# Experiencia Práctica - Endesa

ISMS Forum Spain

ASOCIACIÓN ESPAÑOLA PARA EL FOMENTO DE LA SEGURIDAD DE LA INFORMACIÓN


III Jornada Internacional

**Compliance en Seguridad de la Información:**

Claves y Tendencias

Una visión global del presente y una mirada al futuro

29 de mayo de 2008, Madrid

Organiza: ISMS Forum Spain

Con la colaboración de: INTECO – Instituto Nacional de Tecnologías de la Comunicación

Patrocinadores Oro:

accenture – High performance. Delivered.
dintel
ECIJA
ERNST & YOUNG – Quality In Everything We Do
ESA Security – Seguridad de la Información
FCC
hp invent
IBM
S21sec – La seguridad digital del futuro, hoy
SGS
steria
symantec.
Telefónica

# Experiencia Práctica - Endesa

El Rol de Auditoría Interna en relación a la

**Seguridad de la Información** y su

**Cumplimiento**

Experiencia en Endesa

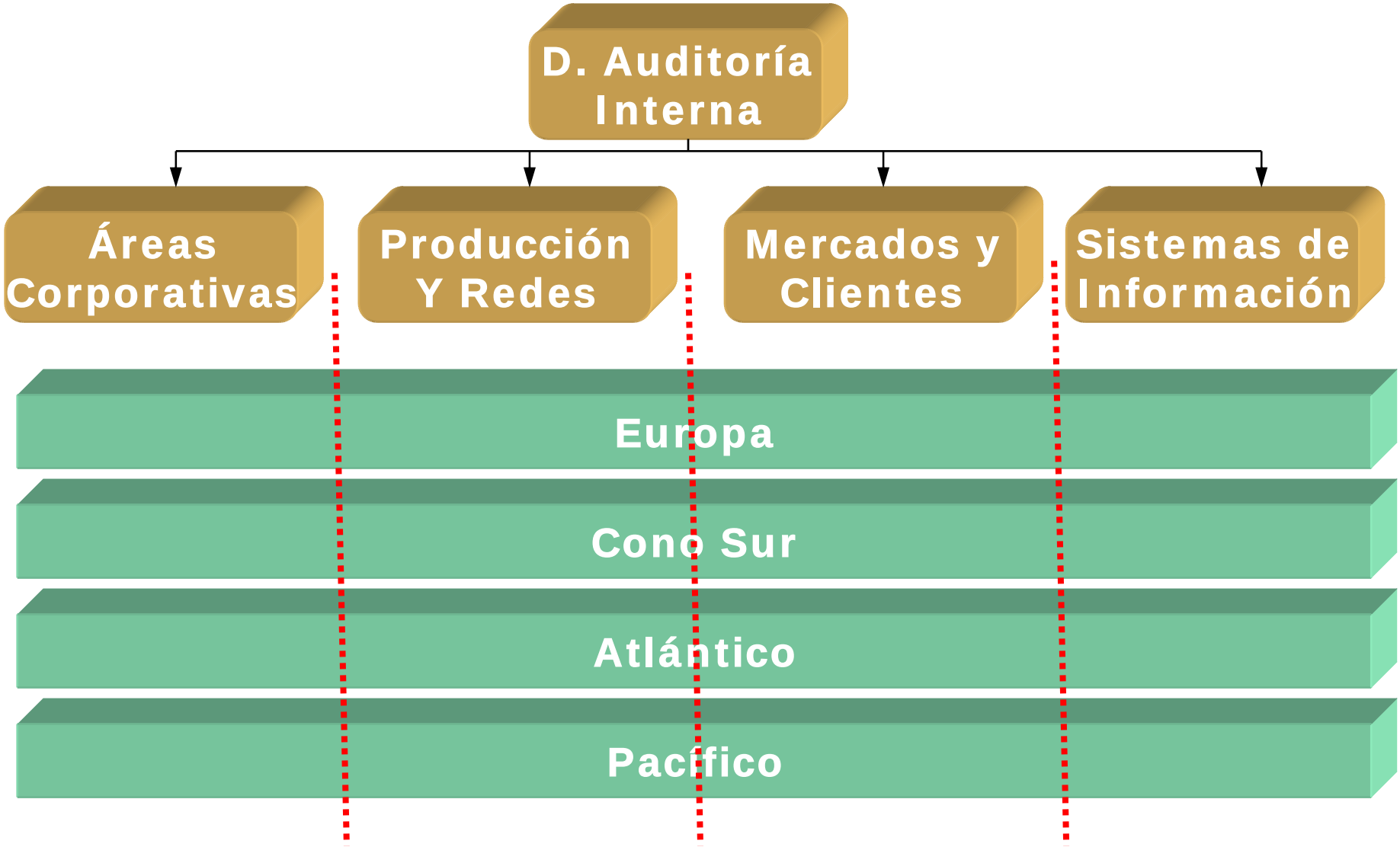
# Experiencia Práctica - Endesa

La Función de Auditoría Interna se crea en Endesa en diciembre de 1975


**Actualmente**

- Única para el toda la compañía
- Estructurada por ámbito funcional o de proceso
- Con unidades operativas en los países donde opera la compañía
- Con metodologías, sistemas y herramientas unificados
- Con un Plan de Auditoría único

# Experiencia Práctica - Endesa



# Experiencia Práctica - Endesa

"La auditoría interna es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización.

Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno."

Instituto de Auditores Internos, The IIA

# Experiencia Práctica - Endesa

- En 1997 elabora un análisis de riesgos de la compañía donde se identifica la importancia que tienen los activos de información y su proyección futura.

