ENS. Caso de estudio en EELL

David López. Cibergob

I Encuentro del ENS.
Tendencias y Políticas de Seguridad

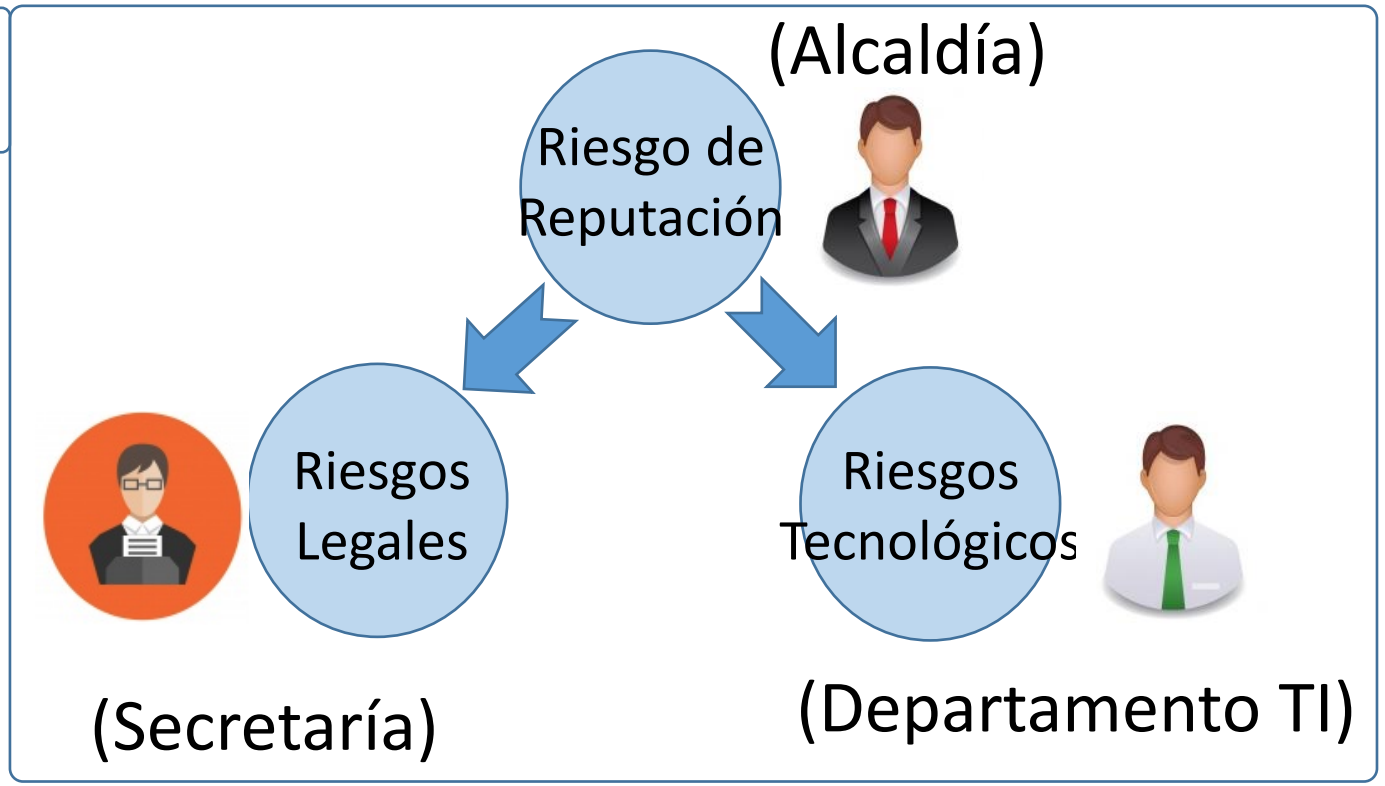
Caso de estudio: 5 Ayuntamientos (<20k hab)

	EJEA DE LOS CABALLEROS (ZGZ)	ALCAÑIZ (TER)	UTEBO (ZGZ)	JACA (HU)	CUARTE DE HUERVA (ZGZ)
Habitantes	16.5 k	16.0 k	18.4 k	12.9 k >55.0 k	12.5 k
Nº PCs	110	120	155	170	60
Informáticos	1	1	1	1+3	1

