

XIII JORNADAS STIC CCN-CERT



ENS x Provincia



**Diputación
de Burgos**



cibergob

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCCNCERT



ens

Esquema Nacional de
Seguridad



ens

Esquema Nacional de
Seguridad



Madrid
(>3M hab.)



Jaramillo Quemado
(8 hab.)



San Mamés
de Burgos
(aprox. 300 hab.)



Zaragoza
(>670K hab.)



Burgos
(>175K hab.)



Tardajos
(aprox. 780 hab.)



Cumplimiento ENS/RGPD → *Dinámica actual*



Cumplimiento del ENS/RGPD → Dinámica actual





MEDIDAS ORGANIZATIVAS

MEDIDAS TECNOLÓGICAS

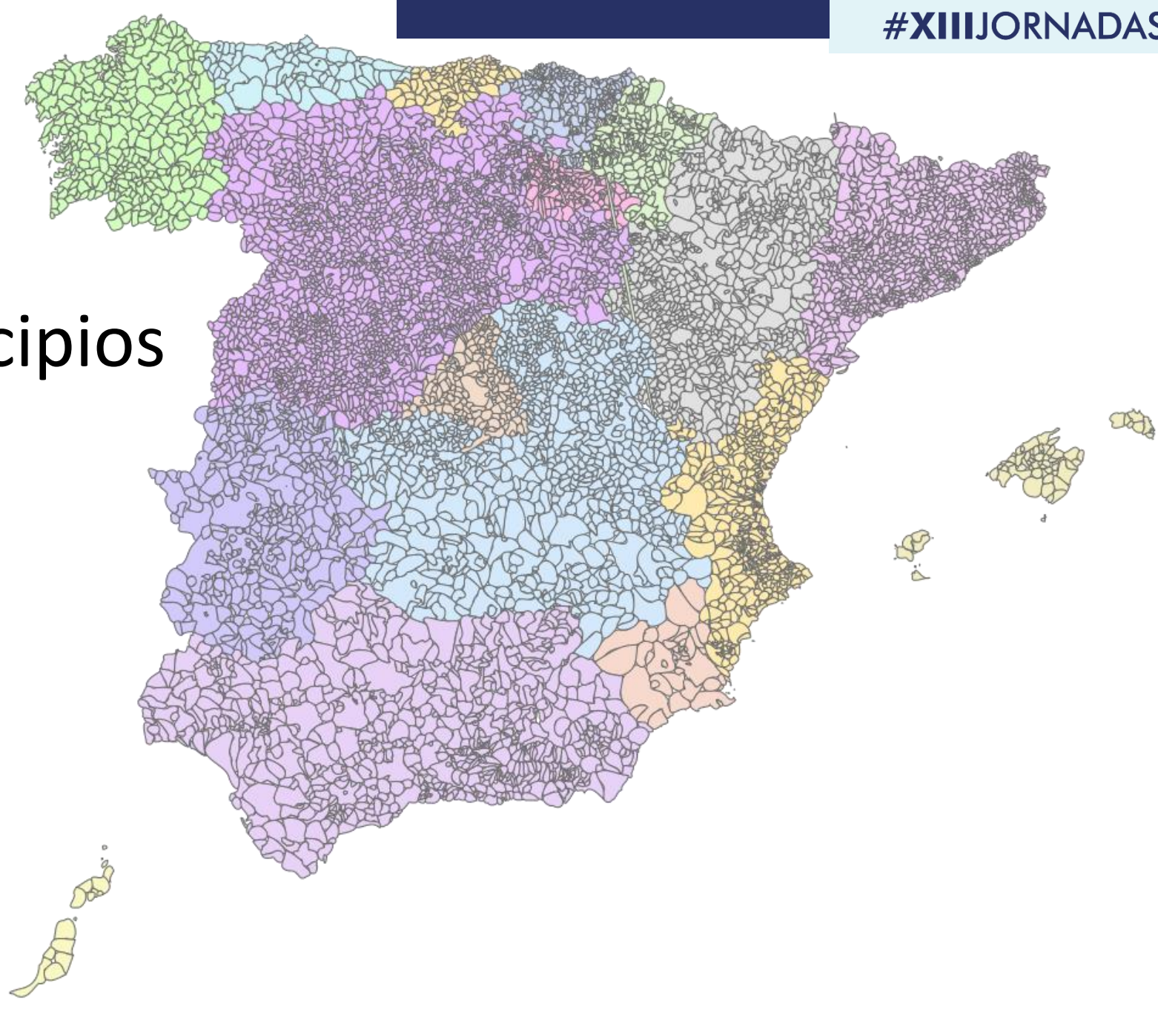
 **ens**

Esquema Nacional de
Seguridad



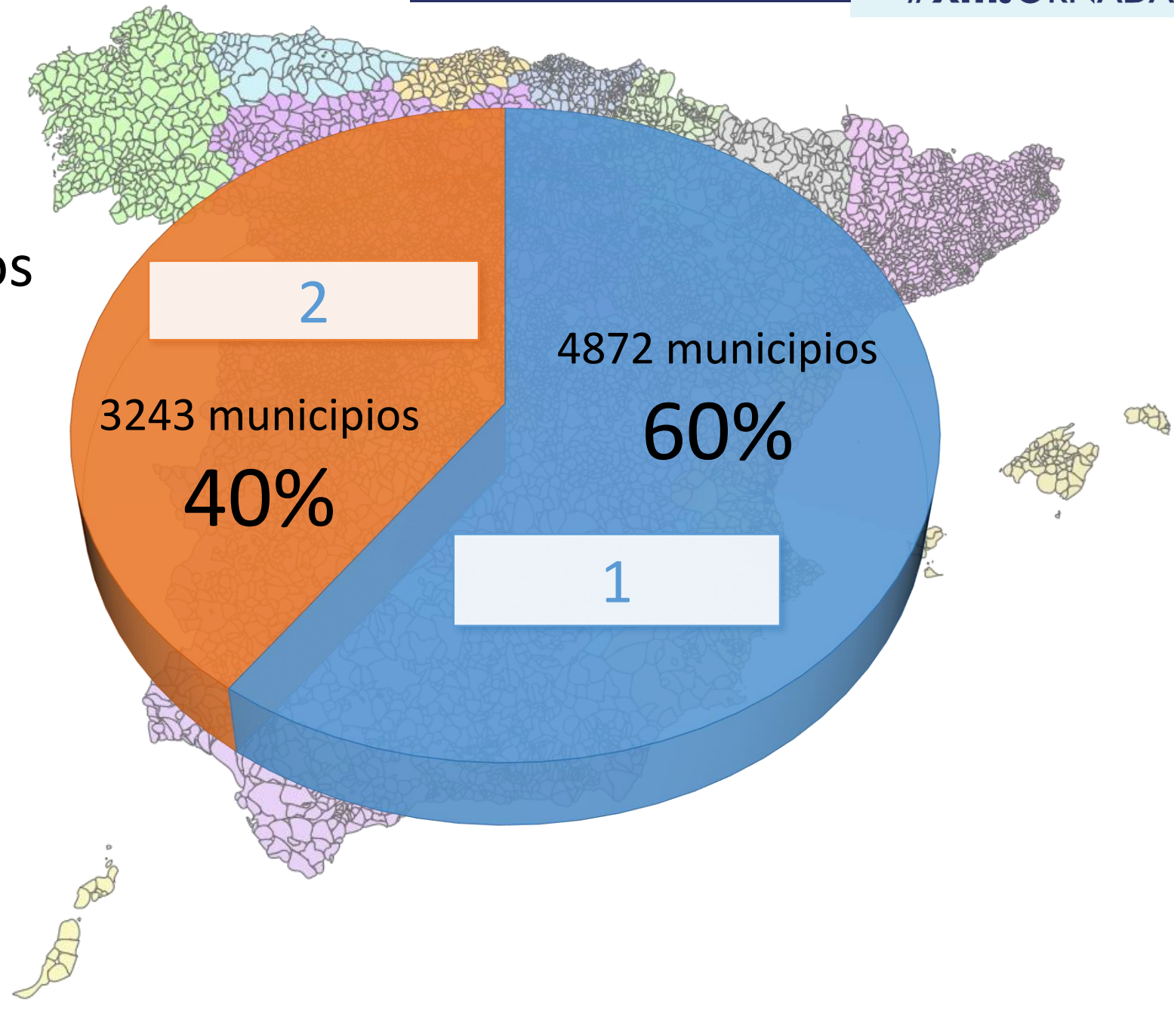


8115 municipios





8115 municipios





DIPUTACIÓN
PROVINCIAL
DE BURGOS

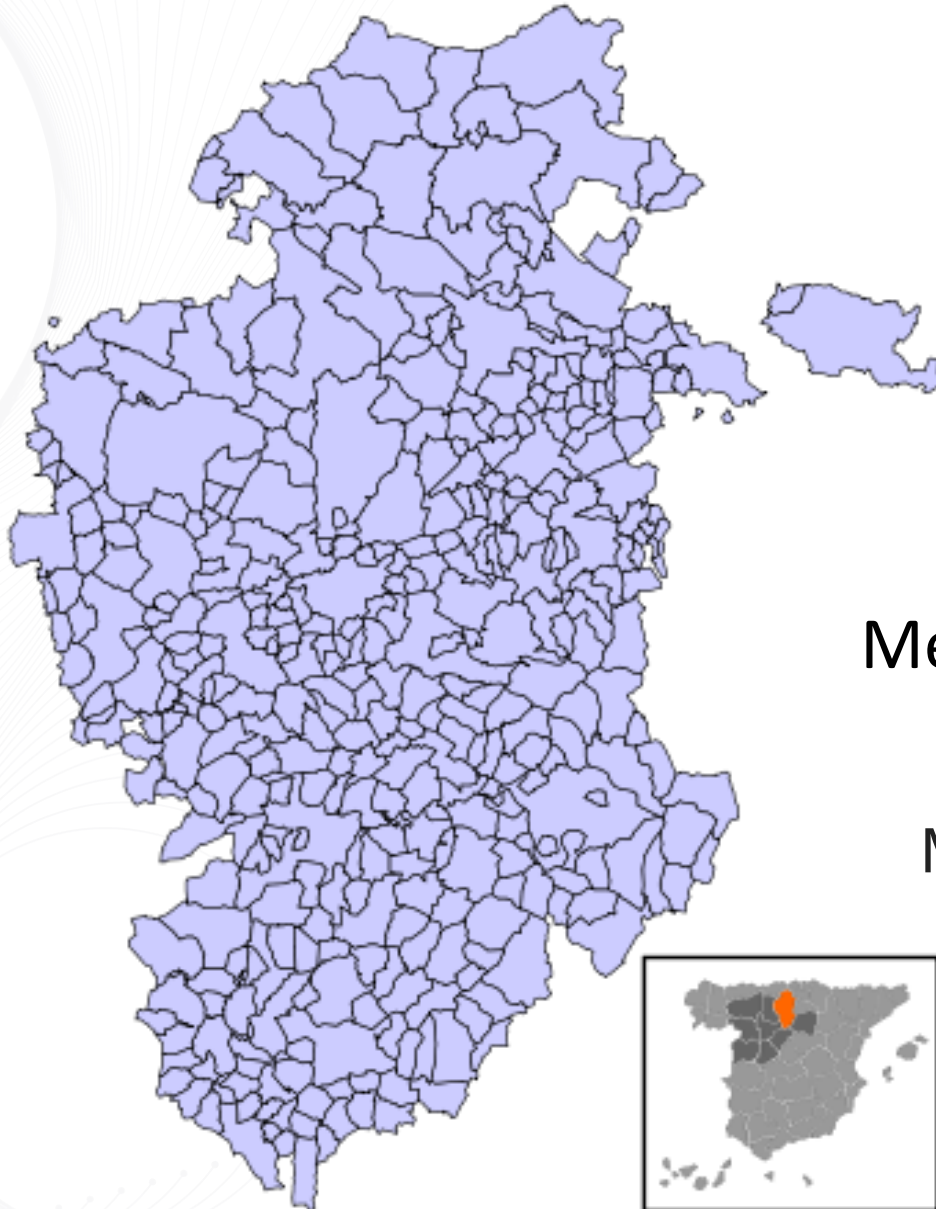
 371 municipios

Menos de 1.000 habitantes, el  93%.

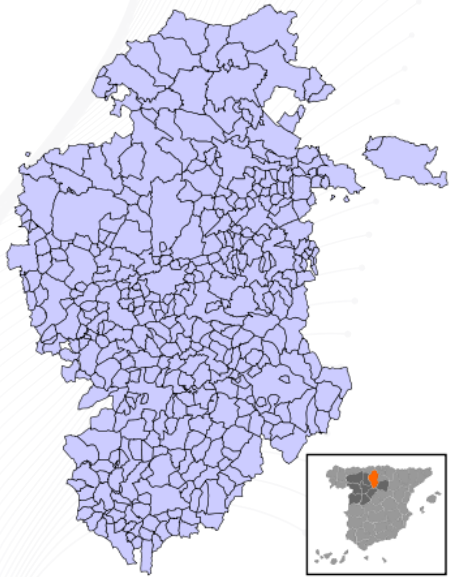
Municipios menores de 1001 hay 345 = 93%