- En 1998 promueve la creación de una función que vele por la adecuada gestión de la seguridad de la información.

- Creación del Comité de Seguridad de la Información y del cuerpo normativo relacionado.

# Experiencia Práctica - Endesa

- En el año 2000 se inicia, en base al análisis de riesgos realizado y al Plan establecido, auditorías relacionadas con la seguridad de los activos de información.

- Ese mismo año, y como recomendación de auditoría, se crea la función de seguridad informática.

- En 2001 se realiza una revisión sobre el cumplimiento de la Ley Orgánica de Protección de Datos Personales 15/1999.

# Experiencia Práctica - Endesa

- Desde al año 2003 se difunde la normativa y buenas prácticas en seguridad de la información a las compañías latinoamericanas del grupo.

- Se crean Comités de Seguridad por país y se realizan campañas de concienciación a los empleados.

- Se auditan las funciones de seguridad de la información y seguridad informática promoviendo cambios en su organización y funcionamiento.

# Experiencia Práctica - Endesa

- Se audita la seguridad de acceso de los principales sistemas promoviendo la creación de una Unidad centralizada de Control de Accesos y la conveniencia de implantar un sso.

- En 2005 para dar cumplimiento a la ley Sarbanes-Oxley se define e implanta un modelo de control interno sobre la información financiera en la compañía.

- Desde esa fecha Auditoría Interna revisa anualmente el alcance del modelo, su diseño y su operatividad.

# Experiencia Práctica - Endesa

- Producto de la auditoría se impulsa el establecimiento de un modelo global de segregación de funciones y la puesta en marcha de un proyecto para su implantación.

- Actualmente este modelo permite dar cumplimiento a la ley 262/2005 italiana.

