



Esquema Nacional de Seguridad. Lecciones aprendidas

Rubén Frieiro Barros, CISM, CISSP
Senior Manager
Gestión de riesgos tecnológicos
Deloitte

Sevilla, 3 de noviembre de 2011



Contenidos

- Introducción al ENS
- Factores clave
- Política de seguridad
- Organización
- Alcance del ENS
- Plan de adecuación
- Conclusiones



¿Qué es el ENS?

- Real Decreto 3/2010, por el que **se regula el Esquema Nacional de Seguridad**, previsto en el artículo 42 de la Ley 11/2007
- Su objetivo es **establecer la política de seguridad** en la utilización de los medios electrónicos y está constituido por unos **principios básicos** y unos **requisitos mínimos** que permitan una adecuada protección de la información.
- Su ámbito de aplicación es el establecido en el artículo 2 de la ley 11/2007, y afecta a las Administraciones Públicas, los ciudadanos en su relación con las mismas y las relaciones entre éstas.
- Fechas clave:



¿Qué es el ENS?

Elementos principales Esquema Nacional de Seguridad:

- Principios Básicos y Requisitos mínimos

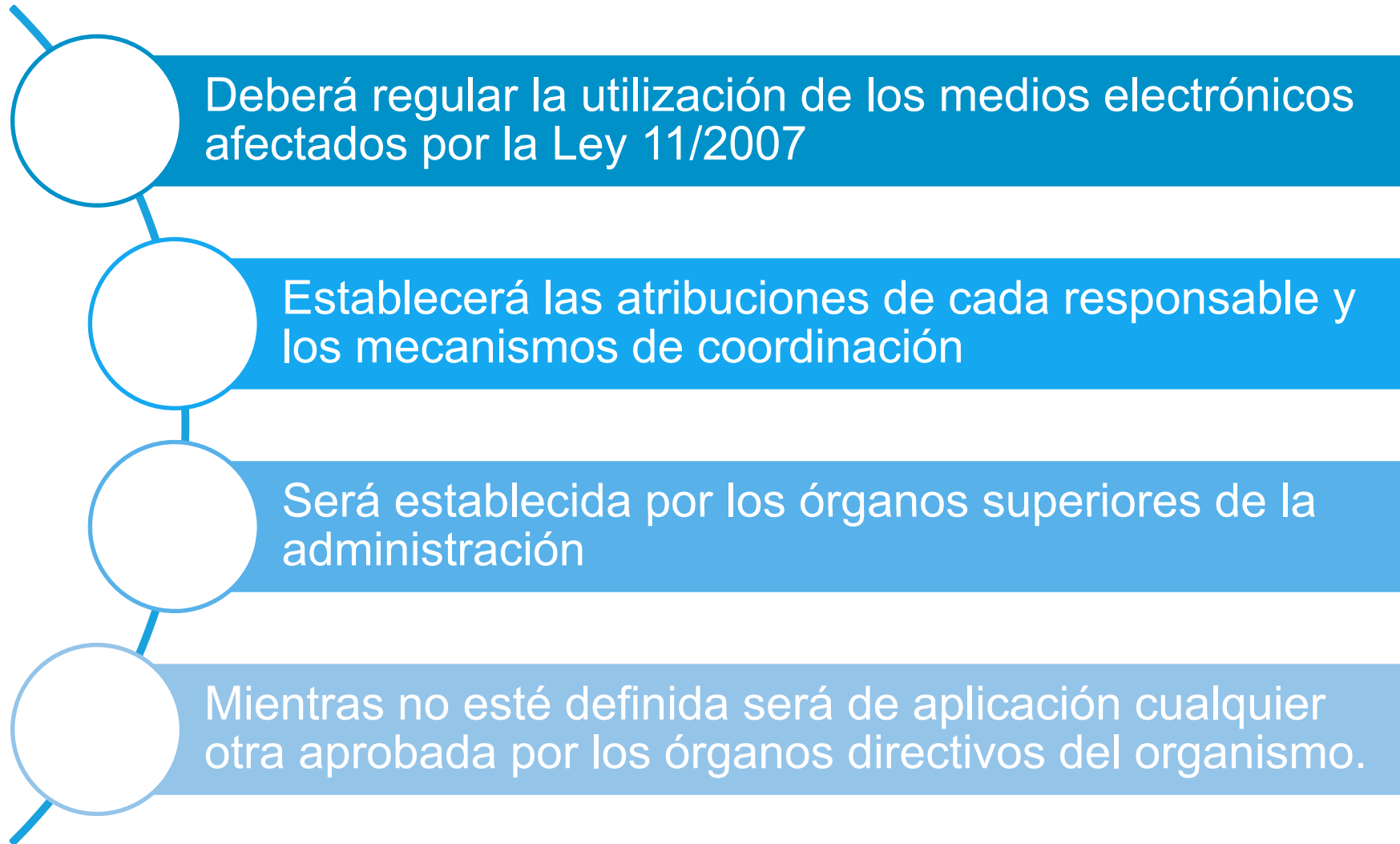


- Integrar la seguridad en los procesos tecnológicos
- Proporcionalidad en la adopción de medidas de seguridad
- Segregación de funciones

Factores clave



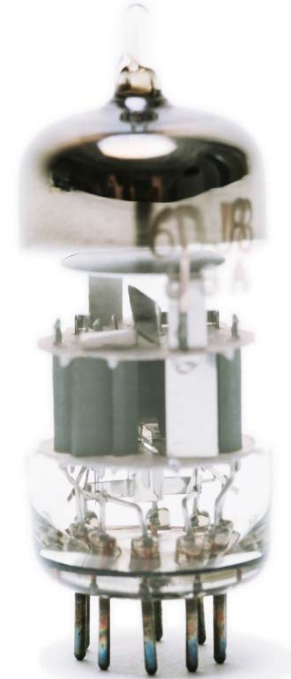
Política de seguridad



Política de seguridad

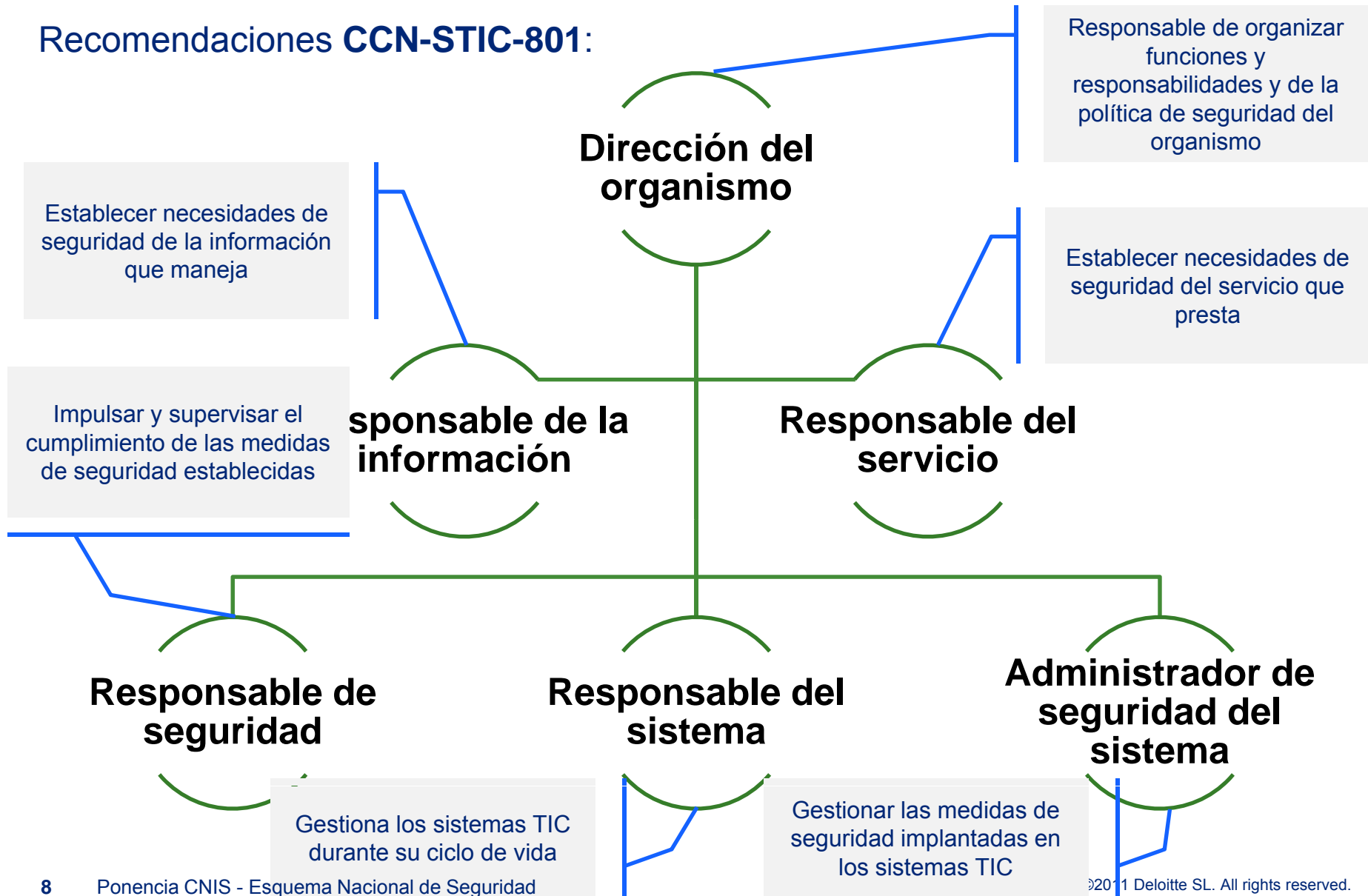
Recomendaciones **CCN-STIC-805**:

