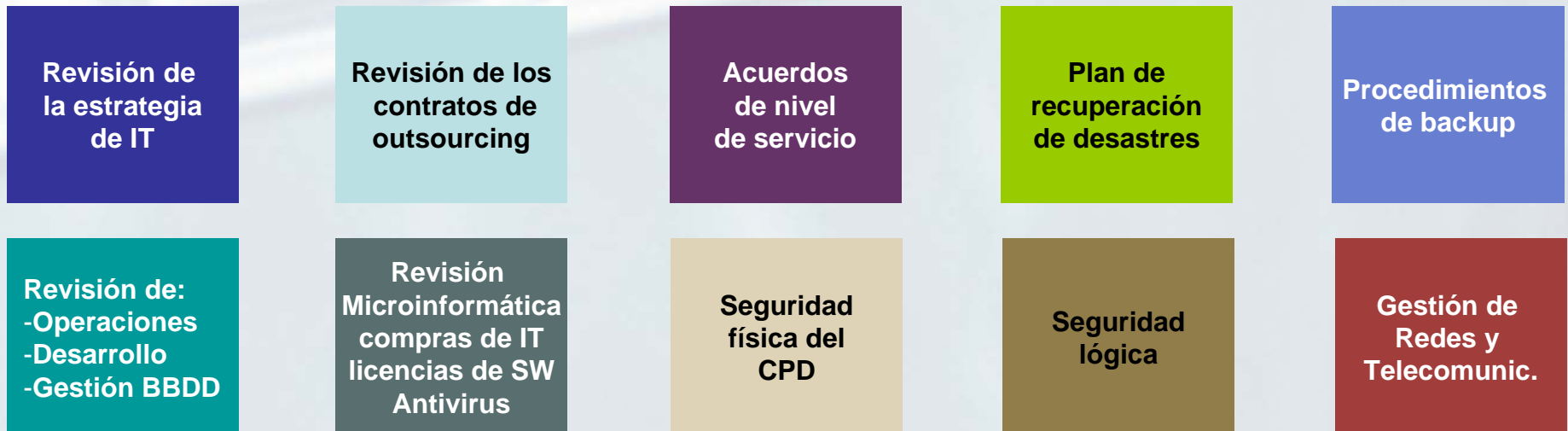
## Ejemplo Estructura Organizativa del Area de Sistemas de Información



### Enfoque metodológico



### Temas que se incluyen en la revisión





- CISA
- **Certification in Information Systems Auditing**
  - ISACA (**Information Systems Audit and Control Association**):
    - Más de 28.000 asociados.
    - Capítulos en más de 60 países.
    - Proporciona certificados como el CISA, CISM, etc.
- Dominios CISA:
  - El proceso de Auditoría de Sistemas de Información.
  - Gerencia, Planificación y Organización de SI.
  - Infraestructura Técnica y Prácticas Operacionales.
  - Protección de Activos de Información.
  - Recuperación ante Desastres y Continuidad de Operación.
  - Desarrollo, Adquisición y Mantenimiento de los Sistemas de Información.
  - Evaluación de Procesos Empresariales y Gerencia de Riesgos.

- **CoBIT**
- **Control Objectives for Information Technology**
- Proporciona un **Marco de referencia** que puede adoptarse para realizar el diagnóstico de auditoría informática.
- **Estándar generalmente aplicable y aceptado** en las revisiones de seguridad y control de Tecnología de Información.
  - Proporciona “**mejores prácticas**” a través de un marco referencial de dominios y procesos.
  - Diseñado para ser un “**check-list**” de **verificación** detallada de cada proceso de Sistemas de Información.