Datos del INE 2016

1. La Seguridad, sin Responsable de Seguridad

Guía de Seguridad de las TIC
CCN-STIC 883



2. Objetivo: la dinámica de cumplimiento

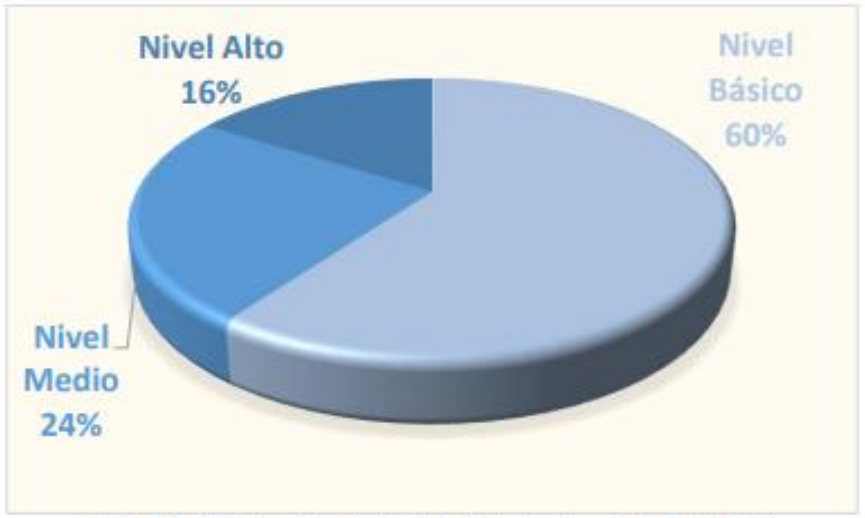


Tabla 1. Distribución de las Medidas de Seguridad del ENS

La cuestión no radica en cuán lejos estamos del cumplimiento del ENS, sino

¿Cómo vamos a generar y mantener la dinámica que nos permita alcanzar el cumplimiento?

Si conseguimos *Dinámica de Cumplimiento* importará menos donde esté la meta

3. El alcance es clave. Sede electrónica

Guía de Seguridad de las TIC
CCN-STIC 883

Tabla 2. Esquema de Alcance cumplimiento del ENS para una Sede Electrónica basada en Servicio SaaS

A más tecnología "en casa", más "duro" cumplir con el ENS

4. Estrategia de cumplimiento

Sede Electrónica

Sede Electrónica Web

Sede Electrónica Web Wi-Fi

Sede Electrónica Web Wi-Fi

. . .

Hay que cumplir el ENS. Pero nadie dice que haya que cumplirlo todo del golpe.

¿Cómo?

a. Aplicabilidad proyectada en Normativas

Código	Medida de Seguridad	B	Salvaguardas existentes
org.1	Política de Seguridad	aplica	Política de Seguridad
org.2	Normativa de seguridad	aplica	Normativa de Uso de Recursos y Accesos a Sistemas de Información
org.3	Procedimientos de seguridad	aplica	Procedimiento Operativo del Servicio ENS
org.4	Proceso de autorización	aplica	Normativa de Gestión de Autorizaciones
op.pl.1	Análisis de riesgos	aplica	Normativa de Gestión de Riesgos
op.pl.2	Arquitectura de seguridad	aplica	Normativa de Arquitectura de Seguridad
op.pl.3	Adquisición de nuevos componentes	aplica	Normativa de Gestión de Ciclo de Vida de las Plataformas Tecnológicas
op.acc.1	Identificación	aplica	Normativa de Gestión de cuentas de usuario
op.acc.2	Requisitos de acceso	aplica	Normativa de Gestión de Acceso Lógico
op.acc.4	Proceso de gestión de derechos de acceso	aplica	Normativa de Gestión de Autorizaciones
op.acc.5	Mecanismo de autenticación	aplica	Normativa de Gestión de Acceso Lógico
op.acc.6	Acceso local (local logon)	aplica	Normativa de Gestión de Acceso Lógico

- La normativa es adaptable
- La normativa son decisiones
- La normativa es ‘palabra de Comité’

MADAC* indica que cada Medida de Seguridad está regida por una Normativa

* MADAC (Metodología Ágil del Adaptación Continua)

b. Normativas ágiles

Norma Ágil = f (B,C,D,E,F)

c. Planes de Contraste

"Confía pero comprueba"

Comprobaciones
- No invasivas
- Técnicas
- Coordinación

d. Contextos

Contextos		Decisiones reflejadas en normativas
Clasificación de normativas de seguridad por contextos		
Organización	1.ORG	sobre la organización de la seguridad dentro de la entidad
Usuarios	2.USU	enfocadas a los usuarios
Seguridad	3.SEG	Decisiones generales sobre ciberseguridad
Tecnología	4.TEC	Decisiones concretas sobre las plataformas tecnológicas
Puesto de Trabajo Digital	5.PTD	Decisiones concretas sobre PC's, portátiles, móviles
Monitorización	6.MON	Para establecer el control adecuado de los servicios
Software	7.SOFT	Decisiones concretas sobre el desarrollo software en la entidad

