Organiza

AEC

XXIII Congreso de Calidad en la Automoción

Calidad y Conectividad

Zaragoza, 4 y 5 de octubre de 2018

Estándares internacionales y su Certificación en la Transformación Digital, Ciberseguridad y Privacidad

Octubre - 2018

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

AENOR

AGENDA

1. AENOR EN EL MUNDO

2. MODELO AENOR DE ISO EN LAS TICS. RIESGOS DE LAS TICs Y SOLUCIONES.

3. ECOSISTEMA DE CIBERSEGURIDAD&PRIVACIDAD DE AENOR. *ISO 27032 – Guidelines for Cybersecurity*

4. SISTEMA GESTION DE SEGURIDAD DE LA INFORMACION – ISO 27001. Un "*commodity*"

5. CASOS DE ÉXITO ISO 27001 EN EL SECTOR AUTOMOCION

6. TESTIMONIALES Y BIBLIOGRAFIA

AENOR

1. AENOR EN EL MUNDO

Desde Enero 2017 – AENOR INTERNACIONAL SAU
Separación en Certificación y Normalización ***(UNE)***

Hasta 2016 Asociación privada de Normalización y Certificación sin ánimo de lucro
AENOR es el representante de ISO en España y algunos países de Latinoamérica.
Constitución: 1986. Real decreto 2200/95
AENOR Corporación
AENOR INTERNACIONAL *(*12 filiales – Europa y Latam*)*
AENOR México *(* +10 años en México DF y Delegaciones*)*
Multisectorial
Normalización
Certificación productos, servicios, sistemas de gestión y personal
Servicios de Formación
AENOR es miembro de IQNET

AENOR

2. Modelo dinámico de ISO para las TICs

Según ISACA (*):

La ***ciberseguridad***, se ocupa de la protección de los **activos digitales** , desde las redes al hardware y la información que es procesada, almacenada o transportada a través los **sistemas de información interconectados.**

(*)*: ISACA – CSX – Cibersecurity Fundamentals Study Guide*

2. Modelo dinámico de ISO para las TICs

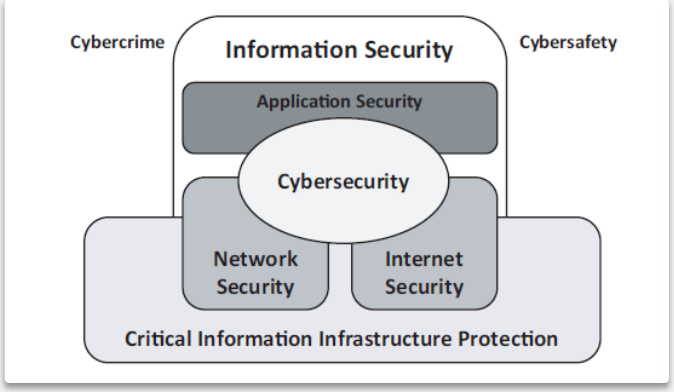
ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity

La **ciberseguridad** es la seguridad en el **ciberespacio**.

El **ciberespacio** es un mundo virtual que contiene los entornos de internet, personas, organizaciones, actividades y toda clase de tecnología, dispositivos y redes interconectados entre si (ISO 27032)

La ciberseguridad es la seguridad en un mundo digital-virtual, para **prevenir** los ciberataques que provienen de **nuevas amenazas y riesgos**.

(Carlos Manuel Fdez. & Boris Delgado - AENOR)



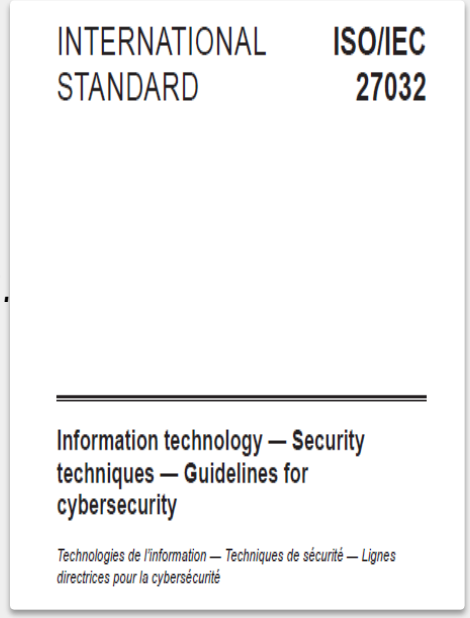
Fuente: ISO 27032 – Relación entre Ciberseguridad y otros dominios de seguridad