- **CISA vs COBIT**

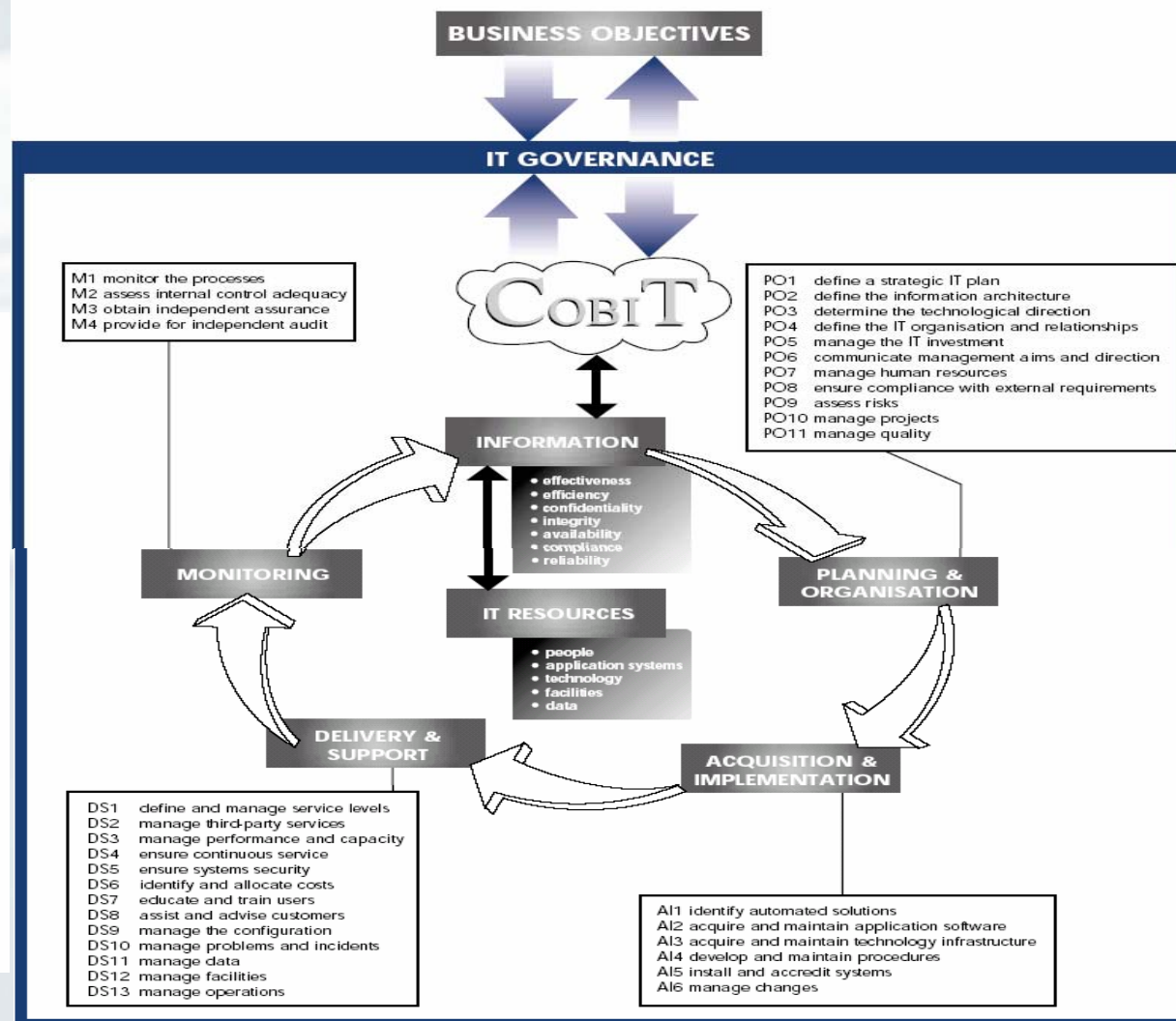
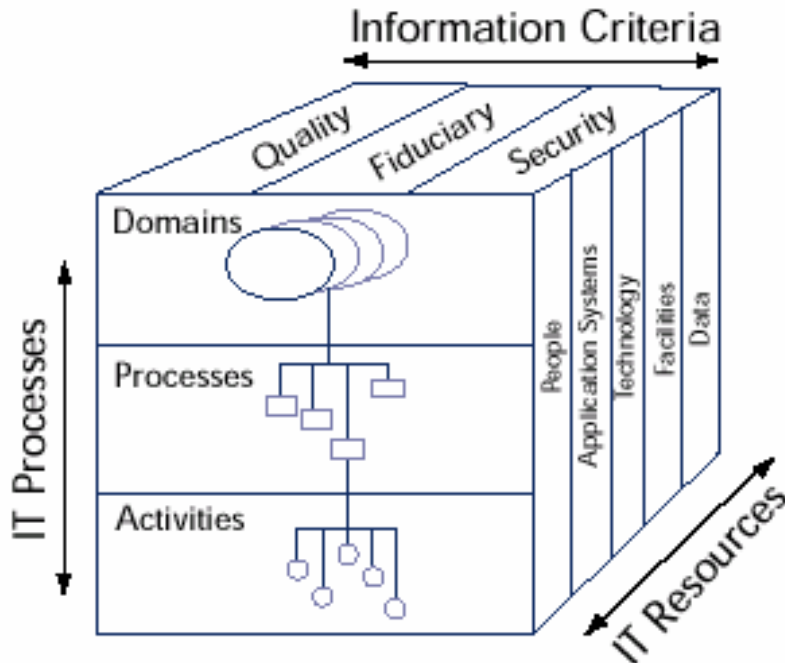
- **CISA:**

- Establece las **directrices de las auditorías de IS** de manera que se encuentren alineadas con los estándares de auditoría generalmente aceptados y define las bases para asegurar que las TIC de las organizaciones son controladas, monitorizadas y valoradas de manera adecuadas.

- **CoBIT:**

- Proporciona un **Marco de referencia** que puede adoptarse para realizar el diagnóstico de auditoría informática.
- El CISA se basa en los objetivos de control y actividades de control referenciados en el CoBIT.

- Procesos de IT basados en
- cuatro dominios según CoBIT:



## Según CoBIT (Procesos según Dominio)

		Information Criteria							IT Resources				
		effectiveness	efficiency	confidentiality	integrity	availability	compliance	reliability	people	applications	technology	facilities	data
DOMAIN	PROCESS												
Planning & Organisation	PO1 Define a strategic IT plan	P	S						✓	✓	✓	✓	✓
	PO2 Define the information architecture	P	S	S	S					✓			✓
	PO3 Determine technological direction	P	S								✓	✓	
	PO4 Define the IT organisation and relationships	P	S						✓				
	PO5 Manage the IT investment	P	P					S	✓	✓	✓	✓	
	PO6 Communicate management aims and direction	P					S		✓				
	PO7 Manage human resources	P	P						✓				
	PO8 Ensure compliance with external requirements	P					P	S	✓	✓			✓
	PO9 Assess risks	P	S	P	P	P	S	S	✓	✓	✓	✓	✓
	PO10 Manage projects	P	P						✓	✓	✓	✓	
	PO11 Manage quality	P	P		P			S	✓	✓	✓	✓	
Acquisition & Implementation	AI1 Identify automated solutions	P	S							✓	✓	✓	
	AI2 Acquire and maintain application software	P	P		S		S	S		✓			
	AI3 Acquire and maintain technology infrastructure	P	P		S						✓		
	AI4 Develop and maintain procedures	P	P		S		S	S	✓	✓	✓	✓	
	AI5 Install and accredit systems	P			S	S			✓	✓	✓	✓	✓
	AI6 Manage changes	P	P		P	P		S	✓	✓	✓	✓	✓

