

III SEMANA DE SEGURIDAD DE LA INFORMACIÓN

“Certificación de Accesibilidad de Sitios Web y

Sistemas de Gestión de Seguridad de la Información”



Tudela, 25 de marzo de 2009

- AENOR
- Certificación
- Accesibilidad de sitios web
- Sistemas de Gestión de Seguridad de la Información

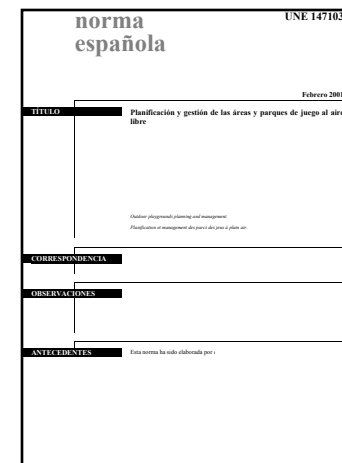
¿Qué es AENOR?

- Organización privada, independiente y sin ánimo de lucro, reconocida en los ámbitos nacional, comunitario e internacional
- Actividades multisectoriales de N+C
- Veintiún centros operativos en España, además de México, Chile, Italia, Portugal, Brasil, El Salvador, Perú y Bulgaria

Misión de AENOR

- 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



Normalización, Difusión e Información, Certificación, Formación, Publicaciones

Implantación de AENOR



AENOR MÉXICO

AENOR CHILE

AENOR EL SALVADOR

AENOR Brasil

AENOR Perú

AENOR ITALIA

lusAENOR

Cifras significativas de AENOR

Sistemas



21.797 Certificados ISO 9001
485 Certificados ISO/TS
72 Certificados EN 9100
128 Certificados QS-9001
80 Certificados ISO 27.001
499 Certificados PRL
457 Certificados OHSAS
101 Certificados I+D+i



4.453 Certificados ISO 14000
440 EMAS Certificados

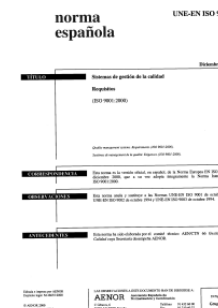


Productos

Más de 30.000 Certificados
Más de 81.000 Productos Certificados

Normalización

27.000 Normas UNE
en catálogo



Internacional



60 Países en los que AENOR
ha emitido sus certificados

Recursos humanos

722 Auditores
(internos y externos)

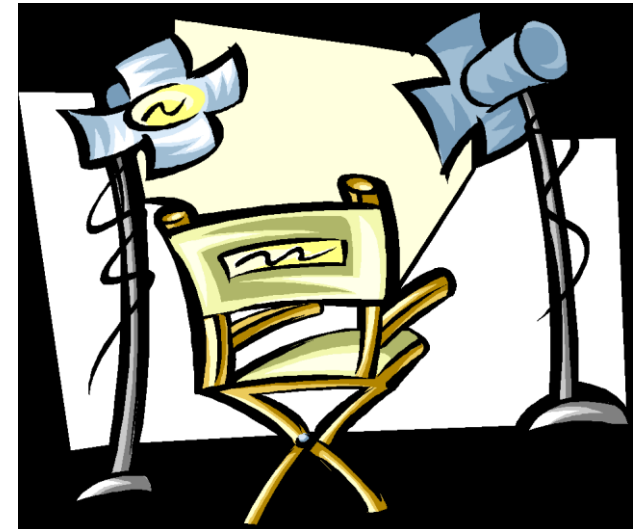


¿Qué es la certificación?

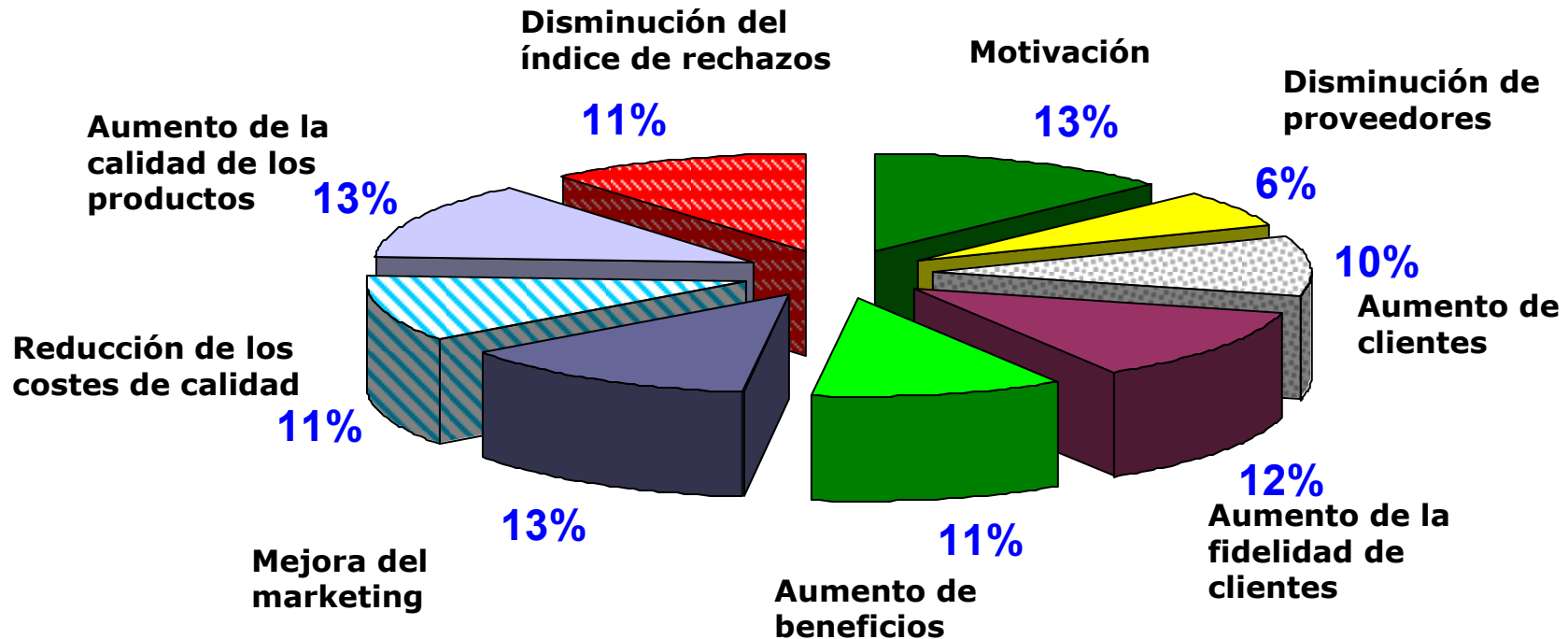
Comprobación de que un sistema, un producto o un servicio cumplen con una serie de requisitos específicos.