AENOR

2. Modelo dinámico de ISO para las TICs

En la ISO 27032 se abordan riesgos y amenazas específicas de ciberseguridad:

- ✓ los ataques de ingeniería social.
- ✓ El acceso secreto y no autorizado a sistemas informáticos (***Hacking***);
- ✓ La proliferación de software malicioso (***Malware***);
- ✓ El software espía (***Spyware***);
- ✓ Otros tipos de software potencialmente no deseables (***Ransomware***).
- ✓ Amenazas Persistentes (***APTs***)



Y propone controles:

- ✓ Controles a nivel de aplicaciones (SW seguro)
- ✓ Controles para la protección de Servidores (Hardening)
- ✓ Controles para usuario final (end-user) e ingeniería social

Propone un marco para proveedores/clientes:

- ✓ **Compartir información** (colaboración segura y confiable, que también proteja la privacidad de las partes implicadas)
- ✓ Coordinación y **gestión de incidentes (CERT y SOC). Por ejemplo INCIBE, CCN-CERT, etc.**

AENOR

2. La solución: el Modelo dinámico de ISO para las TICs

La empresa y su continuidad según procesos críticos

Objetivo: Gobierno y Gestión de las TICs con estándares ISO.

Funciones del CIO

Calidad y seguridad en servicios de TI (el día a día)

Creación de Software

SGCN
ISO 22301
Sistema de Gestión Continuidad del Negocio

Gobierno de TI
ISO 38500
IT Governance

Desarrollo de Software ⟷ **DEVOPS** ⟷ **Operaciones / Servicios**

Nivel de Madurez. Ciclo de Vida de SW
SPICE ISO 33000
Modelo de Evaluación, Mejora y Madurez de Software

ISO 12207
Ciclo de Vida de Desarrollo de Software

ISO 25000
Calidad del Producto Software

SGSTI
ISO 20000-1
Sistema de Gestión Servicios TI

ISO 20000-2
Guía de Buenas Prácticas

SGSI
ISO 27001
Sistema de Gestión Seguridad de la Información

ISO 27002
Guía de Controles

Adicionalmente:

- **SGSI – ENS - Esquema Nacional de Seguridad**
- **Reglamento UE 910/2014 – Prestadores de Servicios de Confianza - eIDAS**
- BPCE – Buenas Prácticas Comercio Electrónico
- SGSI – SCADA

Datacenter Green. Sostenibilidad Energética en CPDs- SE CPD-

NOTA: desde 2004 certificando SGSI/ISO 27001. +400 empresas certificadas

Nota: tiene PDCA / Control interno Tecnologías de Información

AENOR

2. RIESGOS DE LAS TICs Y SUS SOLUCIONES
Solución a los Riesgos en el Modelo de ISO en las TICs

- Riesgos en Seguridad SI **ISO 27001 - ENS**

- Perdida de integridad en la información.
- Suplantación de identidad/Mal uso de roles.
- Intrusión en los sistemas de información.
- Denegación de Servicio *(DoS)*.
- Fuga de Información.
- Riesgo de malware *(virus, troyanos, APTs, etc.)*

- Riesgos en Servicios TI **ISO 20000-1**

- Servicios de TI no definidos, y sin compromiso
- Incumplimiento de los SLAs *(*Acuerdos de nivel de servicio*)*.
- Servicios con un mayor coste.
- Pérdida del servicio, y lentitud en la recuperación.