## Según CoBIT (Procesos según Dominio)

### DOMAIN

#### Delivery & Support

DS1  
DS2  
DS3  
DS4  
DS5  
DS6  
DS7  
DS8  
DS9  
DS10  
DS11  
DS12  
DS13

### PROCESS

Define and manage service levels  
Manage third-party services  
Manage performance and capacity  
Ensure continuous service  
Ensure systems security  
Identify and allocate costs  
Educate and train users  
Assist and advise customers  
Manage the configuration  
Manage problems and incidents  
Manage data  
Manage facilities  
Manage operations

#### Monitoring

M1  
M2  
M3  
M4

Monitor the processes  
Assess internal control adequacy  
Obtain independent assurance  
Provide for independent audit

### Information Criteria

effectiveness  
efficiency  
confidentiality  
integrity  
availability  
compliance  
reliability

### IT Resources

people  
applications  
technology  
facilities  
data

P	P	S	S	S	S	S	✓	✓	✓	✓	✓
P	P	S	S	S	S	S	✓	✓	✓	✓	✓
P	P			S				✓	✓	✓	
P	S			P			✓	✓	✓	✓	✓
		P	P	S	S	S	✓	✓	✓	✓	✓
	P					P	✓	✓	✓	✓	✓
P	S						✓				
P	P						✓	✓			
P				S		S		✓	✓	✓	
P	P			S			✓	✓	✓	✓	✓
			P			P					✓
			P	P						✓	
P	P		S	S			✓	✓		✓	✓
P	P	S	S	S	S	S	✓	✓	✓	✓	✓
P	P	S	S	S	P	S	✓	✓	✓	✓	✓
P	P	S	S	S	P	S	✓	✓	✓	✓	✓
P	P	S	S	S	P	S	✓	✓	✓	✓	✓

Los procesos operativos del área de sistemas de información que se analizan se corresponden con los definidos en el COBIT

### 4 DOMINIOS COBIT

### 34 OBJETIVOS DE CONTROL

#### Estrategia y Organización:

- ✓ Plan de sistemas
- ✓ Arquitectura técnica
- ✓ Dirección tecnológica
- ✓ Organización IT
- ✓ Inversiones IT
- ✓ Comunicación Estrategia
- ✓ Recursos Humanos
- ✓ Cumplimiento requerimientos externos
- ✓ Análisis de riesgos
- ✓ Gestión proyectos
- ✓ Calidad

#### Entrega y Soporte:

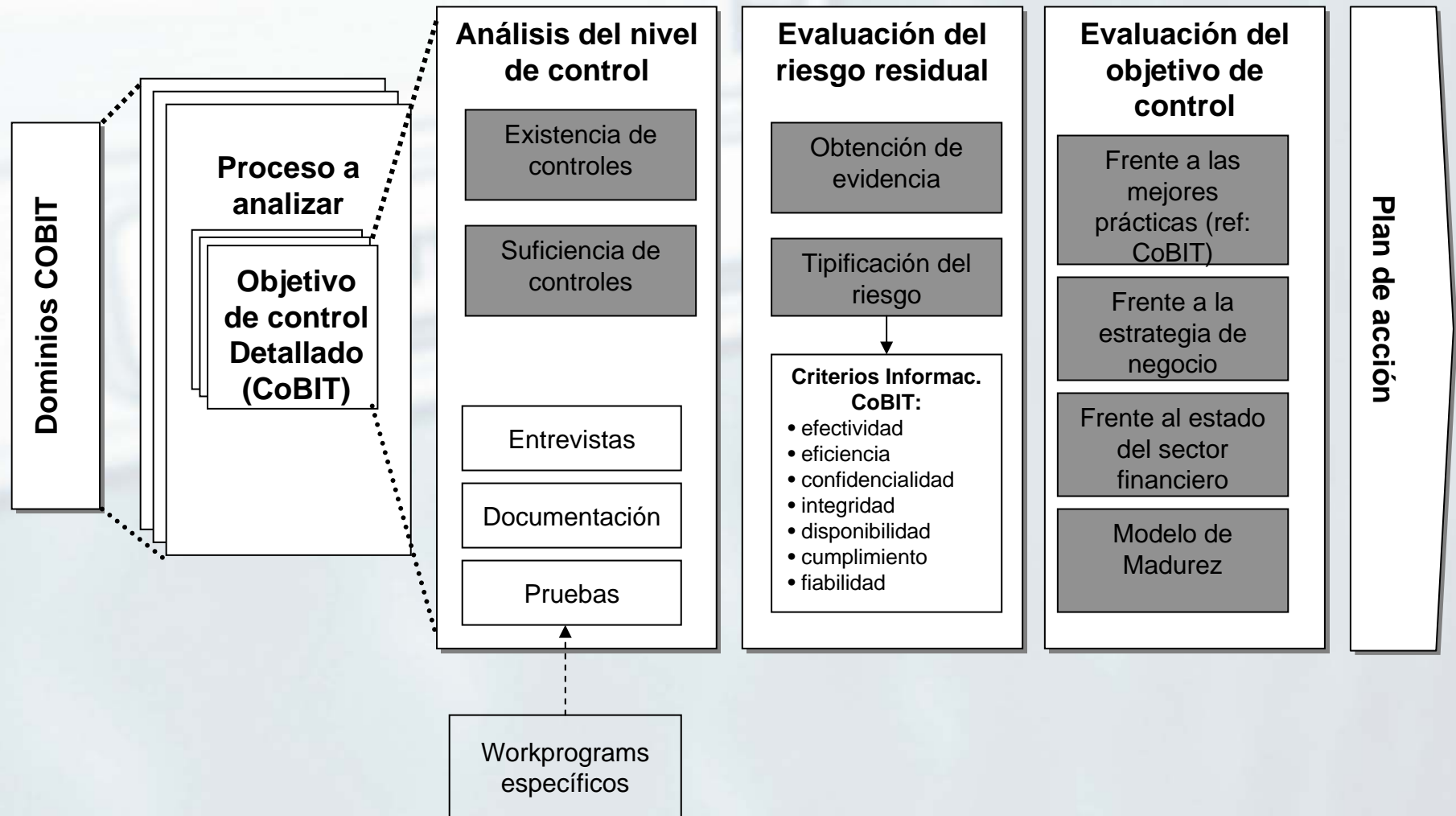
- ✓ Niveles de Servicio
- ✓ Servicios de terceros
- ✓ Rendimiento y capacidad
- ✓ Continuidad del servicio
- ✓ Seguridad
- ✓ Análisis de costes
- ✓ Formación usuarios
- ✓ Información y soporte a usuarios
- ✓ Gestión configuración
- ✓ Gestión incidencias
- ✓ Gestión de datos
- ✓ Gestión instalaciones
- ✓ Operaciones