*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 (ISO 17000).*

- ☒ **Demuestra el cumplimiento** de requisitos.
- ☒ **Imagen** de marca y **diferenciación**.
- ☒ Genera **confianza** para el cliente / usuario.
- ☒ **Mejora interna / de procesos** .



Beneficios de la certificación



Fuente: Dpto. de Ingeniería de Organización, Administración de Empresas y Estadística.
Universidad Politécnica de Madrid

Certificación de Sistemas en AENOR

- Acreditado por la entidad nacional de acreditación (ENAC) para el 100% de los sectores de actividad (CNAE) en Sistemas de Calidad (ISO 9000) y Sistemas de Gestión Medio Ambiental (ISO 14000).



- Organismo autorizado por el Ministerio de Trabajo para realizar la certificación de Prevención de Riesgos Laborales (APRL) y estándar OHSAS 18001:2007
- Miembro español de IQNet



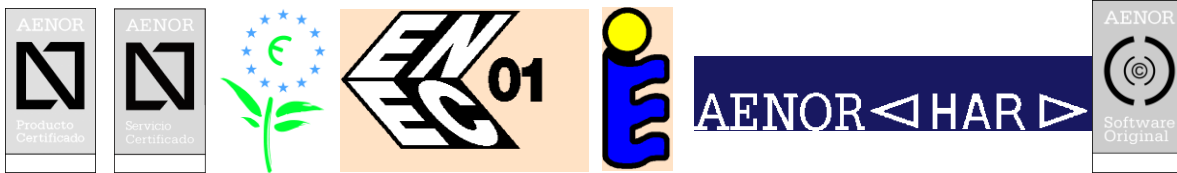
✓ *Más de 22 000 certificados de Empresa Registrada en todos los campos de la industria y el sector servicios;*

Certificación de producto en AENOR

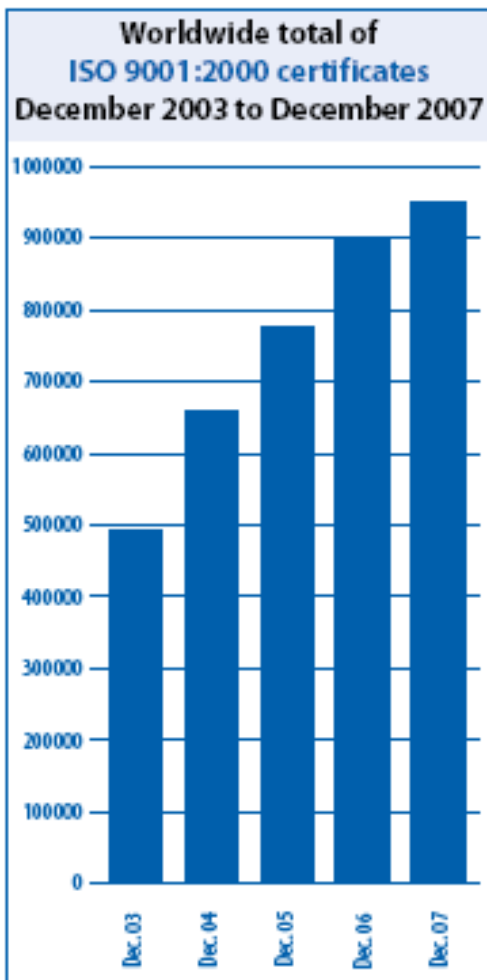
- Miembro español de la red mundial de eco-etiquetado esquema de certificación CENELEC (CCA) y esquema IEC CB.
- Más de 10 clases diferentes de certificados de producto y servicio.
- Organismo notificado para 13 directivas de nuevo enfoque



✓ *Más de 81 000 productos y servicios certificados*



The ISO Survey – 2006. ISO 9001 certificates



World results	Dec. 2003	Dec. 2004	Dec. 2005	Dec. 2006	Dec. 2007
World total	497 919	660 132	773 867	896 929	951 486
World growth	330 795	162 213	113 735	123 062	54 557
Number of countries/economies	149	154	161	170	175

Europe	242 455	320 748	377 196	414 232	431 479
Share in percent	48,69	48,59	48,74	46,18	45,35
No. of countries/economies	47	48	48	49	49

Slovakia	1 148	2 008	2 050	2 195	2 840
Slovenia	465	1 811	2 114	2 182	1 886
Spain	31 836	40 972	47 445	57 552	65 112
Sweden	3 107	4 687	4 744	4 839	5 233
Switzerland	9 200	11 546	12 412	10 094	11 077

The ISO Survey – 2006. ISO 27001 certificates

ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements

2006 was the first year for which the survey recorded ISO/IEC 27001:2005 certificates. At the end of December 2007, at least 7 732 ISO/IEC 27001:2005 certificates had

been issued in 70 countries and economies. The 2007 total represents an increase of 1 935 (+ 33 %) over 2006 when the total was 5 797 in 64 countries and economies