- Riesgos Desarrollo SW ***(ISO 33000-SPICE)***

- No cumplir con requisitos de usuario.
- No cumplimiento de la planificación del proyecto.
- Usuario no prueba antes de entrega final.
- **No trazabilidad de requisitos de usuario hasta código fuente**

2. RIESGOS DE LAS TICs Y SUS SOLUCIONES
Solución a los Riesgos en el Modelo de ISO en las TICs

- Riesgos en Gobierno de TI **ISO 38500**

- No cumplimiento plan de TICs / Business Plan
- Incumplimiento legal.
- Personal no motivado.
- Compras de TI no alineadas con las necesidades del negocio. Costes excesivos

- Riesgos en Continuidad de Negocio **ISO 22301**

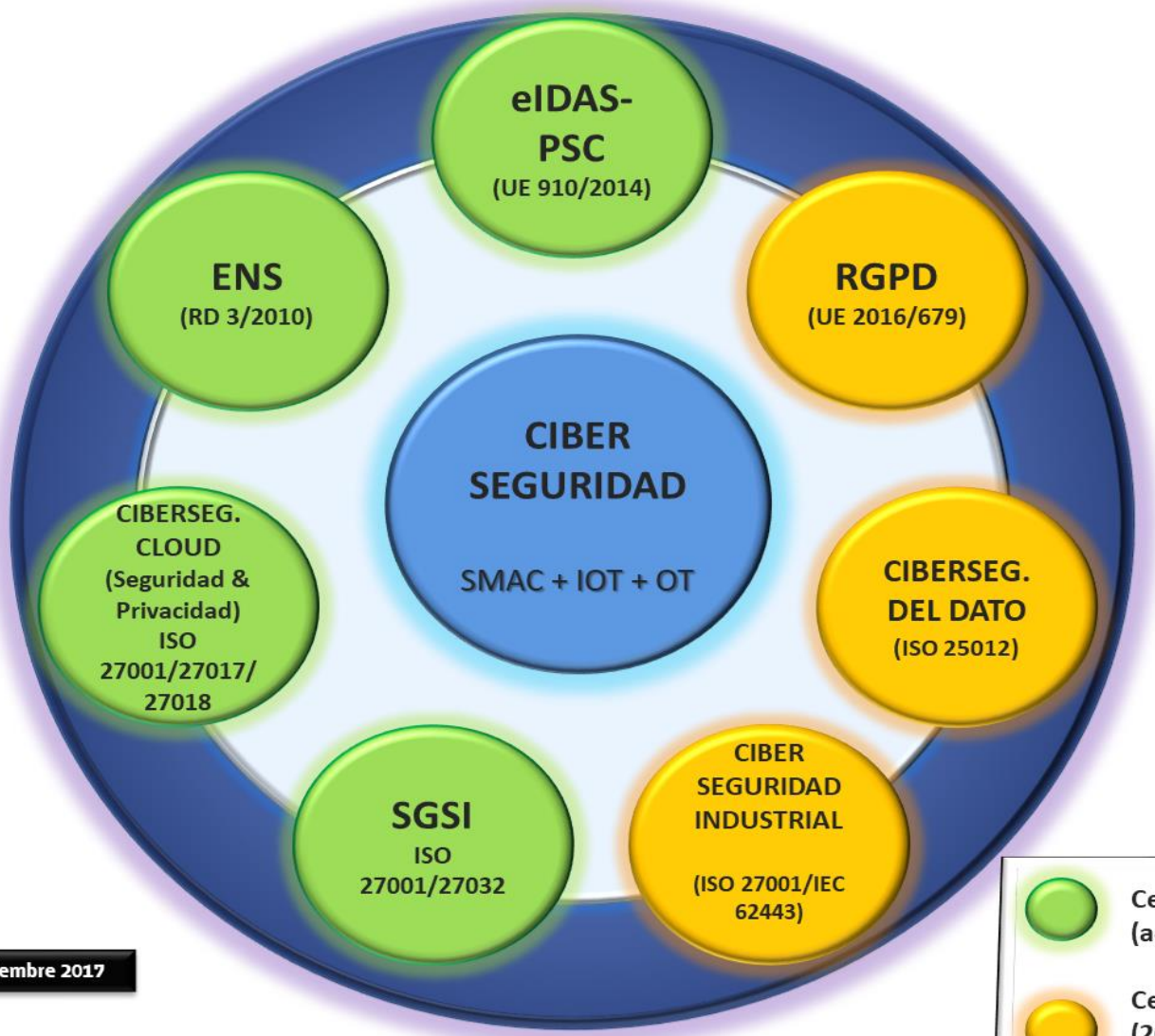
- Desaparición de la empresa. Después de un desastre natural ó provocado ó negligencia.
- No existe **resiliencia** ante un desastre o incidentes graves
- No se identifican procesos críticos.