#### Adquisición e implantación:

- ✓ Identificación de soluciones
- ✓ Adquisición y mantenim. de software
- ✓ Adquisición y mantenim. infraestructura
- ✓ Desarrollo y mantenim. procedimientos
- ✓ Instalación / acreditación de sistemas
- ✓ Gestión de cambios

#### Monitorización:

- ✓ Monitorización procesos
- ✓ Razonabilidad control interno
- ✓ Garantía de independencia
- ✓ Auditoría independiente

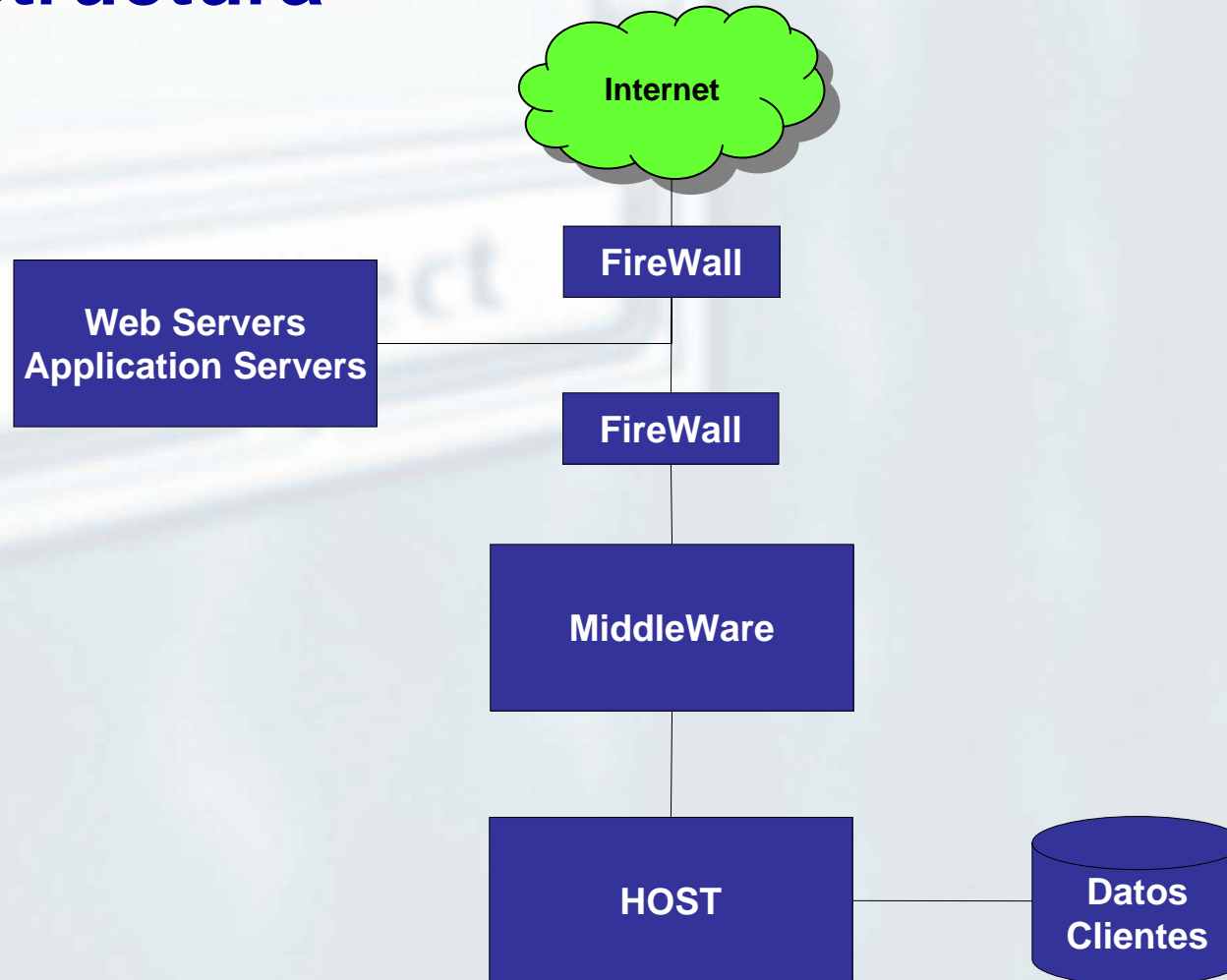




## Objetivo

- Obtener un diagnóstico del estado actual del control interno de la infraestructura de servicios a través de Internet, basándolo en un referente en la auditoría de sistemas, como es el CobiT (Control Objectives for Information and Related Technology).
- Elaborar un Plan de Acción donde se recopilen todas nuestras recomendaciones para subsanar las debilidades detectadas o mejorar otros aspectos que sean susceptibles de mejora.
- No se trata de:
  - realizar pruebas o intentos de levantamiento de los controles de identificación en el acceso.
  - realizar pruebas de intrusión a los entornos de Internet.

- **Infraestructura**



- Áreas de Sistemas a Revisar:
  - Dirección Sistemas de Información.
    - Dirección y Gestión.
    - Desarrollo y mantenimiento.
    - Producción.
    - Seguridad.
    - Técnica de Sistemas.
  - Dirección Comercial Internet.
    - Gestión de Contenidos.

- Detección de riesgos:
  - Dirección Sistemas de Información.
    - Dirección y Gestión.
    - Desarrollo y mantenimiento.
    - Producción.
    - Seguridad.
    - Técnica de Sistemas.
  - Dirección Comercial Internet.
    - Gestión de Contenidos.

## • Plan de trabajo

### Dirección y Gestión

DOMINIO COBIT	PROCESO COBIT	Objetivo de control	Prueba a realizar
PLANIFICACIÓN Y ORGANIZACIÓN	DIRECCIÓN TECNOLÓGICA	Monitorización de tendencias y regulaciones futuras	Verificar que la Dirección evalúa tecnologías de vanguardia, e incorpora las tecnologías apropiadas a la infraestructura.
		Estándares de tecnología	Comprobar la existencia de un estándar tecnológico para la infraestructura de servicios Internet.