Top 10 countries for ISO/IEC 27001:2005

Japan : 4 896

United Kingdom : 519

India : 508

Taipei, Chinese : 256

Italy : 148

China : 146

Germany : 135

USA : 94

Spain : 93

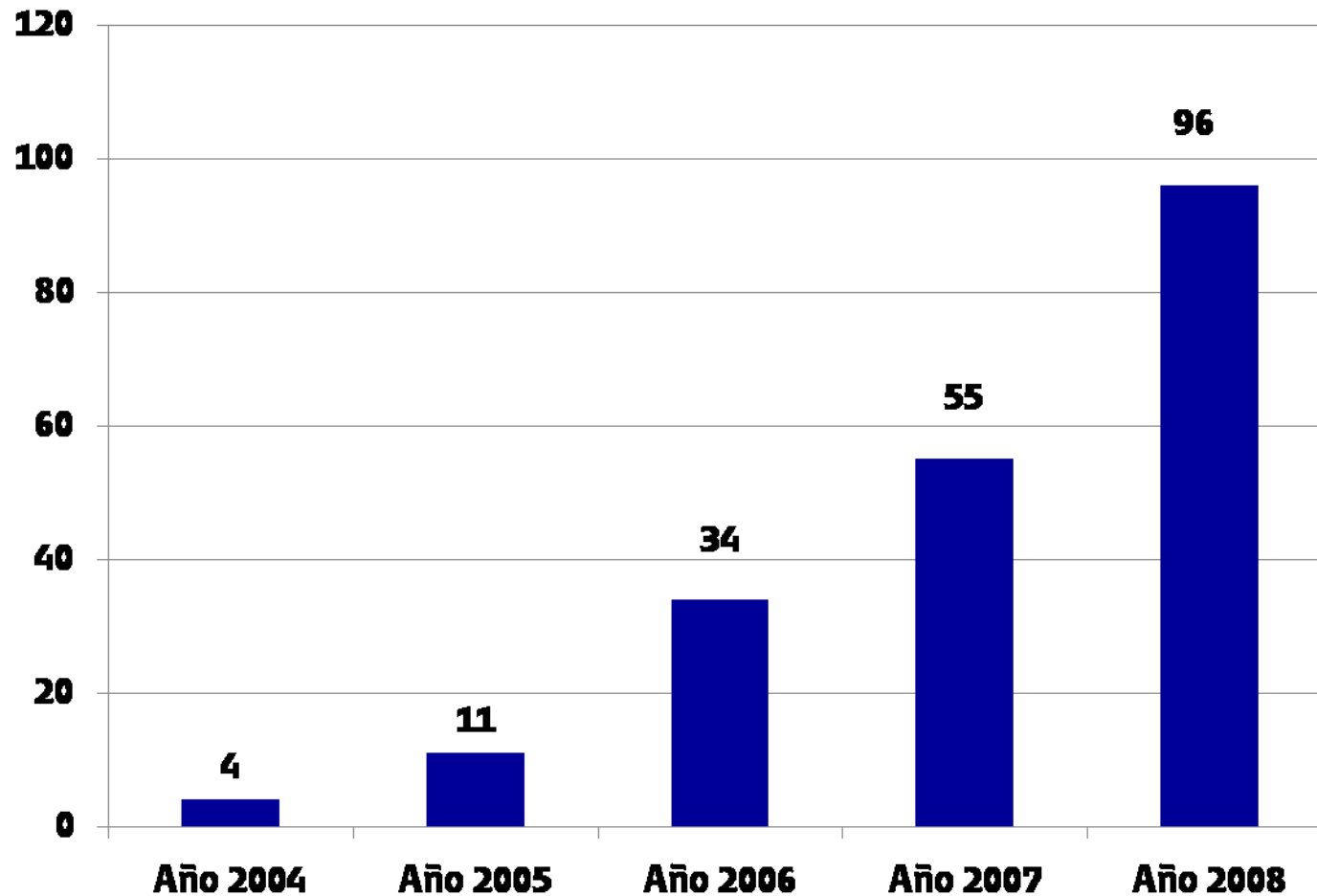
Hungary : 81

World results	Dec. 2006	Dec. 2007
World total	5 797	7 732
World growth	–	1 935
Number of countries/economies	64	70

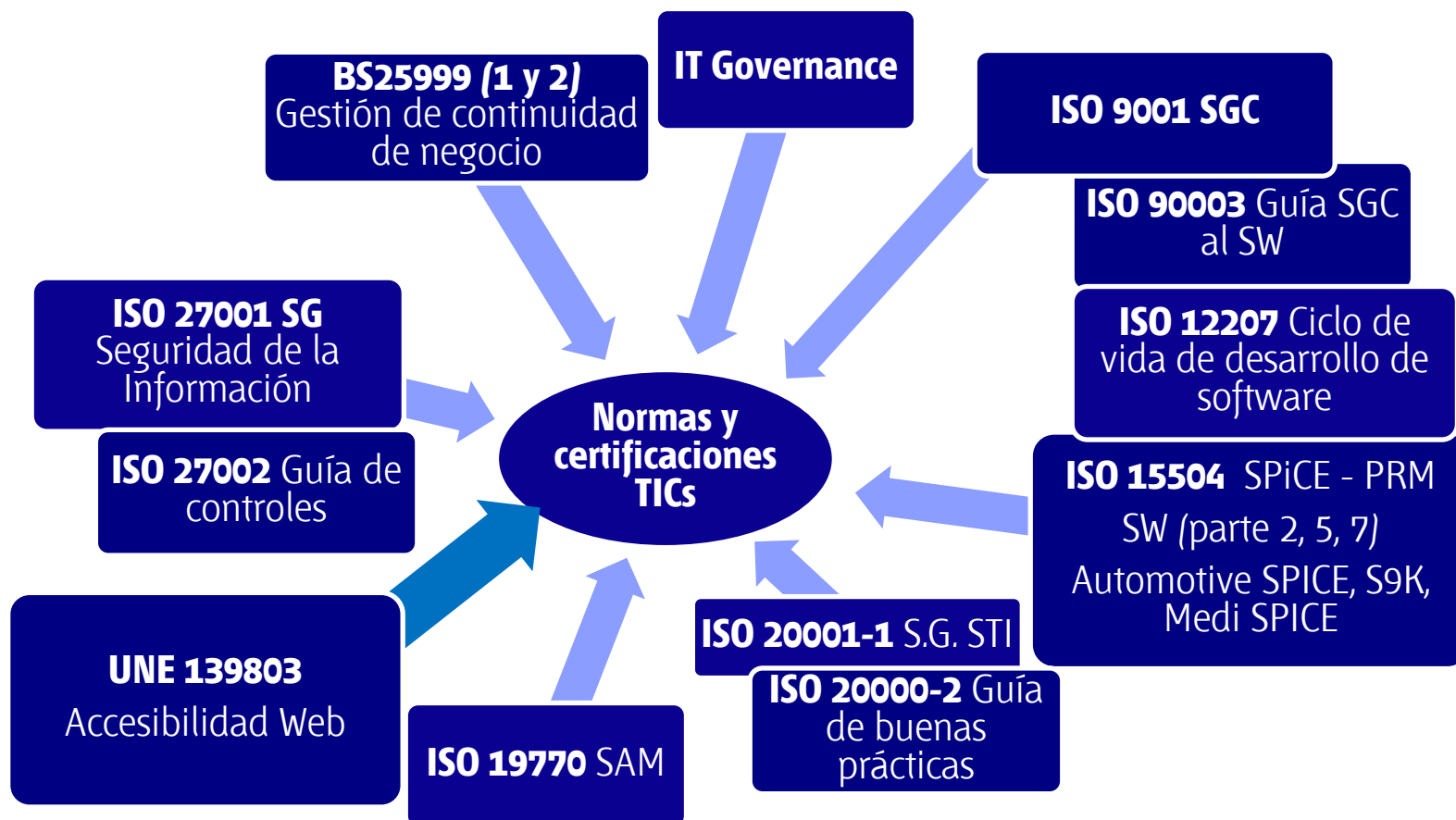
Europe

	Dec. 2006	Dec. 2007
Austria	16	23
Belgium	4	9
Bulgaria	–	8
Croatia	2	5
Czech Republic	27	77
Denmark	3	4
Estonia	–	1
Finland	1	14
France	5	9
Germany	95	135
Greece	3	5
Hungary	54	81
Iceland	10	11
Ireland	6	7
Italy	175	148
Lithuania	–	2
Luxembourg	1	2
Malta	–	1
Moldova, Republic of	1	1
Netherlands ¹	41	41