- Riesgos en Producto SW **ISO 25000**

- No cumple con la funcionalidad prevista
- Costes de mantenimiento desorbitados.
- Complejidad del software

AENOR

3. ECOSISTEMA. Ciberseguridad&Privacidad



Feunte: AENOR-TIC: Septiembre 2017

AENOR

3. Modelo dinámico de ISO para las TICs

AENOR está acreditada por ENAC en:

- *ISO 27001 (a nivel mundial)*
- *PSC (Europa – Reglamento UE 910|2014 eIDAS),*
- *Esquema Nacional de Seguridad (España- RD 3|2010)*

conforme a ISO 17021, ISO 27006 e ISO 17065

Es por ello que estamos en las mejores condiciones para certificar RGPD y que por supuesto seremos entidad certificadora para el RGPD

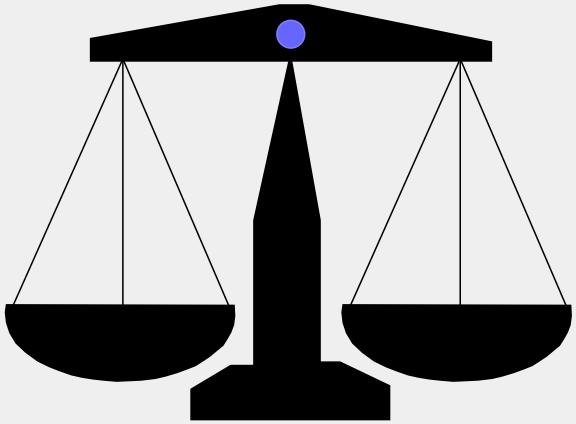
AENOR

ENAC
Entidad Nacional de Acreditación

4. SGSI - UNE ISO/IEC 27001:2014. DIMENSIONES DE SEGURIDAD

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.

- → **Re-ordenar la seguridad**
- → **Cumplimiento normativo-legal en Europa y LATAM *(p.e. RGPD en Europa, LOPD en Perú, México, etc.)***

AENOR

4. SGSI - UNE ISO/IEC 27001:2014. 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**

A

ISO IEC 27002 / Anexo A. ISO IEC 27001	
A.5 Política de Seguridad de Información A.6 Organización de la Seguridad de la información A.7 Seguridad en los RRHH A.8 Gestión de Activos A.9 Control de Accesos A.10 Criptografía A.11 Seguridad Física y ambiental A.12 Seguridad en las operaciones	A.13 Seguridad en las comunicaciones A.14 Adquisición, desarrollo y mantenimiento de sistemas A15 Relación con proveedores A.16. Gestión de incidentes de seguridad A.17 Aspectos de Seguridad de la información dentro de continuidad de negocio A.18 Conformidad