Menores de 501 316 = 85%

Menores de 101 162 = 44%



Pueblo “pequeño”, Ayuntamiento “pequeño” (< 1.000 habitantes)

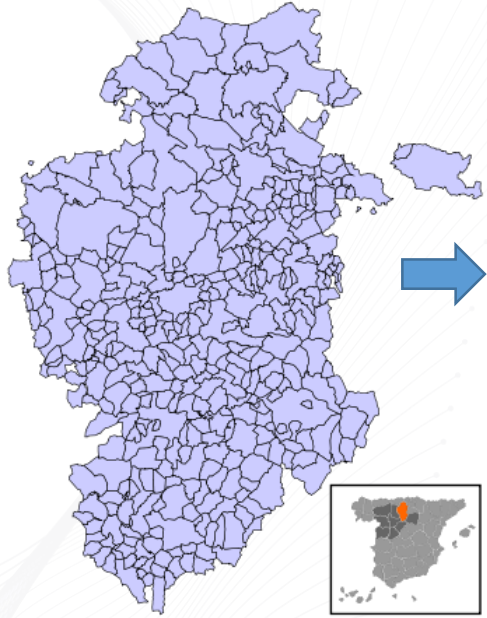


- Secretario compartido (y por horas)
- Alcaldes que ejercen otras profesiones principales
- Alta rotación de personal
- Ayuntamiento solo abierto unas pocas horas (¿proveedores?)
- Presupuestos bajos y con poco margen

¿Tienen estos ciudadanos menos derechos que el resto
a ver protegidos sus datos?