	ORGANIZACIÓN DE IT Y RELACIONES	Segregación de funciones	Evaluar el grado de segregación de funciones dentro del área de IT en lo que concierne a la planificación, desarrollo y explotación de las plataformas de Internet.
	DIRECCIÓN Y GESTIÓN DE PROYECTOS	Participación del usuario	Evaluar el grado de participación de las áreas usuarias y de las áreas técnicas en la definición de los requerimientos de los nuevos desarrollos, y en la determinación de éstos.

### Dirección Comercial Internet

DOMINIO COBIT	PROCESO COBIT	Objetivo de control	Prueba a realizar
ADQUISICIÓN E IMPLEMENTACIÓN	INSTALACIÓN Y ACREDITACIÓN DE SISTEMAS	Paso a Producción	Verificar la existencia de un sistema que provea un workflow automatizado para el control de autorizaciones de los contenidos publicados en las plataformas de Internet. Averiguar si cada publicación ha de ir aprobada por un responsable.
			Validar si se han de autorizar los contenidos facilitados por proveedores de información externos.
	GESTIÓN DE CAMBIOS	Control de cambios	Verificar si se ha implantado un sistema de verificación y monitorización de la autenticidad e integridad de los contenidos publicados en los servidores públicos.

- Plan de trabajo

## Desarrollo y Mantenimiento

DOMINIO COBIT	PROCESO COBIT	Objetivo de control	Prueba a realizar
PLANIFICACIÓN Y ORGANIZACIÓN	CALIDAD	Metodología del Ciclo de Vida de Desarrollo de Sistemas	Determinar si existe una metodología aplicable para el desarrollo de servicios Internet. Verificar que existen aprobaciones formales de los usuarios en las distintas etapas del ciclo de vida. Este punto se debe verificar para los mantenimientos y proyectos. Comprobar si se han establecido un manual de mejores prácticas para el desarrollo seguro de aplicaciones web
		Revisión del Aseguramiento de Calidad sobre el Cumplimiento de Estándares y	Verificar si se aplica el QA sobre los proyectos y mantenimientos de desarrollos de servicios Internet
ENTREGA Y SOPORTE	SEGURIDAD	Procedimientos de la Función de Servicios de Información	Determinar si la documentación de sistemas se restringe exclusivamente al personal que lo requiera para el desempeño de sus funciones