D

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

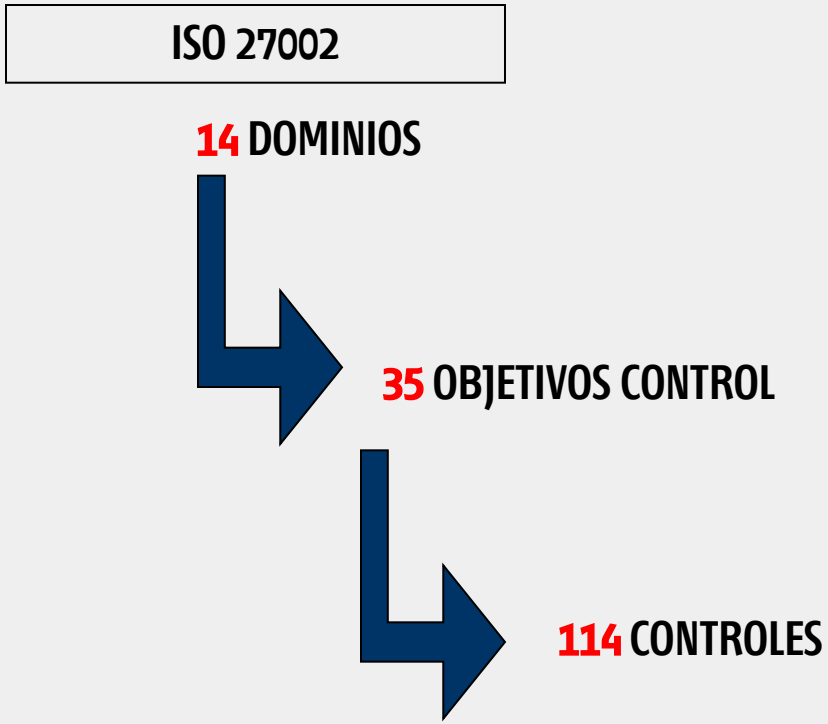
C

Revisar internamente el SGSI
Realizar **auditorias internas** del SGSI
Indicadores y Métricas
Revisión por Dirección

AENOR

UNE-ISO 27002:2014 (Anexo A. ISO 27001:2014)

- Cada área o dominio tiene asociados uno o varios objetivos de seguridad.
- Para cada objetivo se definen, a su vez, uno o más controles de seguridad cuya implantación debe traducirse en la consecución del objetivo de seguridad asociado



ISO 27002:2013 DOMINIO		Total controles
A5	Política de Seguridad de la Información	2
A6	Organización de la seguridad de la información	7
A7	Seguridad de los RRHH	6
A8	Gestión de activos	10
A9	Control de accesos	14
A10	Criptografía	2
A11	Seguridad física y ambiental	15
A12	Seguridad en las operaciones	14
A13	Seguridad en las comunicaciones	7
A14	Adquisición, desarrollo y mantenimiento de los sistemas de información	13
A15	Relaciones con proveedores	5
A16	Gestión de incidentes de seguridad de la información	7
A17	Aspectos de seguridad de la información en continuidad de negocio	4
A18	Cumplimiento	8
	TOTAL	114

5. Proceso de Certificación según ISO 17021/ISO 27006

Audit Partner : Mentoring y Benchmarking

6. Casos de Éxito en ISO 27001 - Automoción

AENOR

Information Security Management System Certificate

AENOR

Seguridad Información

ISO/IEC 27001

SI-

AENOR certifica que la organización

FICOSA INT

has an information security management syst

for the activities: The ope Clea logi prod mar curr

which is/are carried out in: NIL BUR

First issued on: 201
Validity date: 202

AENOR INTERNACIONAL S.A.U.
Génova, 6. 28004 Madrid. España
Tel. 91 432 60 00.- www.aenor.com

AENOR

Certificado del Sistema de Gestión de Seguridad de la Información

AENOR

Seguridad Información

ISO/IEC 27001

SI-0023/2018

AENOR certifica que la organización

GRUPO ANTOLIN INGENIERÍA, S.A.

dispone de un sistema de gestión de seguridad de la información conforme con la Norma UNE-ISO/IEC 27001:2014

para las actividades: El SGSI para los servicios y procesos que soportan el diseño, desarrollo y producción de piezas protofipo para la industria de la automoción, según la declaración de aplicabilidad en vigor a la fecha de emisión del certificado.

que se realizan en: CR NACIONAL I, KM. 244,8. 09007 - BURGOS

Fecha de primera emisión: 2018-06-21
Fecha de expiración: 2021-06-21

Rafael GARCÍA MEIRO
Director General

AENOR INTERNACIONAL S.A.U.
Génova, 6. 28004 Madrid. España
Tel. 91 432 60 00.- www.aenor.com

ENAC

IQNet

IQNet

THE INTERNATIONAL CERTIFICATION NETWORK

CERTIFICATE

IQNet and
AENOR
hereby certify that the organization

GRUPO ANTOLIN INGENIERÍA, S.A.