DIPUTACIÓN
PROVINCIAL
DE BURGOS



La ***Ley Reguladora de bases de régimen local (LRBL)*** establece las competencias de las diputaciones y una de ellas es:

g) La prestación de los servicios de administración electrónica y la contratación centralizada en los municipios con población inferior a 20.000 habitantes

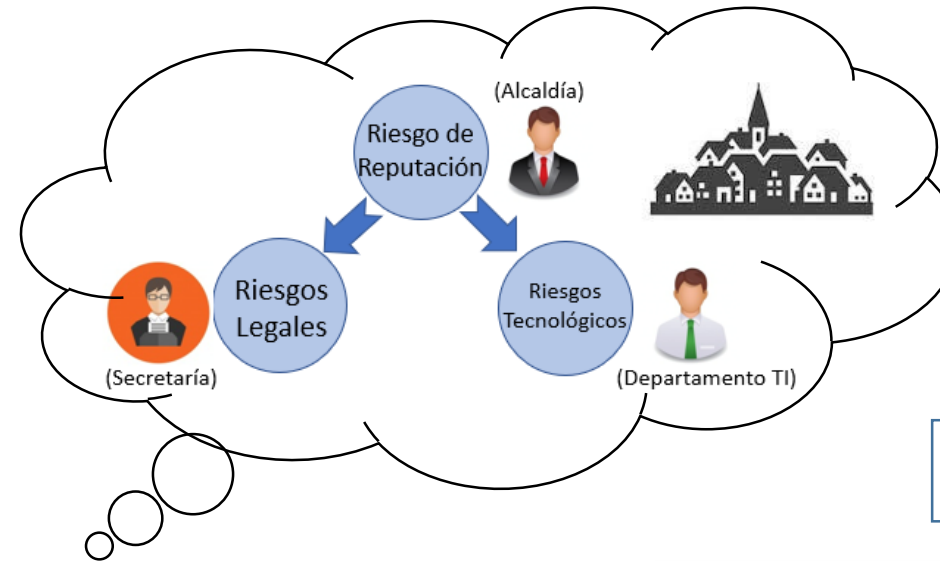
➡ Y que la ***Ley 39/2015*** establece que:

Todas las administraciones tienen que tener:

- *Sede Electrónica.*
- *Registro electrónico de documentos.*
- *Registro electrónico de apoderamiento*
- *Archivo único electrónico.*



