AMETIC

Certificación y consecución de la Adecuación al Esquema Nacional de Seguridad

Murcia, 20 *de octubre de* 2011

José Angel Valderrama Antón
Gerente de Nuevas Tecnologías
AENOR

CCN Centro Criptológico Nacional
ens Esquema Nacional de Seguridad
Gobierno de España — Ministerio de Política Territorial y Administración Pública
plan avanza2
Gobierno de España — Ministerio de Industria, Turismo y Comercio
Unión Europea — Fondo Europeo de Desarrollo Regional — "Una manera de hacer Europa"
AENOR Asociación Española de Normalización y Certificación

Indice

- AENOR
- El modelo ENS y el modelo ISO 27001
- Qué es la certificación, y qué se certifica
- Como se certifica
- Datos de certificaciones
- Ventajas

AENOR

AENOR Asociación Española de Normalización y Certificación

- Contribuir mediante el desarrollo de las actividades de N+C a mejorar la calidad de las empresas, sus productos y servicios, proteger el medio ambiente y con ello lograr:

  El bienestar de la sociedad

Entidad designada por el Ministerio de Industria y Energía (R.D. 1614|1985), como entidad para desarrollar las actividades de N+C. Reconocida como Organismo de Normalización y para actuar como Entidad de Certificación (R.D. 2200|1995)

AENOR

- Miembro español de los organismos de normalización Internacionales, Europeos y Americanos.

- Acreditado por la entidad nacional de acreditación *(ENAC)*, el Ministerio de Trabajo, …
- Miembro español de IQNet
- Miembro español de la red mundial de eco-etiquetado.
- Organismo notificado para 13 directivas de nuevo enfoque.
- …

El modelo ENS y el modelo ISO 27001

- ENS (Real Decreto 3/2010)
- SGSI (UNE-ISO/IEC 27001:2007 - ISO/IEC 27001:2005), con origen en BS 7799-1 y 2 de 1995 y 1998.
- Adecuación // Implantación
- Declaración de conformidad // Certificado

- Establece principios y requisitos de la política de seguridad, como marco general para proteger los datos e informaciones.

  → Garantizar el cumplimiento y eficacia, requiere de un proceso sistemático, documentado y conocido por todos los miembros de la organización.

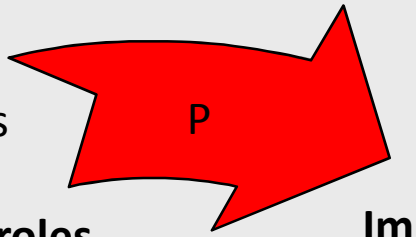
  → Sistema de gestión de la seguridad de la información.

Modelo ENS y el modelo ISO 27001

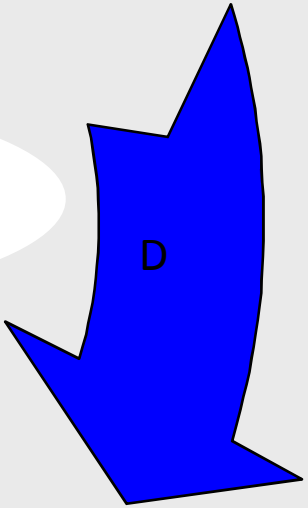
1. Establecer la política de seguridad.
2. Inventariar la información y los servicios.
3. Realizar el análisis de riesgos, y determinar las medidas de seguridad a aplicar.
4. Establecer el plan de adecuación para cumplir el ENS. *(30 Enero 2011 Declaración de conformidad | Plan de adecuación – 2014)*
5. Adecuación.
6. Auditoría.