CR NACIONAL I, KM. 244,8.
09007 - BURGOS

for the following field of activities

ISMS for services and processes supporting design, development and prototyp
the Statement of Aplicability to the issue

has implemented and m

Information Security Mana

which fulfills the requirements of th

ISO/IEC 2700

First issued on: 2018-06-21

Registration Number: E

IQNet

Michael Drechsel
President of IQNet

Rafae
Chief

IQNet Partners*:
AENOR Spain AFNOR Certification France AIB-Vincotte International
CISQ Italy CQC China CQM China CQS Czech Republic Cro
FCAV Brazil FONDONORMA Venezuela ICONTEC Colombia IMNC M
JQA Japan KFQ Korea MIRTEC Greece MSZT Hungary Nem
Quality Austria Austria RR Russia SII Israel SIQ Slove
SQS Switzerland SRAC Romania TEST St Petersburg
IQNet is represented in the USA by: AFNOR Certification, C
* The list of IQNet partners is valid at the time of issue of this certificate. Updated in

IQNet

THE INTERNATIONAL CERTIFICATION NETWORK

CERTIFICATE

IQNet and
AENOR
hereby certify that the organization

FICOSA INTERNATIONAL S.A.

NILÜFER ORGANIZE SAN BOL. AKASYA CAD. N° 4 NILUFER.
16140 - BURSA
Turquia

for the following field of activities

The information systems that support customs and foreign trade operations of the company such as import, export, transit and custom clearance; the electronic information of assets of the activities such as logistic, warehousing, accountancy, finance, HR and information processing related to these operations and the information security management system used to protect these assets in accordance with the current statement of applicability

has implemented and maintains a

Information Security Management System

which fulfills the requirements of the following standard

ISO/IEC 27001:2013

First issued on: 2017-08-04 Validity date: 2020-08-04

Registration Number: ES-SI-0034/2017

IQNet

AENOR

Michael Drechsel
President of IQNet

Rafael García
General Manager

IQNet Partners*:
AENOR Spain AFNOR Certification France AIB-Vincotte International Belgium AHCE Mexico APCER Portugal CCC Cyprus
CISQ Italy CQC China CQM China CQS Czech Republic Cro Cert Croatia DQS Holding GmbH Germany
FCAV Brazil FONDONORMA Venezuela ICONTEC Colombia IMNC Mexico Inspecta Certification Finland IRAM Argentina
JQA Japan KFQ Korea MIRTEC Greece MSZT Hungary Nemko AS Norway NSAI Poland PCBC Poland
Quality Austria Austria RR Russia SII Israel SIQ Slovenia SIRIM QAS International Malaysia
SQS Switzerland SRAC Romania TEST St Petersburg Russia TSE Turkey YUQS Serbia
IQNet is represented in the USA by AFNOR Certification, CISQ, DQS Holding GmbH and NSAI Inc.
* The list of IQNet partners is valid at the time of issue of this certificate. Updated information is available under www.iqnet-certification.com

AENOR

6. Testimoniales del Modelo de AENOR

ISO 27001

Luís Lopes
Director Técnico
CESCE Soluçoes Informatica. Portugal del Grupo SIA España

"Tenemos un análisis de riesgos totalmente adaptado a nuestras necesidades"

ISO 20000-1

Luis Manuel Ortiz
Director Comercial
TI América. México

"La certificación garantiza a los clientes que nuestros servicios se rigen por las mejores prácticas"

SPICE-ISO 33000/ISO 12207

Maximino Álvarez
Director General
Xtream . España

"Base de nuestro crecimiento internacional"