DIPUTACIÓN
PROVINCIAL
DE BURGOS



Comité de Seguridad

- DIPUTADO PROVINCIAL NNTT
- SECRETARIO GENERAL
- RESP ÁREA NNTT
- RESP INFORMÁTICA

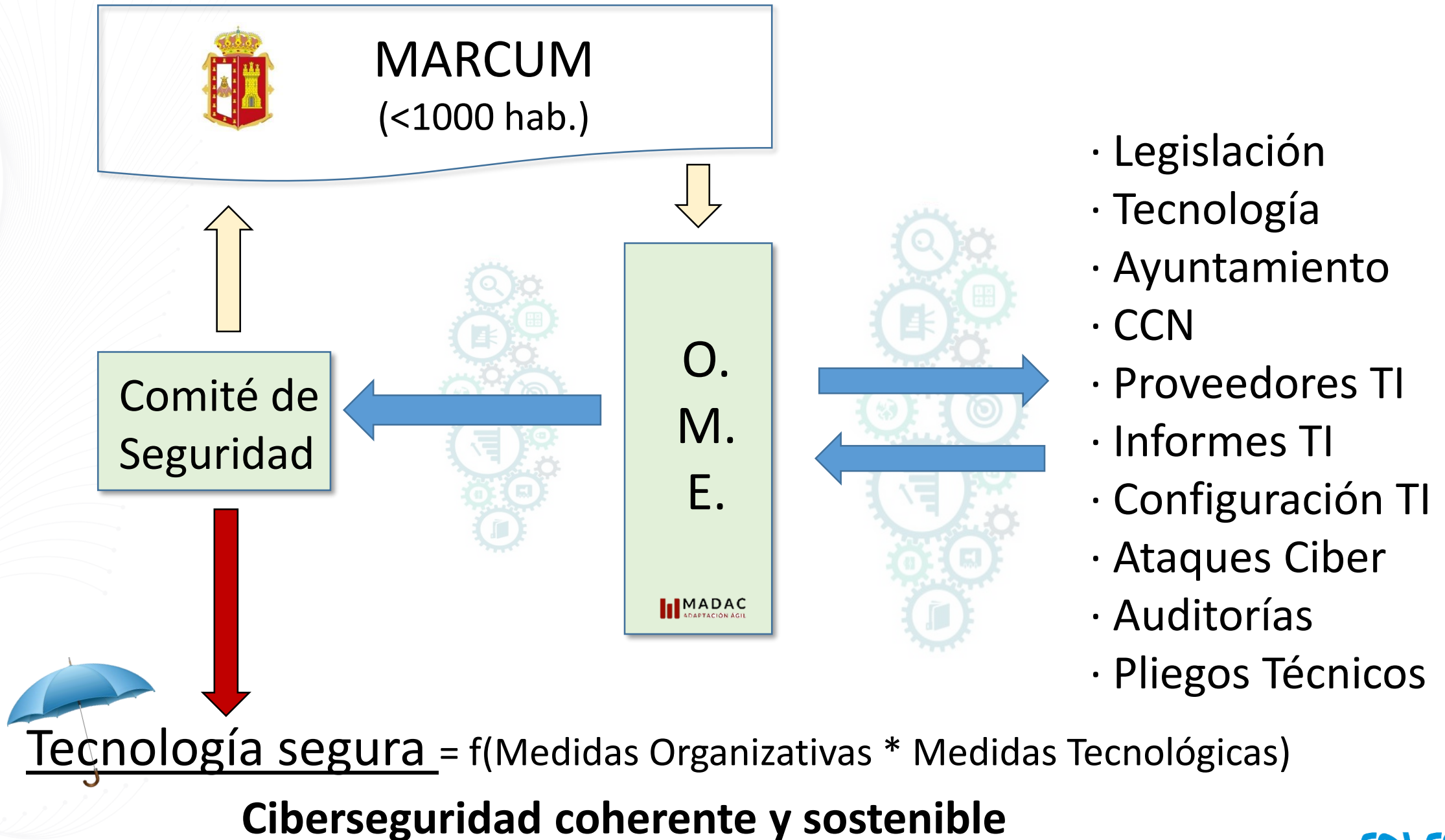


Normativa ágil

Marco Provincial de Cumplimiento (< 1000 hab.)



MADAC
ADAPTACIÓN ÁGIL





Guía CCN-STIC 883



Implantación del ENS para Entidades Locales



¡1ª PROMOCIÓN!



MARCUM

<1000 hab.

O.
M.
E.



- Análisis de Riesgos
- Planes de Contraste
- Cuadro de Mandos
- Coordinación
- Seguimiento Proveedores TI

...



R
E
Q
U
I
S
I
T
O
S



+ proveedor TI



+ proveedor TI



+ proveedor TI



MARCUM

<1000 hab.

O.
M.
E.



Política de Seguridad ·
Adhesión al Marco de Cumplimiento ·
Buenas prácticas (obligatorias) como usuarios ·
Gestión y configuración TI alineada ·

R
E
Q
U
I
S
I
T
O
S



+ proveedor TI



+ proveedor TI



+ proveedor TI



MARCUM

<1000 hab.