Modelo ENS y el modelo ISO 27001

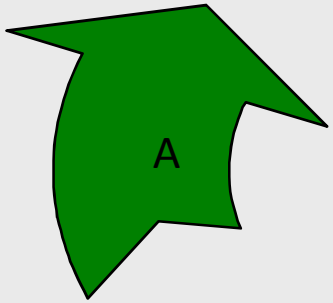
Establecer **alcance y los límites**
Definir **política** de seguridad
Realizar **análisis y evaluación** de riesgos
Evaluar **opciones** para su tratamiento
Seleccionar **objetivos de control** y **controles**
Aprobación de la Dirección del **Riesgo residual**
Autorización para implantar el SGSI
Declaración de Aplicabilidad



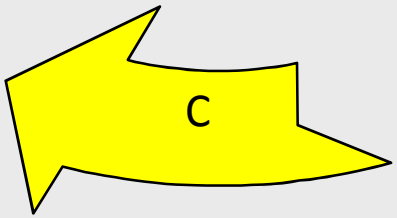
Implantar plan de gestión de riesgos
Implantar el SGSI
Implantar los controles



Modelos ISO
Acreditado - Certificación
Experiencia



Adoptar las **acciones correctivas**
Adoptar las **acciones preventivas**



Revisar internamente el SGSI
Realizar **auditorias** internas del SGSI

ENS vs ISO 27001

ENS	ISO 27001
Obligatorio, según plazos definidos (Plan de adecuación: 30/01 - 2011 / 2014)	Voluntario. Basado en la normalización internacional y nacional
Ámbito nacional	Internacional
Relación con LOPD, pero independiente	Correspondencia / integración con otros SG, y requisitos legales (LOPD y otros).
Administración, entidades de derecho público	Cualquier organización
Alcance a medios electrónicos usados por los ciudadanos en su relación con las AAPP	Alcance adecuado para la organización
Auditoría bienal, según requisitos, para sistemas de cat. media y alta.	Auditoría de certificación, según protocolos ISO y acreditación ENAC
Conjunto particularizado de requisitos y medidas de seguridad. Análisis de riesgos para sistemas cat. media y alta.	Análisis de riesgos real. Medidas de seguridad / controles adecuados y justificados.
Con agentes implicados (CCN, INTECO)	Entidades de acreditación y certificación. (Ley 21/1992, de Industria, y RD 2200/95)

Qué es la certificación, y qué se certifica

Certificación:

- Acto por el que una **tercera parte testifica** que ha obtenido la adecuada confianza en la **conformidad** de un determinado producto, proceso o servicio, debidamente identificado, **con una norma** u otro documento normativo especificado.