ISO 33000 + ISO 25000

Luis Montalban
CEO
BITWARE. España

"La aplicación conjunta de ISO 33000 e ISO 25000 ha supuesto una mejora en la productividad y un ahorro de costes en el mantenimiento del 60% en el software

ENS

Carlos Carnicer
Presidente Consejo General de la Abogacía Española

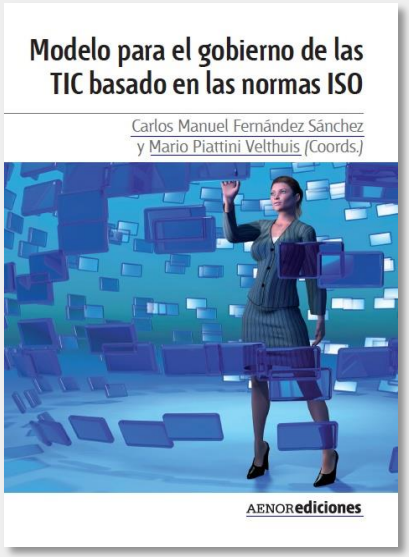
"Los ciudadanos pueden confiar en que sus datos se gestionan con garantías de seguridad"

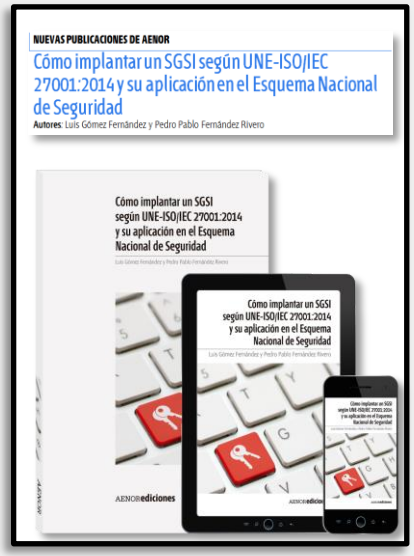
ISO 22301

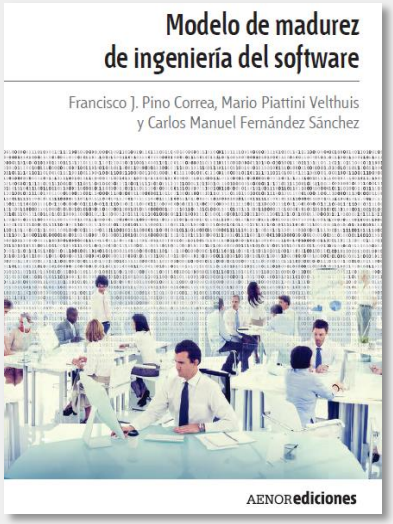
Cristo M. Pérez Rosquete
Área de Seguridad Informática
Sanitas. España

"Para continuar cuidando"