- **Documento a alto nivel** que define lo que **significa la seguridad** de la información en una organización
- **Accesible** a todos los miembros de la organización
- **Aprobada** por el **titular del órgano superior** correspondientes
- **Identificará** claramente a los **responsables** de velar por su cumplimiento
- Su contenido mínimo establecerá:
 - Objetivos y misión de la organización
 - Marco normativo
 - Organización de la seguridad
 - Concienciación y formación
 - Postura para la gestión de los riesgos
 - Proceso de revisión de la política de seguridad



Asignación de responsabilidades

Recomendaciones CCN-STIC-801:



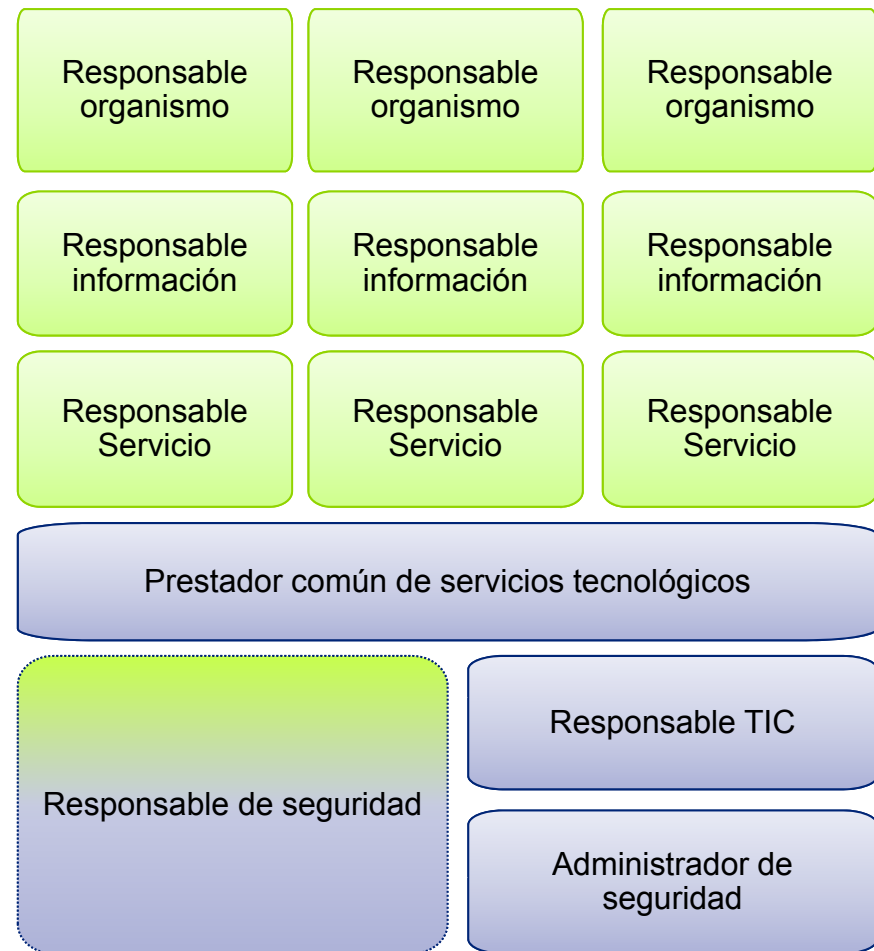
Asignación de responsabilidades

Escenarios habituales

Modelo centralizado



Modelo Descentralizado



Alcance de aplicabilidad



Plan de adecuación

Identificar el alcance

Sede electrónica / herramientas comunes de gestión telemática / catalogo de servicios / ...