## • Plan de trabajo

ADQUISICIÓN E IMPLEMENTACIÓN	ADQUISICIÓN Y MANTENIMIENTO DE SOFTWARE	Metodología de pruebas	Verificar que la metodología define estándares de pruebas unitarias (por módulos funcionales) y de integración.
			Verificar la inclusión del test final de aceptación en la metodología. Verificar la participación de los usuarios en la preparación de juegos de datos, incluyendo operaciones y datos válidos y no válidos.
			Verificar si se realizan pruebas de simulación de volúmenes de carga de datos, tiempos de proceso, disponibilidad, etc., con el objetivo de planificar los recursos que serán necesarios para garantizar la operatividad del nuevo sistema / aplicación.
	IDENTIFICACIÓN DE SOLUCIONES	Definición formal de requerimientos	Verificar el canal por el que se reciben las solicitudes y analizar el circuito de aceptaciones para los desarrollos seleccionados.
			Verificar que los requerimientos se documentan formalmente
		Participación del usuario	Determinar y validar, mediante entrevistas, el origen del impulso inicial para las modificaciones y los nuevos desarrollos.
			Verificar la involucración de seguridad en los desarrollos y mantenimientos: la metodología establece la necesidad de la intervención de Seguridad, comprobar su intervención en actas de reunión, etc.
		Amenazas a la seguridad e impactos potenciales	Verificar que el análisis de requerimientos y el diseño funcional incluye la definición de controles para mitigar los riesgos potenciales identificados y que se incluyen pistas de auditoría, en un proyecto.
	INSTALACIÓN Y ACREDITACIÓN DE SISTEMAS	Entornos de desarrollo, pruebas y producción	Determinar el control que existe en el pase a mantenimiento de los objetos
			Verificar si el pase a mantenimiento de objetos se realiza mediante una herramienta que permita bloquear el objeto e impedir que se realicen mantenimientos paralelos.
			Determinar si existe una herramienta que controle los cambios de versiones y si se mantienen todas las versiones
			Verificar si se bloquean los códigos fuente y ejecutables en el momento que se solicita el pase a producción
			Verificar que las compilaciones se realizan en un punto intermedio, no en los discos duros de los desarrolladores.
			Validar si el personal de desarrollo accede al entorno de producción
			Validar si en desarrollo se hacen pruebas con datos reales

## • Plan de trabajo

### Producción

DOMINIO COBIT	PROCESO COBIT	Objetivo de control	Prueba a realizar
ENTREGA Y SOPORTE	GESTIÓN DE INCIDENCIAS	Procedimientos para la gestión de incidencias	Verificar que existe un procedimiento para la gestión de incidencias que asegure que todos los eventos que no forman parte de las operaciones estándar de los sistemas de las plataformas Internet son registrados, analizados y resueltos de manera oportuna.
			Verificar que se aplica el procedimiento de gestión de incidencias, revisando el tratamiento que se le ha dado a una muestra de estas
			Verificar que las incidencias se registran y reportan a los correspondientes responsables
			Para el caso de datos personales, verificar que está en marcha un procedimiento para la gestión de incidencias que pueda afectar a datos de carácter personal, y que está habilitado un registro para éstas.
	OPERACIONES	Planificación de trabajos	Determinar si se mantiene actualizada la documentación sobre la planificación de los trabajos.
			Determinar si se realiza un seguimiento efectivo de las planificaciones y si se registran las incidencias.
			Verificar la existencia de manuales de operación para los sistemas Internet

## • Plan de trabajo

### Producción

DOMINIO COBIT	PROCESO COBIT	Objetivo de control	Prueba a realizar
ADQUISICIÓN E IMPLEMENTACIÓN	INSTALACIÓN Y ACREDITACIÓN DE SISTEMAS	Paso a producción	Comprobar si existe una herramienta que facilite el control de los traspasos entre entornos, el workflow de autorizaciones, el control de versiones de objetos en los distintos entornos, el bloqueo de objetos,.. (e-changeman) y que todos los pases a producción se realizan mediante ésta.
			Analizar el control de autorizaciones que regula los pases a producción. Verificar que se produce la aprobación de todas las partes afectadas en todos los casos.
			Identificar el personal capacitado para realizar traspasos entre entornos
			Identificar los mecanismos empleados para controlar los traspasos entre entornos: automatización y registro del traspaso, bloqueo de objetos, control de versiones en cada entorno, definición de procedimientos de vuelta atrás, ..
			Comprobar la existencia de mecanismos orientados a asegurar la integridad entre el código fuente y el ejecutable cuando son trasladados entre entornos.
	GESTIÓN DE CAMBIOS	Control de cambios	Verificar el modo en que los programas se encuentran protegidos en el entorno de explotación.

## • Plan de trabajo

### Seguridad

DOMINIO COBIT	PROCESO COBIT	Objetivo de control	Prueba a realizar
ENTREGA Y SOPORTE	ADMINISTRACIÓN DE DATOS	Protección de mensajes sensibles	<ul style="list-style-type: none"> <li>- Verificar que se han implementado mecanismos para verificar la integridad, confidencialidad, autenticidad y el no repudio de las transacciones electrónicas:</li> <li>- mecanismos de autenticación fuerte: PIN + certificados digitales nominativos en navegador o smartcard,</li> <li>- procedimientos de autenticación seguros entre ambas partes de la transacción (certificados en servidor o en cliente y servidor)</li> <li>- mecanismos de cifrado y firma digital</li> <li>- utilización de tarjeta de barcos o claves de operación</li> <li>- ...</li> </ul> <p>Validar que los mecanismos empleados para proteger la confidencialidad de las transacciones electrónicas cumplen adecuadamente con los requerimientos exigibles</p>
	GESTIÓN DE LA CONFIGURACIÓN	Procedimientos de gestión de la configuración	Determinar si se han definido directrices de configuración segura para los sistemas de Internet.