O.
M.
E.

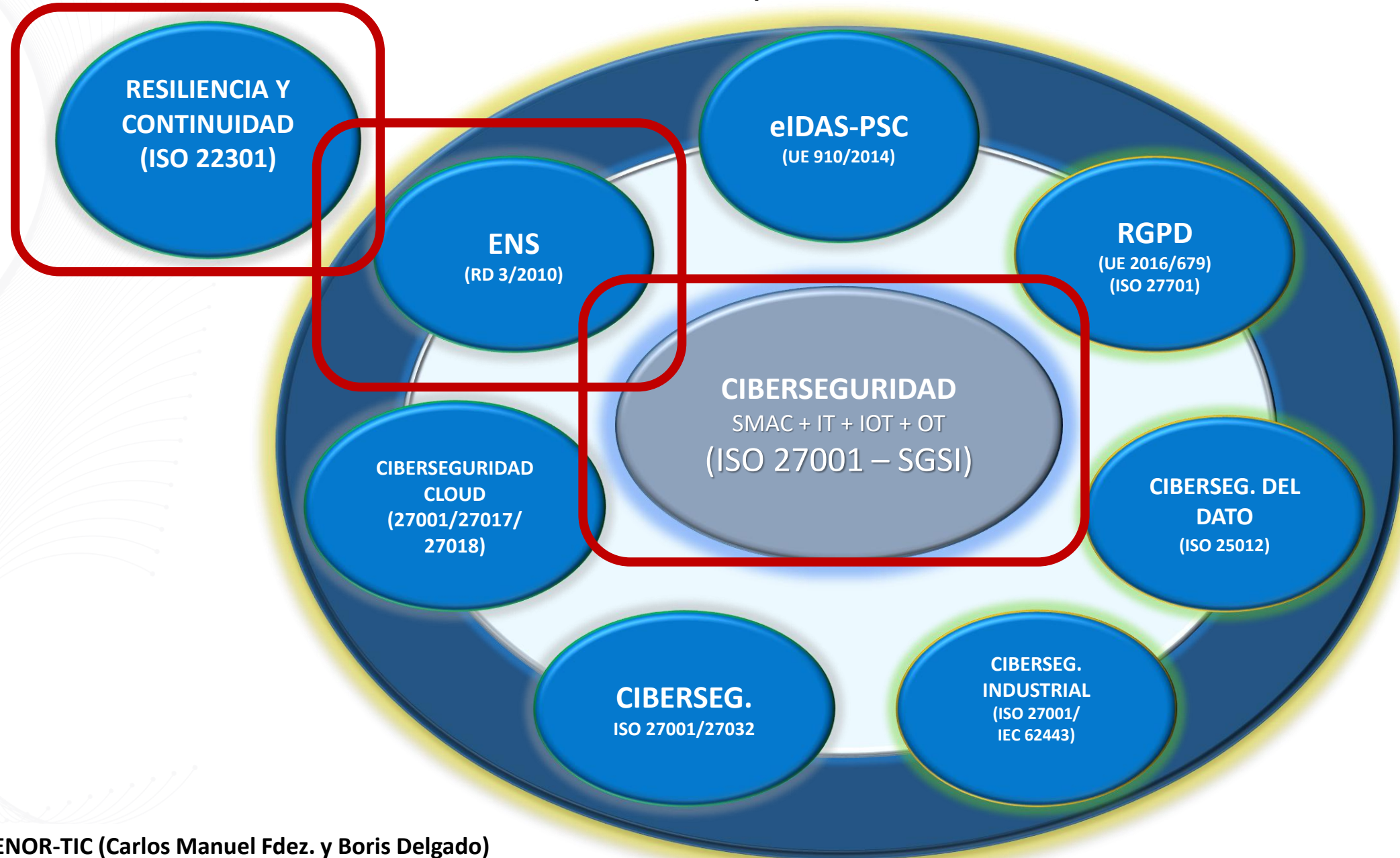


TARDAJOS



R
E
Q
U
I
S
I
T
O
S



MODELO DE CIBERSEGURIDAD, PRIVACIDAD & COMPLIANCE TI

ESQUEMA NACIONAL DE SEGURIDAD – AUDITORIA DE CONFORMIDAD CON EL ENS

Real Decreto 3/2010. Establecer la **política de seguridad** en la utilización de medios electrónicos a través de **principios básicos** y **requisitos mínimos** que permitan una **protección adecuada** de la información.

Se crean las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de **medidas de seguridad** para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos.

Dimensiones de **Seguridad en ENS**:

Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad

PRINCIPIOS BASICOS (6)

Se tienen en cuenta para las decisiones en materia de seguridad

- Seguridad Integral
- Gestión basada en riesgos
- Prevención, reacción y recuperación
- Líneas de defensa
- Evaluación periódica
- Función diferenciada



Requisitos MINIMOS (15)

Permitirán una **protección adecuada** de la información

MEDIDAS DE SEGURIDAD (75)

Se tendrán que cumplir dentro de los **principios básicos** y **requisitos mínimos** establecidos y serán proporcionales a:

- i) El **tipo y nivel** de la información gestionada
- ii) Las **dimensiones** de seguridad relevantes en el sistema a proteger
- iii) La **categoría** del sistema de información a proteger.

ESQUEMA NACIONAL DE SEGURIDAD – AUDITORIA DE CONFORMIDAD CON EL ENS

Auditorías de Conformidad con el ENS

El Art. 34 del ENS :

- ✓ Los sistemas de información serán objeto de **una auditoría regular ordinaria, al menos cada dos años**, que verifique el cumplimiento de los requerimientos del ENS.

El Anexo III – Auditoria de Seguridad:

- ✓ La seguridad de los sistemas de información de una organización será auditada en los siguientes términos:
 - a) Que la **política de seguridad define los roles y funciones** de los responsables de la información, los servicios, los activos y la seguridad del sistema de información.
 - b) Que existen **procedimientos para resolución de conflictos entre dichos responsables**.
 - c) Que se han designado personas para dichos roles a la luz del principio de "**separación de funciones**".
 - d) Que se ha realizado **un análisis de riesgos, con revisión y aprobación anual**.
 - e) Que **se cumplen las recomendaciones de protección descritas en el anexo II**, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso.
 - f) Que existe un **sistema de gestión de la seguridad de la información**, documentado y con un proceso **regular de aprobación por la dirección**.