Determinar responsabilidades funcionales

Servicios soportados / información gestionadas

Valoración de los sistemas de información

Disponibilidad / Integridad / Confidencialidad / Trazabilidad / Autenticidad

Plan de adecuación

Evaluar las medidas implantadas actualmente

Marco organizativo / marco operacional /
medidas de protección

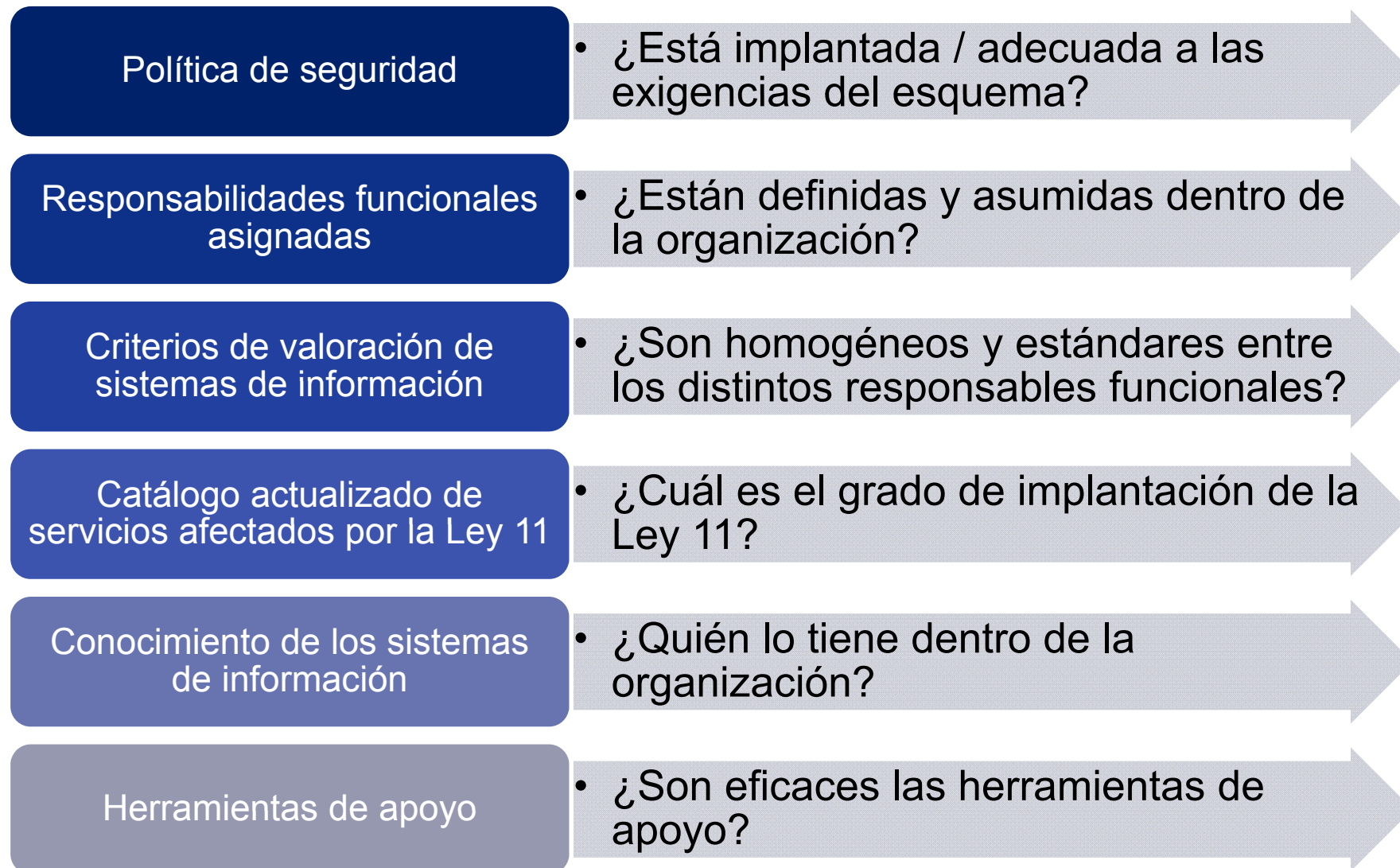
Determinar el GAP de cumplimiento

Categorización de los SI Vs. Requerimientos por
categoría

Definir acciones correctoras

Implantar / adecuar medidas en los sistemas
analizados

Retos para la confección de plan



Conclusiones

- La aplicación de medidas de seguridad tiene que considerar el ciclo de vida de los sistemas de información
- Definir medios que sistematicen la categorización de los sistemas empleando criterios objetivos:
 - Tipología de datos manejados en el servicio
 - Plazos asociados a la tramitación de un expediente
 - Sanciones / penalizaciones que se puedan efectuar
 - Servicios que afectan a los derechos fundamentales de las personas
- Conocer bien las dependencias e interrelaciones de los sistemas de información entre sí.
- [Grado de cumplimiento de ley 11 en la actualidad.](#)

Ranking de servicios ofrecidos al ciudadano

Tabla 7. Ranking de los servicios on-line ofrecidos al ciudadano, 2009								
ÁREA	SERVICIOS	Nivel 0	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5	Total
EDUCACIÓN	1. Consulta de notas y faltas de asistencia	23%	0%	0%	23%	38%	15%	100%
HACIENDA	2. Impuesto sobre transmisiones patrimoniales y actos jurídicos documentados	0%	0%	21%	0%	71%	7%	100%
SANIDAD Y SALUD PÚBLICA	3. Cita previa	13%	7%	7%	0%	67%	7%	100%