- Plan de trabajo

DOMINIO COBIT	PROCESO COBIT	Objetivo de control	Prueba a realizar
ENTREGA Y SOPORTE	GESTIÓN DE INCIDENTES	Procedimientos para la gestión de incidencias	Verificar que se han formalizado los procesos de notificación, registro, clasificación, priorización, tratamiento, seguimiento y publicación de incidentes de seguridad que supongan la materialización de amenazas externas o sobre los sistemas expuestos, con el fin de detectar problemas repetitivos y buscar medidas para solventarlos
			Determinar si se ejecutan análisis de los incidentes de seguridad ocurridos en los sistemas Internet o provocados por ataques externos, evaluando parámetros tales como: tipo de incidencias más reportadas, sistemas más afectados, tiempo de inactividad de usuarios, tiempo medio de respuesta, acciones correctoras más comunes, dpto. que más informa, costes..., con el fin de detectar problemas repetitivos y buscar medidas para solventarlos.
			Comprobar si se ha implantado sistemas de detección de intrusiones a nivel de aplicativo.
		Autorizaciones temporales para emergencias	Analizar tratamiento de los accesos de emergencia con perfiles potentes. Verificar que se registran y se supervisan. Se notifica también en el Registro de Incidencias.



## • Plan de trabajo

DOMINIO COBIT	PROCESO COBIT	Objetivo de control	Prueba a realizar
ENTREGA Y SOPORTE	SEGURIDAD	Identificación y autenticación. Control de acceso	- Verificar si existe un registro de las solicitudes de acceso autorizado.
			- Verificar que la concesión de derechos privilegiados se restringe tanto como sea posible.
			- Determinar si se ha establecido un procedimiento formal de análisis, bloqueo y eliminación de usuarios obsoletos a nivel sistema.
			- Verificar el mecanismo de custodia de contraseñas privilegiadas.
			- Validar que las políticas de identificación y autenticación son adecuadas para preservar el control de acceso a los sistemas y a la información contenida en estos. Comprobar la implementación de estas políticas en los sistemas actuales.
			- Revisar las políticas de utilización de los identificadores de usuario, analizando la conveniencia del uso de identificadores de usuario genéricos vs. personalizados. Validar que están implementadas en los sistemas actuales.
			- Verificar si se ha configurado una política de contraseñas robustas y uniformes en los distintos sistemas de validación de usuarios.
			- Determinar si las contraseñas se almacenan y presentan siempre en formato ininteligible, haciendo uso de un algoritmo de cifrado irreversible.
			- Verificar si las contraseñas de los usuarios generados por defecto durante la instalación de los sistemas actuales han sido convenientemente modificadas.
			- Validar los procedimientos de control de sesiones http.



## • Plan de trabajo

DOMINIO COBIT	PROCESO COBIT	Objetivo de control	Prueba a realizar
ENTREGA Y SOPORTE	SEGURIDAD	Gestión de cuentas de usuario	<ul style="list-style-type: none"> <li>- Determinar si existen procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios. Estos procedimientos cubren todas las etapas del ciclo de vida del usuario, desde el registro inicial de los nuevos, las concesiones adicionales que se puedan requerir, hasta la baja final del usuario, ya sea cliente o usuario técnico.</li> </ul>
		Reportes relacionados con las actividades de seguridad e intentos de violación de la seguridad	<ul style="list-style-type: none"> <li>- Determinar si están activados los principales eventos de auditoría en los sistemas actuales. Los principales eventos de auditoría son: intentos no autorizados de acceso al sistema, cambios de políticas y reglas de seguridad, utilización de súper usuarios y comandos críticos del sistema, ...</li> </ul>
			<ul style="list-style-type: none"> <li>- Validar si se explotan los logs de los sistemas de forma integrada</li> </ul>
			<ul style="list-style-type: none"> <li>- Determinar si se mantienen pistas de auditoría de todas las transacciones realizadas.</li> </ul>
		Control de la actividad de las cuentas de usuario	<ul style="list-style-type: none"> <li>- Validar los mecanismos de mantenimiento y protección de logs.</li> <li>- Verificar que existe un plan para aplicar políticas de bloqueo de cuentas de usuarios tras reiterados intentos de conexión fallidos. Comprobar que estas políticas están implementadas y se han parametrizado los sistemas actuales en este sentido.</li> </ul>

- Plan de trabajo

## Sistemas

DOMINIO COBIT	PROCESO COBIT	Objetivo de control	Prueba a realizar
ADQUISICIÓN E IMPLEMENTACIÓN	INSTALACIÓN Y ACREDITACIÓN DE SISTEMAS	Entornos de desarrollo, pruebas y producción	Comprobar la existencia de entornos diferenciados para desarrollo, test y producción soportados sobre máquinas físicas y dominios de seguridad independientes
	GESTIÓN DE CAMBIOS	Gestión de cambios	Verificar si se ha implantado un flujo de autorizaciones para la gestión de cambios en la configuración de la infraestructura base

- **Conclusiones**
- Dirección y Gestión.
  - Definir una metodología para el ciclo de vida del desarrollo y para una correcta administración y seguimiento de los proyectos.
  - Realizar un control sistemático de la calidad del desarrollo.
  - Establecer formalmente las normas y pautas que deben seguir los distintos equipos de desarrollo (instrucciones prohibidas, etc.).
- Desarrollo y Mantenimiento.
  - Resulta imprescindible conseguir una más efectiva involucración del usuario desde el inicio del proyecto, asegurando una efectiva definición de necesidades.
  - Seguridad debería participar en todos estos proyectos para asegurar un adecuado tratamiento de los requerimientos de seguridad propios del entorno.
  - Debe mejorarse la coordinación con los distintos equipos de desarrollo con el fin de disponer a tiempo de todos los juegos de prueba necesarios.
  - Deben mejorarse los sistemas y controles de traspaso de programas a explotación y de publicación de contenidos.