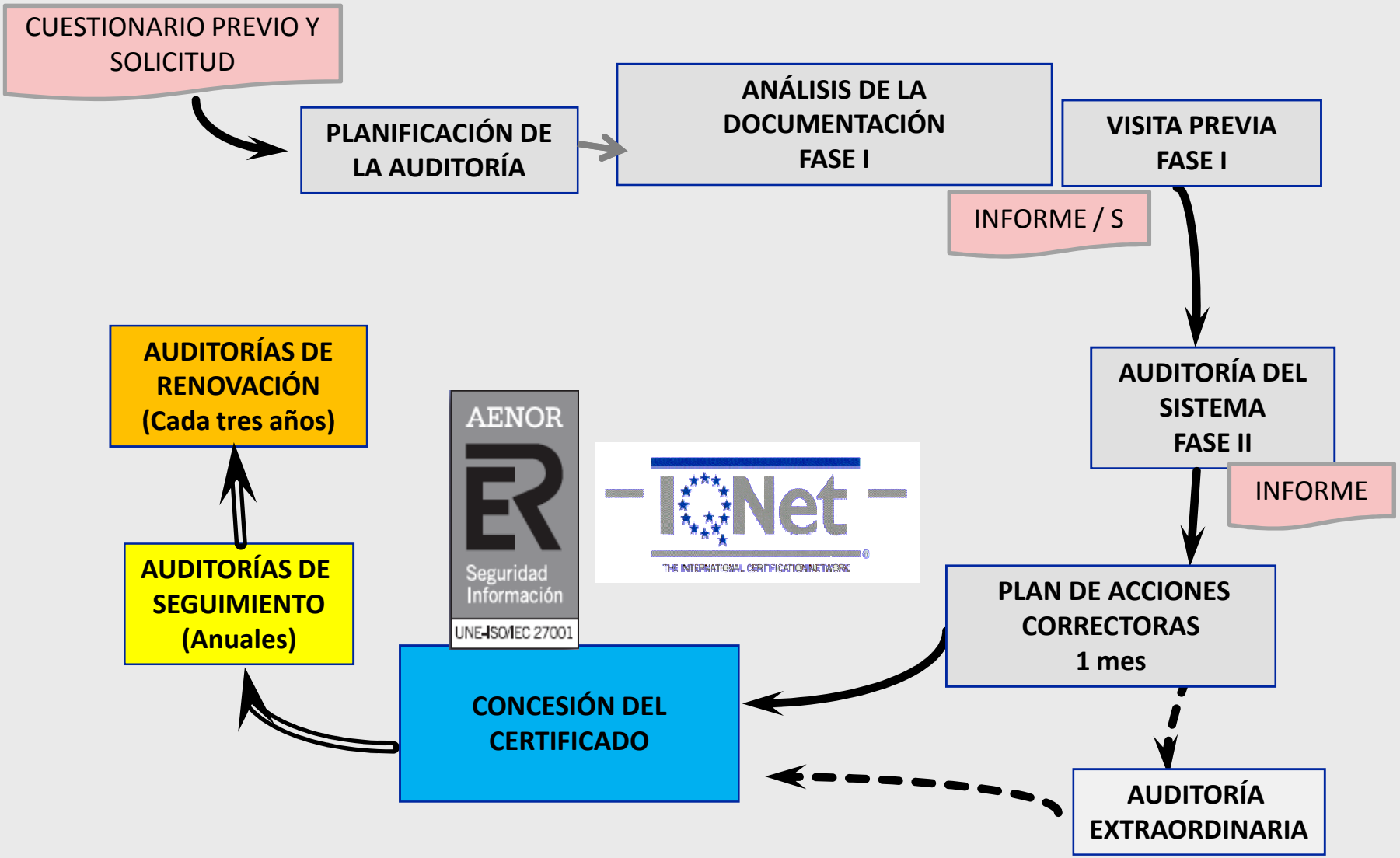
Comprobación de que un SGSI cumplen con una serie de requisitos especificados ... en ISO 27001

Certificación acreditada

ENAC
Entidad Nacional de Acreditación

AENOR

Como se certifica



AENOR

Como se certifica

Actividad	Objetivo
Solicitud de oferta y cuestionario previo	Recopilar información del SGSI. Dimensionar la certificación y determinar la competencia necesaria del equipo auditor. Oferta aceptada.
Planificación	Asignar equipo auditor, acordar fechas, preparar actividades, … Planificación
Fase I (análisis de documentación, visita a instalaciones, …)	Revisar las líneas generales del SGSI (documentación, ubicación e instalaciones, alcance del SGSI, enfocar y acordar planificación de Fase II). Informe
Fase II (Auditoría inicial)	Confirmar la implantación del SGSI, y adecuación a la ISO 27001. Informe de auditoría inicial.
Plan de acciones correctivas, y Decisión	Evaluar las acciones correctivas tomadas contra las no conformidades. Decisión de concesión del certificado (Si / No, con o sin Aud. Extraordinaria)
Emisión y entrega del certificado	Entrega del certificado acreditado, licencia de uso, y registro de la certificación. Certificado válido por tres años.
Aud. de seguimiento	Evaluar la implantación del SGSI , prevenir desviaciones. Anual.
Aud. de renovación	Evaluar implantación del SGSI, y emitir nuevo certificado. Cada tres años.

El certificado del SGSI

Certificado del Sistema de Gestión de Seguridad de la Información.