ISO 17065 – Certificación de Productos y Servicios

Instrucción Técnica de Seguridad (ITS) de conformidad con el Esquema Nacional de Seguridad. (BOE 265 – 2-Nov-16), y complementariamente con **CCN-STIC-809** – *Declaración y Certificación de conformidad con el ENS y el distintivo de cumplimiento.*

- ✓ **Registro de la conformidad** con todos los requisitos auditados (evidencias de conformidad y no conformidad; Articulado y medidas)
 - El Art. 34 del ENS.
 - **ITS de Auditoria de Seguridad (BOE-A-2018-4573)**
 - *CCN-STIC-802. Auditoría del ENS*
 - *CCN-STIC-804. Guía de Implantación*
 - *CCN-STIC 808. Verificación del cumplimiento medidas ENS.* (
 - **CCN-CERT IC-01/09 – ENS: Criterios adicionales de Auditoría y Certificación**
- ✓ **No hay ciclo de certificación.** (son bienales)
- ✓ **Obligatorio** Cat. **Media** y **Alta**. Autoeval. **Básica**
- ✓ **AENOR emite certificados acreditados con estos criterios/formato**

✓ ADICIONALMENTE

CCN-STIC-801-Guía de Responsabilidades y funciones (2 roles; 3 roles).

CCN-STIC-803 – Guía de Valoración de Sistemas (ejemplo Cat. EELL)