MEDIO AMBIENTE	4. Expedición de licencias de caza y pesca	0%	7%	13%	27%	47%	7%	100%
ADMINISTRACIÓN	5. Licitación electrónica	0%	13%	33%	13%	33%	7%	100%
INVESTIGACIÓN	6. Becas de formación de personal investigador	7%	0%	47%	13%	27%	7%	100%
ECONOMÍA, TRABAJO Y EMPLEO	7. Registro de cooperativas	13%	7%	40%	13%	20%	7%	100%
EMPRESAS Y TRANSPORTE	8. Autorización de Instalaciones Eléctricas de Baja Tensión	0%	0%	25%	12%	56%	6%	100%
ECONOMÍA, TRABAJO Y EMPLEO	9. Oferta de Empleo Público	0%	6%	25%	12%	50%	6%	100%
ECONOMÍA, TRABAJO Y EMPLEO	10. Ofertas de empleo privado	6%	6%	19%	25%	37%	6%	100%
EDUCACIÓN	11. Preinscripción en centros de enseñanza	6%	6%	50%	0%	31%	6%	100%
ADMINISTRACIÓN	12. Consulta y adquisición de publicaciones	6%	6%	31%	31%	19%	6%	100%
EDUCACIÓN	13. Ayudas, Becas y subvenciones (para estudiantes)	0%	12%	50%	12%	19%	6%	100%
ADMINISTRACIÓN	14. Quejas y sugerencias de los ciudadanos	0%	0%	13%	20%	67%	0%	100%
MEDIO AMBIENTE	15. Gestión de residuos	0%	12%	19%	6%	62%	0%	100%
SISTEMA DE INFORMACIÓN GEOGRÁFICA (SIG)	16. Ubicación de servicios	0%	10%	10%	20%	60%	0%	100%
OCIO, TURISMO Y CULTURA	17. Reserva de plaza en albergues	7%	0%	23%	15%	54%	0%	100%
MEDIO AMBIENTE	18. Expedición de permisos de caza y pesca	15%	15%	8%	8%	54%	0%	100%
OCIO, TURISMO Y CULTURA	19. Consulta Bibliotecas Públicas	0%	13%	13%	20%	53%	0%	100%
SISTEMA DE INFORMACIÓN GEOGRÁFICA (SIG)	20. Servicios georeferenciados	0%	17%	8%	25%	50%	0%	100%

NIVELES: 0= No implementado; 1= Ofrece información, 2= Efectúa interacción en un sentido, 3= Efectúa interacción en ambos sentidos, 4= Trámite completo, 5= Personalización