Certificados SGSI en AENOR



Certificaciones en las TIC en AENOR



Accesibilidad de sitios Web

La web ... es para todos, ... e independiente de

- el dispositivo de acceso (PC, teléfono, TV, PDA, ... ; el ancho de banda; el navegador, sin color, sin sonido, ... sin pantalla).
- Capacidades de los usuarios (dificultades visuales, auditivas, motoras, cognitivas, ... el cansancio, ...).
- La cultura o el conocimiento (textos, representaciones, ... formato de fechas,).

Tecnológicamente diversa,

contenidos diversos,

usuarios diversos

La web debe ser accesible

y usable

Accesibilidad de sitios Web. ¿Qué es?

W3C

La accesibilidad, aplicada a los sitios Web, permite el **acceso a la Web independientemente del tipo de hardware, software, infraestructura de red, idioma, localización geográfica y capacidades de los usuarios**. De esta manera, un sitio Web diseñado de manera que pueda ser utilizado con seguridad y eficacia por personas con discapacidad, se puede calificar de accesible.

Wikipedia:

La accesibilidad Web se refiere a la **capacidad de acceso a la Web y a sus contenidos** por todas las personas **independientemente** de la **discapacidad** (física, intelectual o técnica) que presenten o de las que se deriven del **contexto de uso** (tecnológicas o ambientales). Esta cualidad está íntimamente relacionada con la usabilidad.

- ✓ *Cubre la mayoría de las discapacidades (física, visual, auditiva y cognitiva) y las necesidades de las personas de edad avanzada.*
- ✓ *Incluso problemas de conexión lenta, navegadores anticuados, ausencia de dispositivos (ratón, teclado, ...)*

Marco legal

- **Real Decreto 1494/2007**, de 12 de noviembre, **Reglamento sobre las condiciones básicas** para el Acceso de las Personas con Discapacidad a las tecnologías, productos y servicios relacionados con la Sociedad de la Información y Medios de Comunicación Social.
- **Ley 49/2007**, de 26 de diciembre, establece el **régimen de infracciones y sanciones** en materia de Igualdad de Oportunidades, No Discriminación y Accesibilidad Universal de las personas con discapacidad.
- **Ley 56/2007**, de 28 de diciembre, de **Medidas de Impulso** de la Sociedad de la Información.
 - **Ley 51/2003**, de 2 de diciembre, de Igualdad de Oportunidades, No Discriminación y Accesibilidad Universal de las personas con discapacidad.
 - Legitimación individual y de las personas jurídicas para la defensa del derecho de igualdad de oportunidades.
 - Inversión de la carga de la prueba, ante graves indicios de discriminación por discapacidad .
 - **Ley 34/2002**, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

Páginas de Internet y sus contenidos de las

- **AAPP o Web de financiación pública** (diseño/ mantenimiento).
- **Entidades y empresas que se encarguen de gestionar servicios públicos.**
Especialmente las de carácter educativo sanitario y servicios sociales (incluyendo centros privados sostenidos, total o parcialmente, con fondos públicos).
- **Empresas que presten servicios al público en general de especial trascendencia económica:** (art. 2 L56/2007)
 - ✓ Comunicaciones electrónicas, financieros, suministro de agua, gas o electricidad, agencias de viajes, transporte de viajeros, actividades de comercio al por menor (podrán ampliarse a otras empresas que tengan interlocución telemática); y tengan
 - ✓ Más de 100 trabajadores o superen 6.010.121€ de operaciones anuales.
- Otros: oferta pública de contratación electrónica de transparencia garantizada, entre empresas;

L: Excepcionalmente, esta obligación no será aplicable cuando una funcionalidad o servicio no disponga de una solución tecnológica que permita su accesibilidad.

RD: Esta obligación no será aplicable cuando una información, funcionalidad o servicio no presente una alternativa tecnológica económicamente razonable y proporcionada que permita su accesibilidad.

- **Todas las páginas de internet**, actualmente existentes o de nueva creación, deberán cumplir la **prioridad 2** de la **Norma UNE 139803:2004** a partir del **31 de diciembre de 2008**.

Deber de informar sobre el grado de accesibilidad y la fecha de revisión; ofrecer un sistema de contacto, y evaluar periódicamente los resultados.

- Las **AAPP promoverán medidas de sensibilización, divulgación, educación** y, en especial, **formación** en el terreno de la accesibilidad para los titulares de otras páginas de Internet

- **A los efectos de este RD**, las páginas de Internet se podrán **certificar por una entidad de certificación** cuya competencia técnica haya sido reconocida por una entidad de acreditación. *(RD 2200/1995, Infraestructura para la calidad y seguridad industrial)*
... emplearán preferentemente normas técnicas españolas o europeas y, en su defecto, otras normas internacionales.
- Los **incumplimientos de accesibilidad** están sometidos al régimen de infracciones y sanciones de la LIONDAU, y Ley 49/2007
Infracción: acciones y omisiones ... incumplimiento de exigencias de accesibilidad y de realizar ajustes razonables
 - ✓ **graves** (incumplimiento de exigencias de accesibilidad, y la negativa a adoptar los ajustes razonables). De 30.000€ - 90.000€

Normativa oficial española

UNE 139803:2004

- Desarrollada en el CTN139/SC8. Secretariado por AENOR.
- Requerida por Legislación.
- Toma como referencia los puntos de verificación de las WCAG 1.0:
Nivel AA incorpora 3 puntos de verificación (identificar el idioma del documento, poner resúmenes a las tablas y mantener orden lógico del tabulador).
- Contiene 68 requisitos distribuidos en siete categorías, y se agrupan en función de su prioridad. Incluye tabla equivalencia con WCAG 1.0.