# Experiencia Práctica - Endesa

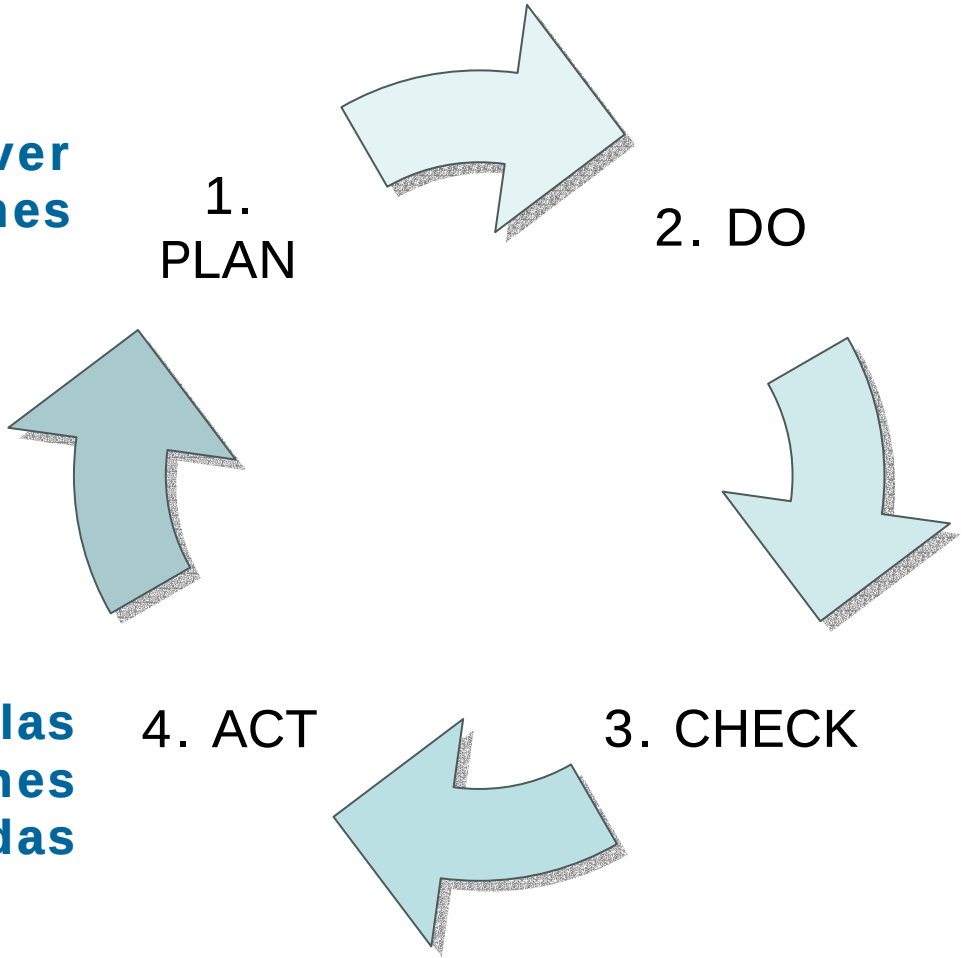
- Periódicamente se informa al Comité de Auditoría del Consejo y a los Comités Internos de Auditoría sobre los principales riesgos encontrados, producto de las auditorías realizadas en base al Plan establecido.

- Según el Plan establecido se realizan auditorías sobre:
  - Seguridad de los diferentes entorno
  - Planes de continuidad
  - Segregación de funciones
  - Confidencialidad de las bases de datos
  - Cumplimiento de leyes sectoriales
  - Cumplimiento de SOX y LOPD

# Experiencia Práctica - Endesa

- Colaboración con las funciones de seguridad en relación a proyectos piloto e implantación de nuevas herramientas.

# Experiencia Práctica - Endesa



# Experiencia Práctica - Endesa

## Dos Acciones

### Promover

Dada su comunicación con los Órganos de Gobierno.

Su carácter independiente.

Enfocado a la mitigación de riesgos.

### Supervisar

A través de un Plan de auditorías elaborado a partir de un análisis de riesgos de la compañía.

Apoyado en un adecuado seguimiento a las recomendaciones emitidas.

# Gracias por su atención


# Preguntas

www.ismsforum.es

ISMS Forum Spain

ASOCIACIÓN ESPAÑOLA PARA EL FOMENTO DE LA SEGURIDAD DE LA INFORMACIÓN