6. HERRAMIENTAS: Bibliografía AENOR TICs





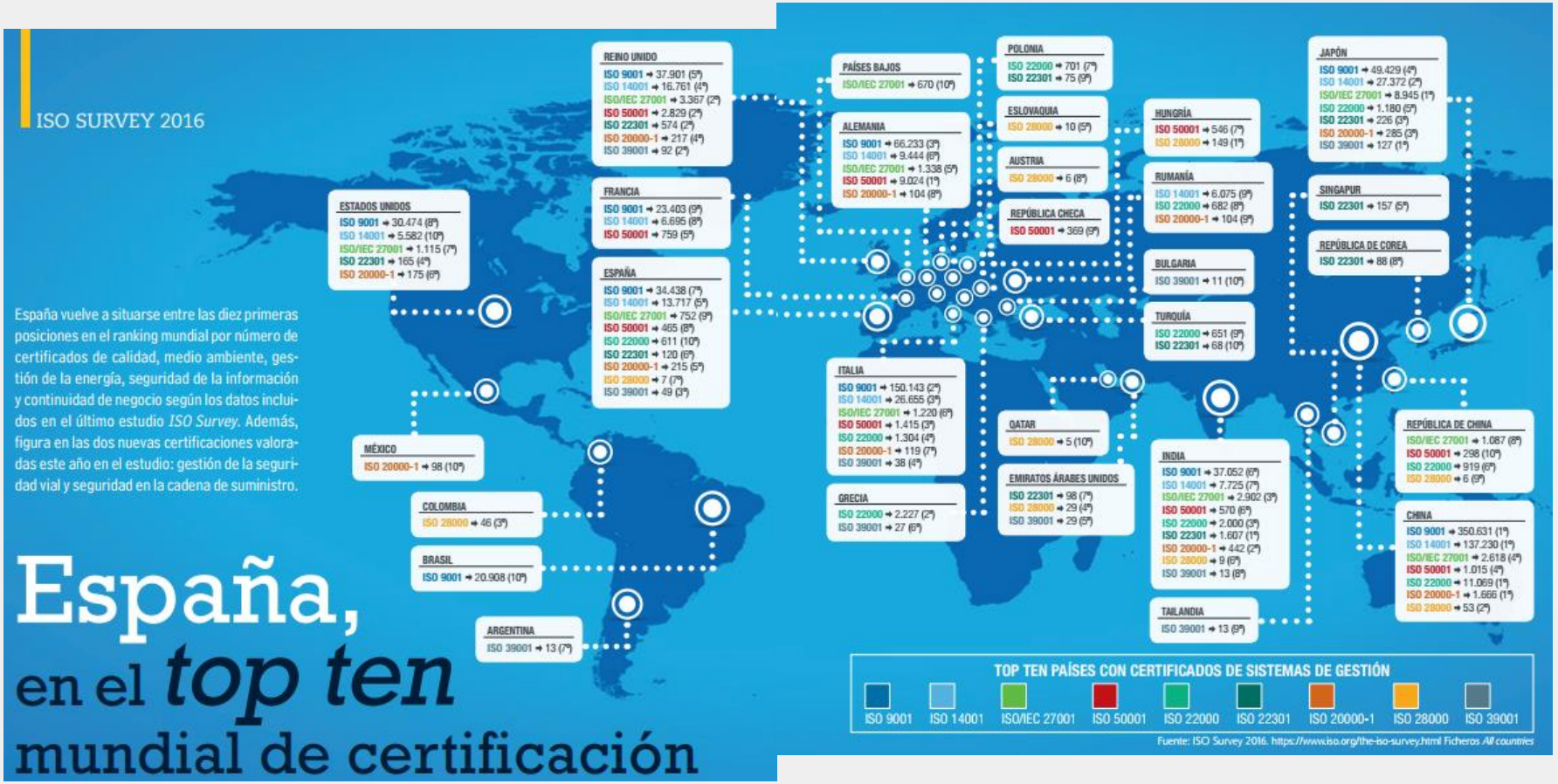


https://www.aenor.com/normas-y-libros/la-editorial

https://revista.aenor.com/

https://www.ciberseguridadaenor.com

ISO SURVEY 2016/2017 – ESPAÑA en el TOP TEN (ISO 27001 e ISO 20000-1)



AENOR líder en ISO 27001, con + 60% en España, Latam, USA y Europa

AENOR

Muchas gracias por su atención

"La Ciberseguridad & Privacidad con estándares ISO aportan:
Confianza en el nuevo ecosistema de Transformación Digital *(SMAC+IoT+OT)*".

En conclusión:
¿Dormirá tranquilo el/la CEO, CIO, CDO, DPO, … ?

Muchas gracias a tod@s por vuestra atención

AENOR INTERNACIONAL SAU
Paseo Sagasta, 72 - entlo. dcha.
50006 ZARAGOZA
Tel.976 259 680
dar@aenor.com

Boris DELGADO. RISS CISA, CISM
Gerente de TIC
bdelgado@aenor.com
Ana MARTÍNEZ DEL AMO
Desarrollo de Negocio
amartinezd@aenor.com

AENOR