CCN-STIC-824-Guía INES

CCN-STIC-882-AARR para EELL

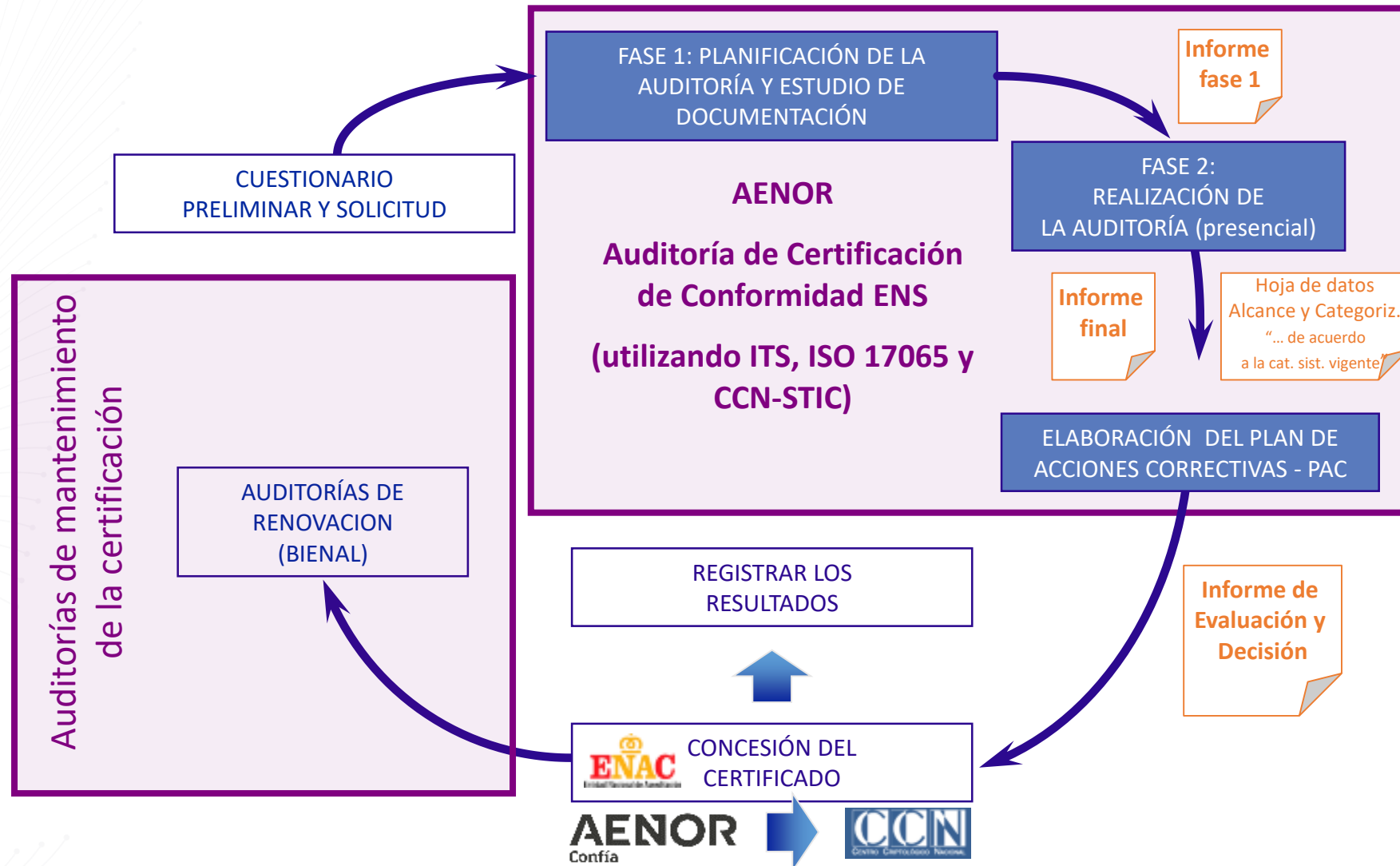
CCN-STIC-883-Implantación EELL

Guías de la FEMP



ESQUEMA NACIONAL DE SEGURIDAD – AUDITORIA DE CONFORMIDAD CON EL ENS

PROCESO DE AUDITORIA DE CONFORMIDAD DEL ENS



AENOR como AUDIT PARTNER : Mentoring&Benchmarking

ESQUEMA NACIONAL DE SEGURIDAD – AUDITORIA DE CONFORMIDAD CON EL ENS

FASE 1**Estudio de Documentación (entre otras):**

- 1.- Política de seguridad
- 2.- Organigrama de los servicios o áreas afectadas
- 3.- Descripción detallada del sistema de información
- 4.- Categoría del sistema según el Anexo I y Análisis de Riesgos
- 5.- La Declaración de Aplicabilidad

INFORME DE AUDITORIA

Con un resumen de los aspectos auditados, se presenta al Responsable del sistema y Responsable de seguridad y se realiza un dictamen final: **FAVORABLE, FAVORABLE CON NO CONFORMIDADES o DESFAVORABLE**

Además de identifican las desviaciones detectadas

(No Conformidades Mayores/Menores, Observaciones, Oportunidades de Mejora)

FASE 2**Presencial:**

- ✓ Revisión de los artículos y Anexos I y II RD 3/2010
- ✓ Análisis y Gestión de Riesgos
- ✓ Categorización del sistema
- ✓ Declaración de Aplicabilidad (y medidas compensatorias – Art. 27)

Revisión de las medidas según la categorización del sistema:

- ✓ **El marco organizativo** y la segregación de funciones
- ✓ **El marco operacional** (Planificación, Control de Accesos, Explotación, Servicios Externos, Continuidad del Servicio, y Monitorización del Sistema)
- ✓ **Las medidas de protección** (Protección de las instalaciones e infraestructuras, Gestión del personal, Protección de equipos, de las comunicaciones, de los soportes de información, de las aplicaciones informáticas, de la información, y de los servicios).



MARCUM

<1000 hab.

O.
M.
E.



TARDAJOS



R
E
Q
U
I
S
I
T
O
S

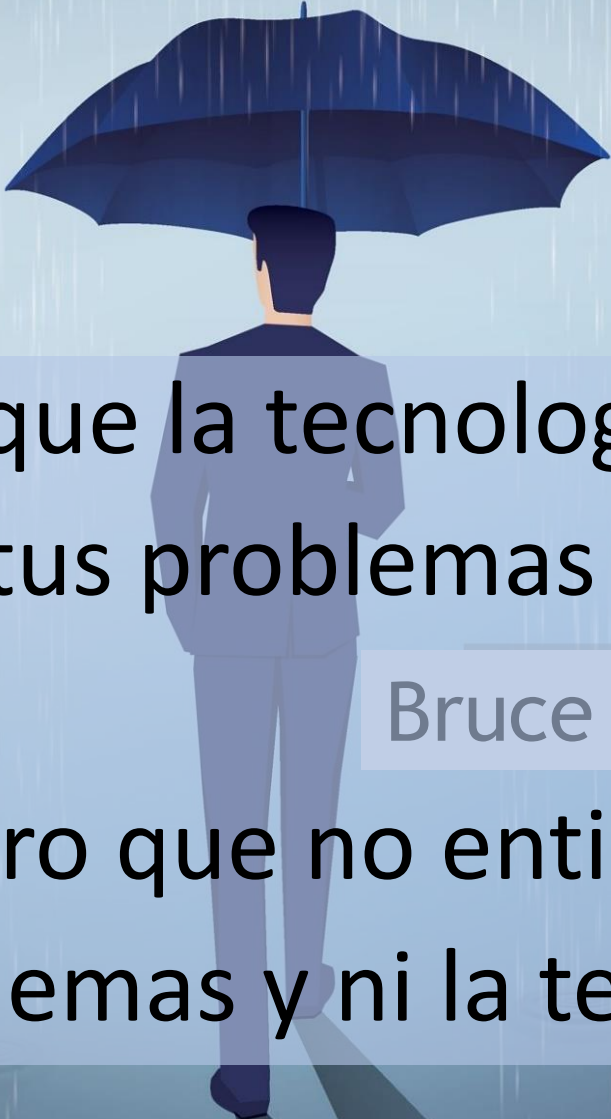


[illegible][illegible]

Cumplimiento ENS/RGPD → ¿Dinámica futura?



Seguridad
~~Economía~~ de Escala



Si piensas que la tecnología puede
resolver todos tus problemas de seguridad,

Bruce Schneier - 2004

está claro que no entiendes
ni los problemas y ni la tecnología.

Muchas Gracias

ENS x Provincia



Diputación
de Burgos



AENOR
Confía

COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

**XIII
JORNADAS
STIC
CCN-CERT**

ccn-cert
centro criptológico nacional