EMPRESA CERTIFICADA

AENOR

AENOR
ER
Seguridad Información
UNE-ISO/IEC 27001

IQNet
THE INTERNATIONAL CERTIFICATION NETWORK

ENAC
Entidad Nacional de Acreditación

La declaración de conformidad del ENS

Declaración de conformidad con el ENS, y **distintivos de seguridad**:

- Publicados en las sedes electrónicas, y fácilmente accesibles.
- Contenido a publicar:
  - Identificar al declarante.
  - El sistema o sistemas, y servicios a los que se refiere.
  - El mecanismo de control del cumplimiento del ENS.
  - Fecha y lugar de emisión, y firma del titular del organismo emisor.

- Y otros distintivos como: certificaciones en accesibilidad, interoperabilidad o calidad.
  - Indicando datos de la entidad emisora y ámbito al que se aplica.

- 30 Enero 2011: Publicar Declaración o Plan de adecuación
- CCN-STIC-809 – art. 41 del ENS

The ISO Survey 2010

ISO/IEC 27001 - Information security management systems - Requirements				
Overview				
Year	**2006**	**2007**	**2008**	**2009**
TOTAL	**5797**	**7732**	**9246**	**12934**
Africa / West Asia	426	600	983	1554
Central / South America	18	38	72	99
North America	79	112	212	322
Europe	1064	1432	2172	3564
Far East	4150	5494	5740	7335
Australia / New Zealand	60	56	67	60

Top 10 countries for ISO/IEC 27001 certificates - 2009		
1	Japan	5508
2	India	1240
3	United Kingdom	946
4	Taipei, Chinese	934
5	Spain	483
6	China	459
7	Romania	303
8	Italy	297
9	Czech Republic	264
10	Germany	253

ISO/IEC 27001 - Europe				
Year	**2006**	**2007**	**2008**	**2009**
Country	**810**	**988**	**1545**	**2546**
Czech Republic	27	77	88	264
Germany	95	135	239	253
Italy	175	148	233	297
Romania	4	16	44	303
Spain	23	93	203	483
United Kingdom	486	519	738	946

The ISO Survey 2010

ISO/IEC 27001 - Certificates by industrial sector

The following table gives an idea of the number of certificates by industrial sector. Not all data sources responded to the request …

EA* Code Nos.	ISO/IEC 27001 BY INDUSTRIAL SECTOR	2006	2007	2008	2009
33	Information technology	890	1236	1152	2086
35	Other Services	189	204	228	380
36	Public administration	23	33	79	181
34	Engineering Services	25	33	48	173
31	Transport, storage and communication	60	70	63	170
32	Financial intermediation, real estate, rental	47	54	68	148
19	Electrical and optical equipment	38	58	50	135
28	Construction	55	17	12	127
38	Health and social work	14	10	61	102
37	Education	8	9	25	47
TOTAL		**1349**	**1724**	**1786**	**3549**

Ventajas de certificar el SGSI

- **Apoya** enfoque de la Dirección.
- Apoya la actividad del Responsable del SGSI.
- **Demuestra** el cumplimiento de los requisitos:
  - ISO 27001,
  - Alineamiento con requisitos legales *(*LOPD, LSSICE, ENS, *…)*
- **Auditores** formados, cualificados, y expertos *(El análisis del experto, novedades y oportunidades de mejora).*

- Genera **confianza / credibilidad** interna y externa
  *(*clientes, empleados, accionistas / propietarios, administraciones / jueces, *…)*
- **Imagen** de marca y diferenciación *(AENOR, ENAC, IQNet).*
- **Novedoso** …

Muchas gracias, estamos a su disposición

José Angel Valderrama Antón

Gerente Nuevas Tecnologías

nuevastecnologias@aenor.es

AENOR - REGIÓN DE MURCIA:

Área de Negocios Plazarte

José Manuel Sánchez-Pedreño, 1, of. 5º B - El Ranero - 30009 MURCIA

Tel.: 968 272 770 - **drm@aenor.es**

InfoAENOR - 902 102 201

www.aenor.es