Estandares Internacionales del w3c:

- La legislación española no lo toma como referencia (w3c no es organismo oficial de normalización).
- Web Content Accessibility Guidelines (WCAG)
 - WCAG 1.0 – 5 de mayo de 1999. Organizada en 14 pautas, con 65 puntos de verificación - prioridad.
 - WCAG 2.0 – 11 de diciembre de 2008. Organizada en 4 principios ,12 directrices, 61 criterios de éxito.

UNE 139803:2004 Aplicaciones informáticas para personas con discapacidad. Requisitos de accesibilidad para contenidos en la Web.

Categorías:

1. **Principios Generales.** Aspectos globales relacionados con la tecnología usada para recoger contenidos en la Web.
2. **Presentación.** Manera de mostrar los contenidos: hojas de estilo, tablas, colores,
3. **Estructura.** Forma de organizar los contenidos.
4. **Contenido.** Requisitos acerca de los propios contenidos.
5. **Navegación.** Aspectos de recorrido entre los contenidos Web.
6. **Scripts, objetos de programación y multimedia.** Elementos dinámicos o interactivos.
7. **Situaciones excepcionales.** Imposibilidad de cumplimiento.

Niveles de conformidad / prioridad (1, 2 y 3).

No contempla el uso de logos, ni la declaración de conformidad.

norma española		UNE 139803
		Diciembre 2004
TÍTULO	Aplicaciones informáticas para personas con discapacidad Requisitos de accesibilidad para contenidos en la Web <small>Computer applications for people with disabilities. Web content accessibility requirements. Aplicaciones informáticas para las personas discapacitadas. Especificación de la accesibilidad a los contenidos Web.</small>	
CORRESPONDENCIA		
OBSERVACIONES		
ANTECEDENTES	Esta norma ha sido elaborada por el comité técnico AEN/CTN 139 Tecnologías de la Información y las Comunicaciones para la Salud cuya Secretaría desempeña AENOR.	
<small>Edición e impresión por AENOR. Deposito legal: M 52463-2004</small>	<small>LAS OBSERVACIONES A ESTE DOCUMENTO HAN DE DIRIGIRSE A: AENOR Asesoría Española de Normatización y Certificación C/ Génova, 5 28014 MADRID-España</small>	<small>Teléfono 91 432 40 00 Fax 91 201 40 32</small>
<small>© AENOR 2004 Reproducción prohibida</small>		<small>23 páginas Grupo 12</small>

Algunos ejemplos de requisitos

- Utilizar las tecnologías y pautas del W3C.
- Proporcionar alternativas equivalentes al contenido visual y auditivo.
- No basarse solo en el color.
- Crear tablas que se transformen correctamente.
- Utilizar de forma apropiada los marcadores y las hojas de estilos.
- Identificar el lenguaje natural usado.
- Asegurar que las páginas con nuevas tecnologías se transformen correctamente.
- Asegurar al usuario el control sobre los contenidos tempodependientes.
- Diseñar con independencia del dispositivo.
- Proporcionar información de contexto y orientación para ayudar a los usuarios a entender páginas o elementos complejos.
- Proporcionar mecanismos claros de navegación.
- Asegurarse de que los documentos sean claros y simples, para facilitar su comprensión.

Requisitos de accesibilidad para sitios web



**Norma UNE
139803:2004**



Referencia del RD 1494/2007

NIVEL BÁSICO

A

PRIORIDAD 1

El sitio Web **debe** satisfacer el requisito. En otro caso, será imposible para uno o más grupos de personas con discapacidad utilizar el sitio. *Básicos y obligatorios*

NIVEL MEDIO

AA

PRIORIDAD 2

El sitio Web **debería** satisfacer el requisito. En otro caso, será muy difícil para uno o más grupos de personas con discapacidad utilizar el sitio. *Barrera significativa*

NIVEL ALTO

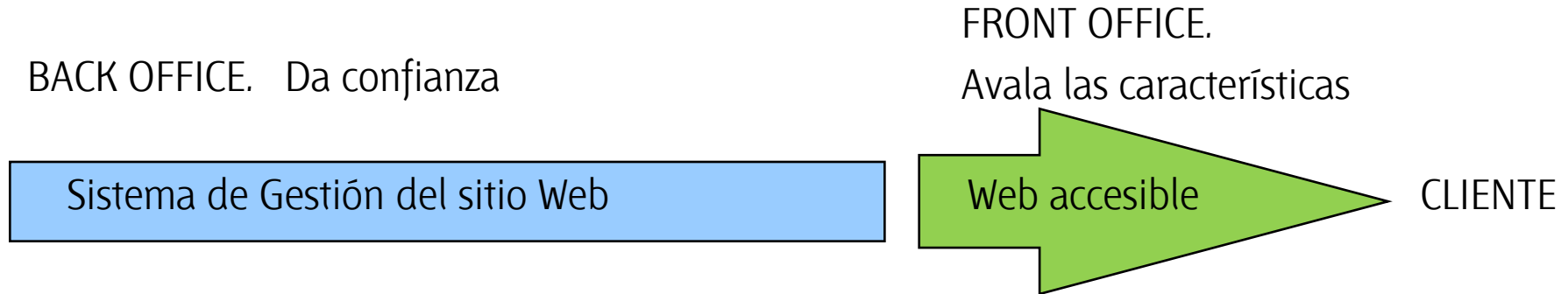
AAA

PRIORIDAD 3

El sitio Web **puede** satisfacer el requisito. En otro caso, algunos grupos podrían encontrar una dificultad relativa para utilizar el sitio. *Mejora*

Certificación accesibilidad Web. AENOR

¿Qué se certifica?




- ❑ El **Sistema de Gestión** debe ser conforme al **Anexo D del RP A90.01**.

- ❑ El **sitio Web** debe ser conforme a la norma **UNE 139803 “Requisitos de accesibilidad para contenidos Web”**. *(conforme pautas de la accesibilidad al contenido en la Web - WCAG)*

¿Quién certifica?

- ❑ Por 3ª parte: certifica **una organización independiente** con la necesaria competencia técnica.

Características de la certificación AENOR

- ✓ Se realiza **por tercera parte** independiente (asegura objetividad y rigor de las inspecciones).
- ✓ Certifica la **conformidad con la Norma UNE 139803** – *Requisitos de accesibilidad para contenidos Web*. Conformidad con **pautas de la accesibilidad de la WAI**.
- ✓ La certificación de AENOR **sólo admite los niveles de conformidad AA y AAA**.
- ✓ Requisitos **para el Sistema de gestión para la accesibilidad**.
- ✓ **Dos tipos de certificación** de accesibilidad: el **Certificado AENOR – Marca**  de Accesibilidad TIC, y el **Certificado de conformidad**.
- ✓ Establece una opción independiente para certificar la accesibilidad de los desarrollos / sitios Web.