- **Conclusiones**

- **Seguridad.**

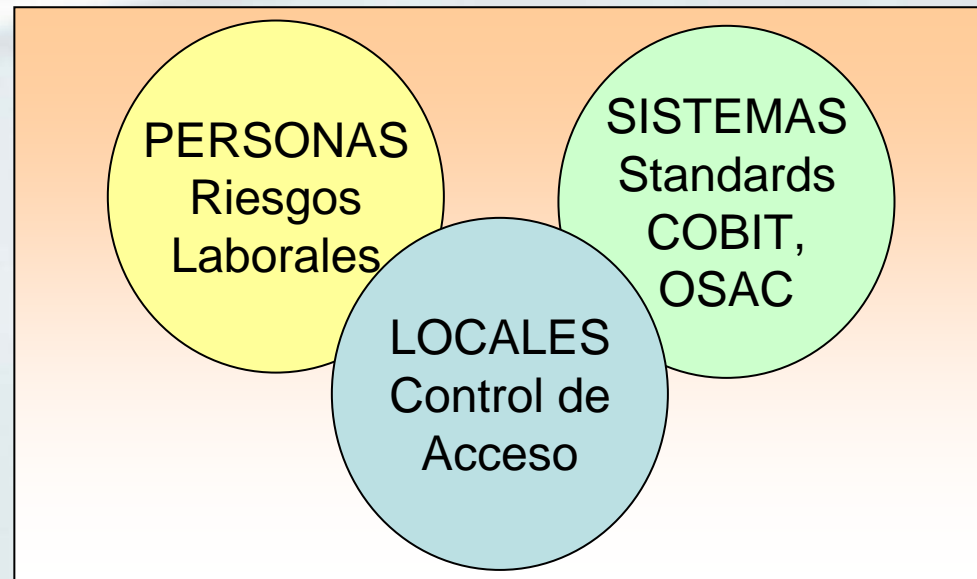
- No se dispone de un Plan de Contingencias para este entorno.
- Consideramos el sistema de identificación basado en DNI y PIN de 4 dígitos como poco robusto.
- Debería estudiarse la posibilidad de introducir mecanismos de firma digital avanzada.

### Pilares de la seguridad física

- Los SISTEMAS
- Los LOCALES
- Las PERSONAS

### Fundamentos

- Standards de Seguridad Física: COBIT, OSAC,...
- Procedimientos y políticas de control de acceso - Seguridad Perimetral
- Normativas vigentes en Riesgos Laborales



- **Características de la sala de ordenadores**
- **Sistemas de extinción de incendios**
- **Sistemas de drenaje y control de humedades (en ventanas, paredes y techos)**
- **Suministro de energía eléctrica**
- **Sistemas de aire acondicionado**
- **Aspectos generales:**
  - Prohibiciones específicas (manipulación de equipos, entrada de bebidas o comidas, fumar, utilizar instrumentos o materiales incendiarios o peligrosos [i.e. sopletes, soldadores, productos de limpieza corrosivos...], etc.)
  - Conocimientos y formación de los operadores y personal de mantenimiento.
  - Accesibilidad de cuadros de mando, controles, interruptores etc.
  - Orden y limpieza de las salas
  - Paneles informativos con instrucciones específicas (en caso de incendio, etc.)
  - Principales equipos Hardware (CPUs, sistemas de almacenamiento, robots de copias, impresoras, equipos de comunicaciones, etc.)
  - Alumbrados de emergencia



- **Ubicación física de las instalaciones**
  - Análisis riesgos medioambientales (inundaciones, incendios,...)
  - Análisis locales próximos de riesgo potencial
  - Otros elementos de riesgo (circulación pesada de vehículos, aeropuertos, líneas de tren o metro,...)
- **Protecciones externas**
  - Existencia de un perímetro de seguridad bajo control y vigilancia
  - Etc.
- **Protecciones internas**
  - Protección de activos de acceso restringido (documentación, archivos,...)
  - Restricciones de acceso a equipamiento crítico
- **Control de accesos**
  - Mecanismos
  - Tipos de cerraduras y modos de apertura.
  - Detectores de apertura de puertas
  - Detectores de presencia
  - Cámaras de vigilancia en puertas y ventanas. Grabación de las salas

- El **objetivo final** de la revisión de la seguridad física en el ámbito de las **Personas** es la realización del diagnóstico de las instalaciones en lo referente a **Prevención de Riesgos Laborales**.
  - Organización preventiva: existencia de estructura organizativa de acuerdo a lo estipulado en la normativa vigente (R.D. 39/1997)
  - Evaluación de riesgos: según lo requerido en la Ley 54/2003
    - Instalaciones eléctricas
    - Medios de protección contra incendios
    - Plan de emergencia
    - Formación e información del personal
    - Coordinación de actividades empresariales