Fuente Informe Administración Electrónica en las CCAA (CAE) 2009

Ranking de servicios ofrecidos al ciudadano

Tabla 8. Ranking de los Servicios on-line ofrecidos al ciudadano por CCAA, 2009 (primeros 10 servicios)																			
SERVICIOS	Andalucía	Aragón	Principado de Asturias	Illes Balears	Canarias	Cantabria	Castilla - La Mancha	Castilla y León	Cataluña	Comunitat Valenciana	Extremadura	Galicia	Comunidad de Madrid	Región de Murcia	Navarra	País Vasco	La Rioja	Ceuta	Melilla
1. Consulta de notas y faltas de asistencia	ND	3	4	0	3	4	ND	3	ND	5	5	ND	4	ND	4	0	4	0	ND
2. Impuesto sobre transmisiones patrimoniales y actos jurídicos documentados	4	4	4	4	2	5	ND	4	4	4	2	ND	2	4	4	ND	4	ND	ND
3. Cita previa	4	4	4	2	4	0	ND	0	4	4	5	ND	4	4	1	4	4	ND	ND
4. Expedición de licencias de caza y pesca	4	2	4	3	ND	3	ND	3	4	2	3	ND	5	1	4	4	4	4	ND
5. Licitación electrónica	2	3	2	4	2	1	ND	2	4	4	3	ND	4	1	4	5	2	ND	ND
6. Becas de formación de personal investigador	4	2	2	2	2	0	ND	3	4	3	5	ND	2	2	4	4	2	ND	ND
7. Registro de cooperativas	4	1	3	0	ND	3	ND	2	2	2	2	ND	4	2	4	5	2	0	ND
8. Autorización de Instalaciones Eléctricas de Baja Tensión	4	2	4	4	3	3	ND	4	2	4	5	ND	2	2	4	4	4	4	ND
9. Oferta de Empleo Público	4	2	4	4	2	4	ND	4	3	2	5	ND	2	3	4	4	4	1	ND
10. Ofertas de empleo privado	1	2	2	3	2	3	ND	3	3	4	5	ND	4	4	4	4	4	0	ND

ND: dato no disponible

(1) Incluye toda la gestión de autorización o denegación de los diferentes validadores del proceso

(2) Consiste en una especie de "pack de bienvenida" con información de recursos (material, instalaciones, beneficios, normativa general, etc.)

Fuente Informe Administración Electrónica en las CCAA (CAE) 2009

Alguna pregunta.....

...Gracias por su atención



Si desea información adicional, por favor, visite www.deloitte.es

Deloitte se refiere a Deloitte Touche Tohmatsu Limited, (*private company limited by guarantee*, de acuerdo con la legislación del Reino Unido) y a su red de firmas miembro, cada una de las cuales es una entidad independiente. En www.deloitte.com/about se ofrece una descripción detallada de la estructura legal de Deloitte Touche Tohmatsu Limited y sus firmas miembro.

Deloitte presta servicios de auditoría, asesoramiento fiscal y legal, consultoría y asesoramiento en transacciones corporativas a entidades que operan en un elevado número de sectores de actividad. La firma aporta su experiencia y alto nivel profesional ayudando a sus clientes a alcanzar sus objetivos empresariales en cualquier lugar del mundo. Para ello cuenta con el apoyo de una red global de firmas miembro presentes en más de 140 países y con aproximadamente 170.000 profesionales que han asumido el compromiso de ser modelo de excelencia.

Esta publicación contiene exclusivamente información de carácter general, y Deloitte Touche Tohmatsu Limited, Deloitte Global Services Limited, Deloitte Global Services Holdings Limited, la Verein Deloitte Touche Tohmatsu, así como sus firmas miembro y las empresas asociadas de las firmas mencionadas (conjuntamente, la "Red Deloitte"), no pretenden, por medio de esta publicación, prestar servicios o asesoramiento en materia contable, de negocios, financiera, de inversiones, legal, fiscal u otro tipo de servicio o asesoramiento profesional. Esta publicación no podrá sustituir a dicho asesoramiento o servicios profesionales, ni será utilizada como base para tomar decisiones o adoptar medidas que puedan afectar a su situación financiera o a su negocio. Antes de tomar cualquier decisión o adoptar cualquier medida que pueda afectar a su situación financiera o a su negocio, debe consultar con un asesor profesional cualificado. Ninguna entidad de la Red Deloitte se hace responsable de las pérdidas sufridas por cualquier persona que actúe basándose en esta publicación.

© 2011 Deloitte, S.L.