Tipos de certificados AENOR

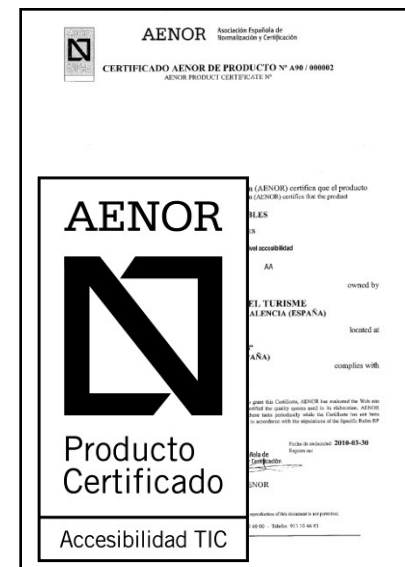
❑ Certificado de conformidad, sin seguimiento.

- * Refleja la accesibilidad del site en un momento dado.
- * Garantía para el desarrollador y cliente.
- * No lleva seguimiento.
- * No se audita el Sistema de Gestión.
- * Sólo se verifica la accesibilidad del site.
- * No se puede utilizar la marca AENOR ❑.



❑ Certificado con marca AENOR ❑

- * Refleja que el site se mantiene accesible de manera constante.
- * Certificado emitido para el propietario del sitio.
- * Garantiza al usuario que el sitio Web es accesible.
- * Verificaciones semestrales del sitio Web.
- * Auditorías anuales, al sistema de gestión (Anexo D).
- * Concesión del derecho de uso de la marca ❑ de AENOR de Accesibilidad.



Requisitos del Sistema de gestión. Marca

Anexo D, del Reglamento Particular AENOR A90.01

El Sistema de gestión debe asegurar en el tiempo la conformidad de la Web con los requisitos de la norma. Para ello, la organización ha de implantar un manual y los procedimientos necesarios para gestionar y evidenciar:

D.1 Gestión de los recursos

D.2 Elaboración y mantenimiento del sitio Web

D.3 Gestión de proveedores

D.4 Tratamiento de reclamaciones de clientes

Algunas notas de interés

22 sitios Web certificadas (AA - AAA) y varios desarrollos

<http://www.asturias.es>

[Gobierno del Principado de Asturias](#)

<http://www.zaragoza.es>

[Ayuntamiento de Zaragoza](#)

<http://www.bilbao.net/>

[Ayuntamiento de Bilbao](#)

<http://www.cajastur.es>

[Caja de Asturias](#)

<http://www.cites.es>

[Secretaría de Estado de Comercio \(AAA\)](#)

[Altia consultores, SL \(AAA\)](#)

...

Norma UNE 139803:2004 disponible en:

www.inteco.es



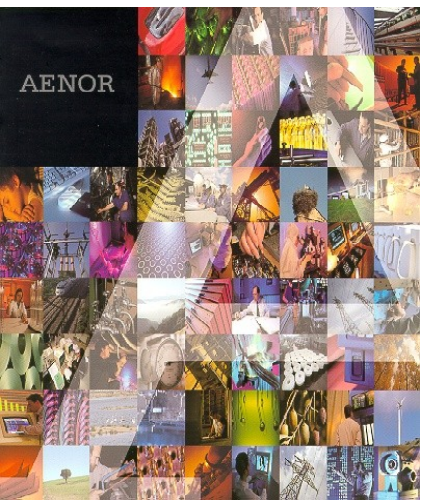
Reglamentos de certificación y más información en:

www.accesible.aenor.es

Solución a los Riesgos Empresariales,

Decisión estratégica de la organización

- Modelo para la definición, implementación, operación, revisión, mantenimiento y mejora del SG de la SI.
 - ✓ Sigue pautas de ISO 9001 e ISO 14001.
 - ✓ Para todo tipo de organizaciones.
 - ✓ En el marco de los riesgos empresariales generales.
 - ✓ Fin, seleccionar controles de seguridad, adecuados y proporcionados.
 - ✓ Enfoque por procesos, y para la mejora continua.



Factores que influyen en la Seguridad de los SI:

- Actualmente: Nueva York y en los 80's :
Mainframe – Ciudad de Ávila. Magerit
- Amplio uso de la Tecnología.
- Interconectividad de los sistemas. Sistemas abiertos y distribuidos.
- Cambios muy rápidos en las TICs.
- Ataques a Organizaciones. Tema atractivo?.
- Factores externos: Legislación .etc...

(Information Security Governance. 2001. IT Governance Institute).

En el ***World Economic Forums Annual – DAVOS meeting-SWISS RE*** informa de su estudio – encuesta a nivel mundial (60 entrevistas a senior executives en USA, Francia, Alemania, Italia, Japón y Reino Unido. Dic-2005).

- El **riesgo de los Ordenadores y las TICs** ocupa el primer lugar en 3 países (Japón, Reino Unido y USA), y en el top three de los otros países, para sus negocios.
- Como **herramienta primordial** para mitigar estos riesgos de SI indican el **Control Interno Informático**.

Informe de riesgos en las TICs

- Uno de cada 5 empleados deja a su familia y amigos usar sus portátiles corporativos para acceder a Internet. (21%).
- Uno de cada diez confiesa que baja algún tipo de contenido que no debiera mientras está en el trabajo.
- Dos tercios admiten tener conocimientos muy limitados en materia de seguridad.
- Un 5% dice que tienen acceso a áreas de la red corporativa que no deberían tener.

Fuente: **McAffee**.

Gestión de las TICs con criterios de Negocio.

Calidad en el servicio TICs y la Ingría. del Software

- Informe Penteo (2006):
 - Sólo un 21% de las cías gestionan el Dpto. de SI con criterios de negocio
 - 31 % gestionan el dpto. de SI sólo con criterios tecnológicos
 - 48 % gestionan con criterios híbridos
 - Conclusiones:
 - La Dirección de las cías. Tiene una percepción más positiva de los CIOs que siguen criterios de Negocio. Les dan el rol de líderes contribuidores de negocio en un 58%
 - La Gestión de las TICs mejora el posicionamiento del dpto. de SI y del CIO
 - En un futuro los CIOS más gestores y menos tecnólogos
- (Encuesta a: 85 Directores de TICs, 36 Dir. Generales y 12 Presidentes)

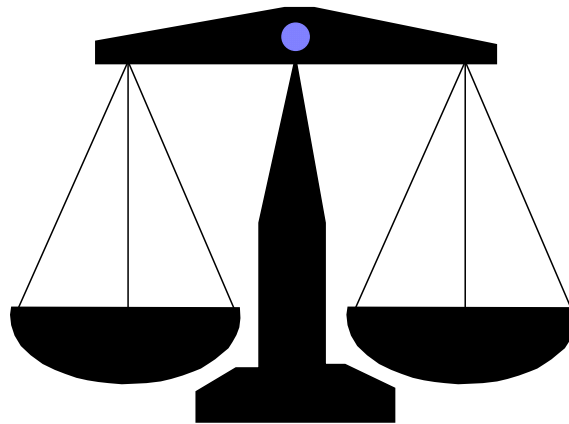
Para conducir y operar exitosamente una organización se requiere, que se

- salvaguarden los activos,
- mantenga la integridad de los datos e infraestructura,
- suministre información relevante y fiable,
- trabaje de forma eficiente,
- tengan dispuestos controles internos que aporten garantía razonable de que los objetivos de negocio se alcanzan.

Propiedades principales asociadas a la Información

DISPONIBILIDAD

Asegurar que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.



CONFIDENCIALIDAD

Asegurar que la información es accesible solo para aquellos autorizados a tener acceso.

INTEGRIDAD

Garantizar la exactitud y completitud de la información y los métodos de su proceso

La gestión eficaz de la **Seguridad de la Información** permite a la organización preservarlas.

El Sistema de Gestión de la SI

Es,

- Aquella **parte del sistema general de gestión** que comprende la política, la estructura organizativa, los procedimientos, los procesos, y los recursos necesarios para **implantar la gestión de la seguridad de la información**.
- La **herramienta de que dispone la Dirección** para implantar las políticas y objetivos de Seguridad de la Información.

Permite, establecer y reordenar la Seguridad de los Sistemas de Información en **concordancia con los Planes Estratégicos** de la Organización y con sus Políticas de Seguridad.

SGSI - UNE ISO 27001. MODELO PDCA

Definir **política** de seguridad
Establecer **alcance** del al SGSI
Realizar análisis de **riesgos**
Seleccionar los **controles**

“P”

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

ISO IEC 27002

1 Política de Seguridad de Información
2 Estructura organizativa de la SI
3 Clasificación y control de activos
4 Seguridad ligada al personal
5 Seguridad física y del entorno

6 Gestión de comunicaciones y operaciones
7 Control de accesos
8 Desarrollo y mantenimiento de sistemas
9 Gestión de Incidentes de Seguridad
10. Gestión Continuidad de Negocio
11 Conformidad y Cumplimiento legislación

“A”

“D”

“C”

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

Revisar internamente el SGSI
Realizar auditorias internas del SGSI

Gestión de riesgos – Implantación de controles

Procesos



Activos de SI

- Sistemas de información (aplicativos)
- Software
- Hardware
- Telecomunicaciones
- Personas

Análisis y Gestión de riesgos

$$R = F(X_1, X_2, X_3, X_n)$$

- Integridad (X_1)
- Confidencialidad (X_2)
- Disponibilidad (X_3)
- Amenazas (X_4)
- Vulnerabilidades (X_5)
- Impacto Económico (X_6)
- X_N

Riesgo Residual

Activo₁-----R'₁

Activo₂-----R'₂

Aplicando
ISO/IEC 27002
(Selección de
Controles)

Este Sistema **proporciona mecanismos para la salvaguarda:**

- De los Activos de Información.
- De los Sistemas que los procesan.

En concordancia con las políticas de Seguridad y planes estratégicos de la Organización.

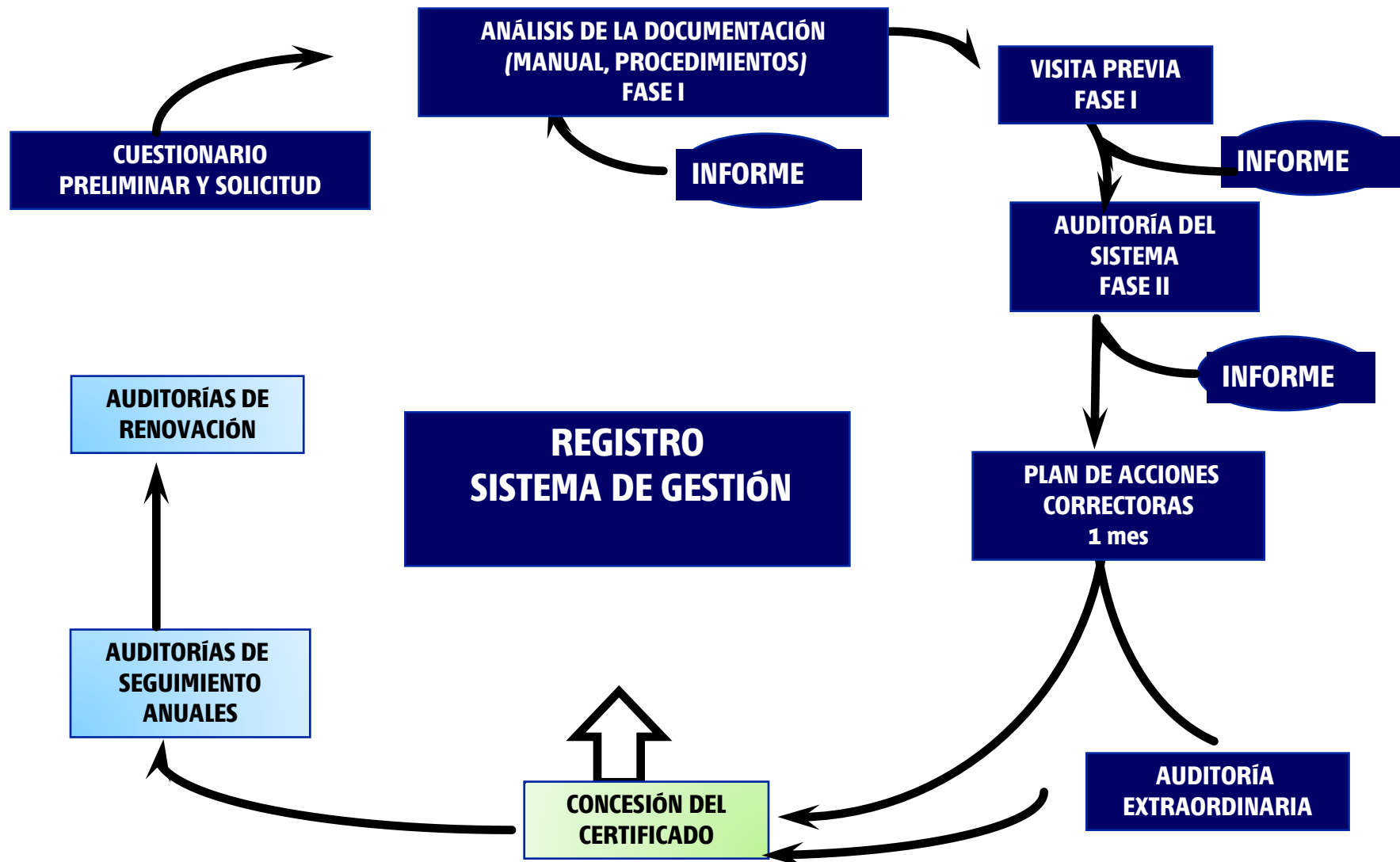
Es la **herramienta de que dispone la Dirección** para implantar las políticas y objetivos de Seguridad de la Información:

Integridad, confidencialidad y disponibilidad.

Factores críticos para el éxito

- Una seguridad **orientada al negocio**
- Implementar la Seguridad en **consonancia con la cultura de la empresa**
- **Apoyo** visible y compromiso de la **Dirección**.
- Buen **entendimiento** de los requisitos de seguridad, de la evaluación y gestión de los riesgos.
- **Convencer** de la necesidad de la seguridad a directivos y empleados.
- Proveer **formación** y guías sobre políticas y normas a toda la organización.
- Un **sistema de medición** para evaluar el rendimiento de la gestión de la seguridad y sugerir mejoras.

El proceso de certificación



Ventajas de certificar la Seguridad de la Información

- *Para el Negocio:*
 - **Integrar la gestión de la seguridad** de la información con otras modalidades de **gestión empresarial**
 - **Mejorar la imagen, confianza y competitividad empresarial.**
Certificación y reconocimiento por terceros.
 - **Comprobar su compromiso con el cumplimiento de la legislación:** protección de datos de carácter personal, servicios sociedad de información, comercio electrónico, propiedad intelectual, etc...
 - **Dar satisfacción a accionistas** y demostrar el valor añadido de las actividades de seguridad de la información en la empresa.

APORTA CONFIANZA A LOS SISTEMAS DE INFORMACIÓN

Ventajas de certificar la Seguridad de la Información

Para los Sistemas de Información:

- **Sistematizar** las actividades de SI
- **Ahorro de recursos** en las actividades de SI, mejorando la motivación e implicación de los empleados
- **Analizar riesgos:** identificar amenazas, vulnerabilidades e impactos en la actividad empresarial
- **Establecer objetivos** y metas que permitan aumentar el nivel de confianza en la seguridad
- **Planificar, organizar y estructurar** los recursos asignados a seguridad de la información
- **Identificar y clasificar los activos** de información

Ventajas de certificar la Seguridad de la Información

- **Seleccionar controles y dispositivos físicos y lógicos** adecuados a la estructura de la organización
- **Asegurar el nivel necesario** de disponibilidad, integridad, y confidencialidad de la información
- **Establecer planes** para adecuada gestión de la **continuidad del negocio**
- **Establecer procesos** y actividades de **revisión, mejora continua y auditoría** de la gestión y tratamiento de la información

Otras certificaciones. Multisectoriales / Calidad

– EFQM

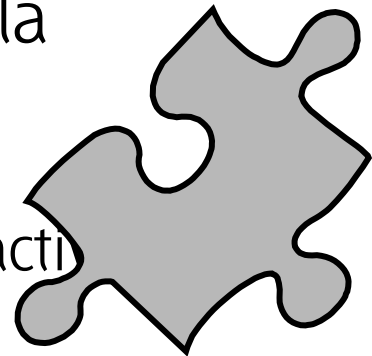


- Modelo europeo de excelencia.
- Dirigido a todos los sectores.
- Herramienta de autoevaluación, guía para la mejora.
- Agentes – Resultados (clientes, accionistas, personal, sociedad).



– **UNE EN ISO 9001** - Sistema de Gestión de la Calidad. ... *UNE EN ISO 9004*

- Modelo internacional ISO. Acreditación.
- Genérico (cualquier organización, sectores de actividad)
 - ISO 90003 – guía aplicación ISO 9001 al software.
 - ISO 12207 – ciclo de vida del software



- Único certificable, en la serie de normas ISO 9000 (14).
- Integrable con otros esquemas ISO. Lenguaje común...

Otras certificaciones. Procesos / servicios TIC

– **SGSTI- UNE-ISO 20000:**



- Sistema de Gestión de TI.
- Calidad en la Gestión de servicios de TICs a la empresa o clientes.(CPD externo o CPD interno).
- Modelo PDCA.
- Basado en las librerías ITIL.

– **SGSI –UNE ISO 27001:**



- Sistema de Gestión de la Seguridad de la Información.
- Premio revista SIC a mejor labor en Seguridad de SI. 2006.
- Mas de 100 empresas certificadas, en todos los sectores.

– **SPICE – ISO 15504 :**

- Modelo de madurez del desarrollo de software. Evaluación por niveles.
- Modelo ISO – Modelo de Procesos de Referencia
 - **ISO 12207** : Ciclo de Vida de Desarrollo de Software. Fases en la creación de un software.
 - ...
- Es la competencia a CMMI.
- **Plan Avanza**

– **SAM (Software Asset Mangement) ISO 19770 :**

- El software como activo. Fase Inicial. Traducción norma.
- Proyecto BSA . España y LatinoAmerica.

Otras certificaciones TIC



- **Marca AENOR de Buenas Prácticas Comerciales para el Comercio Electrónico**



- **Certificado AENOR de Sistemas de Gestión de Software Original**

MUCHAS GRACIAS

D. José Angel Valderrama Antón
Gerente de Nuevas Tecnologías
AENOR

www.aenor.es
www.accesible.aenor.es

Tel. 902 102 201 /
91 432 61 05

Fax: 91 319 05 81

c/ Génova, 6
28004 Madrid

nuevastecnologias@aeonr.es

AENOR Asociación Española de
Normalización y Certificación