Control sobre la Ciberseguridad

Transversal

Capacidad transformadora

Transformación Digital

e. Dinámica de Cumplimiento

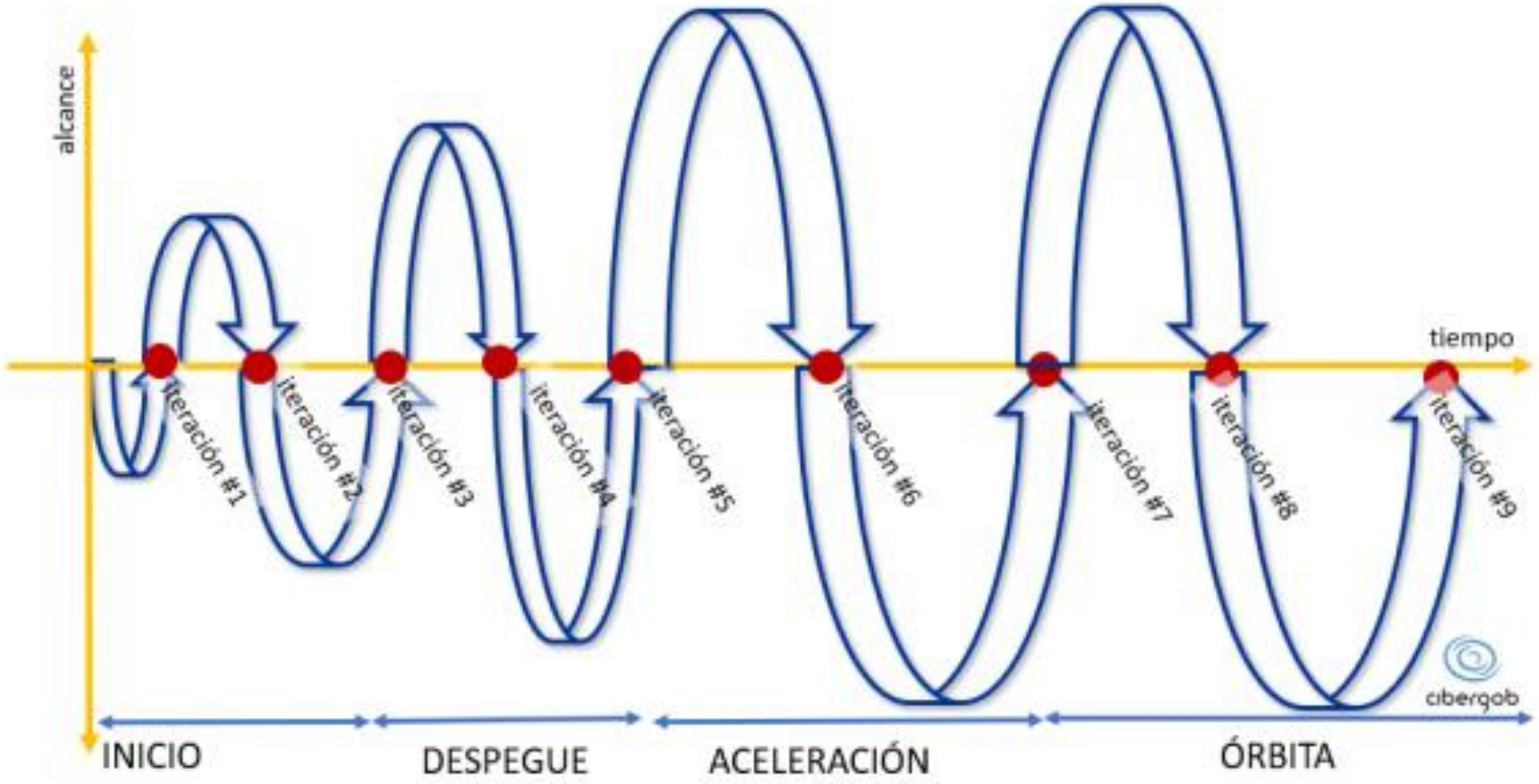
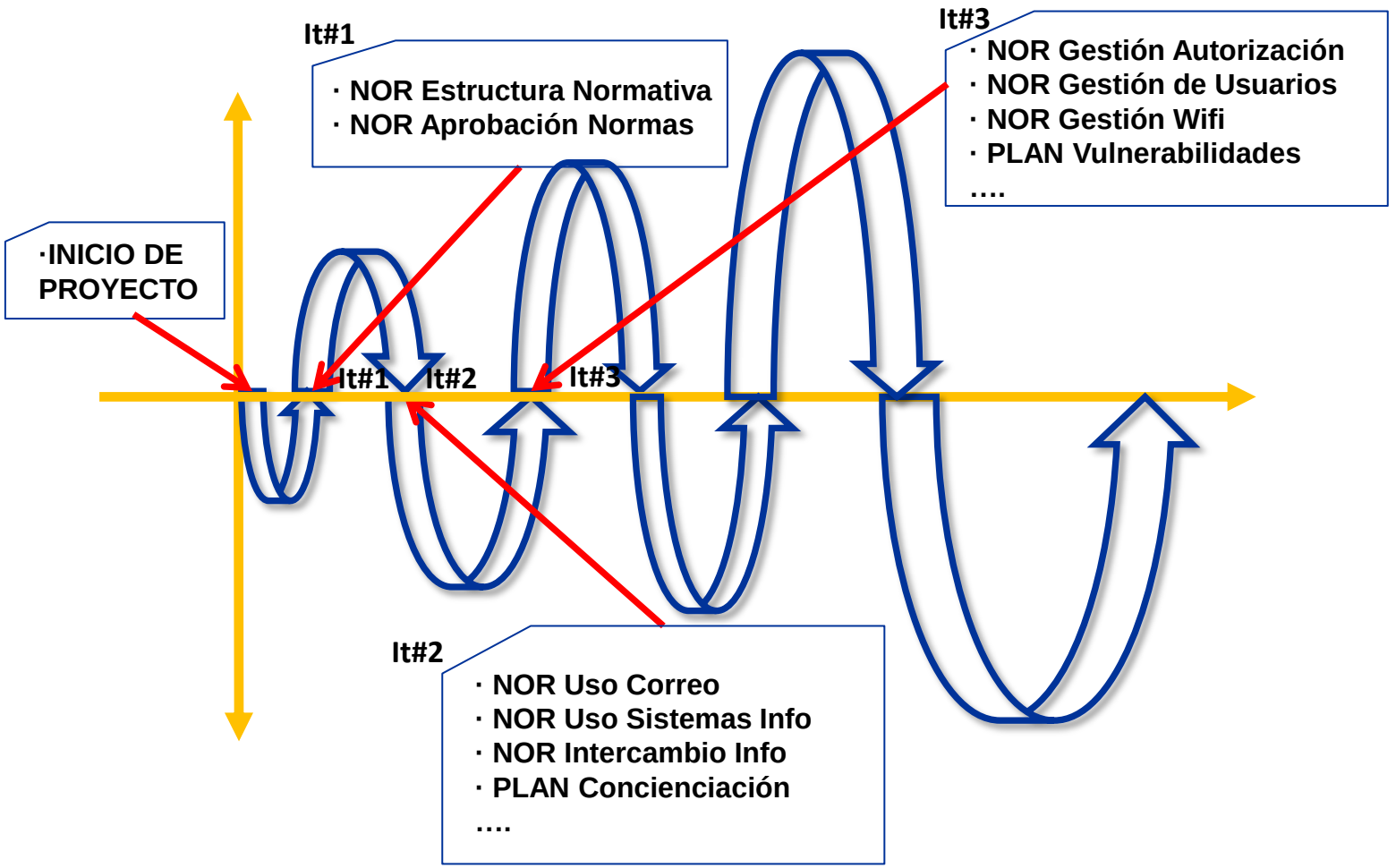


Tabla 4. Fases y ejemplo de Iteraciones según Metodología MADAC

f. Dinámica de Cumplimiento y…



…Gestión del Riesgo

centro criptológico nacional

¿La evolución?

Cuadro de Mando Integral. Progresión (I)

FASE I

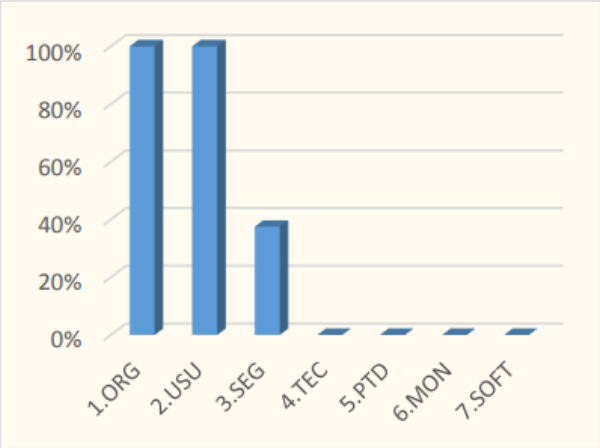


Tabla 7. Cobertura del Cuerpo Normativo – Fase I

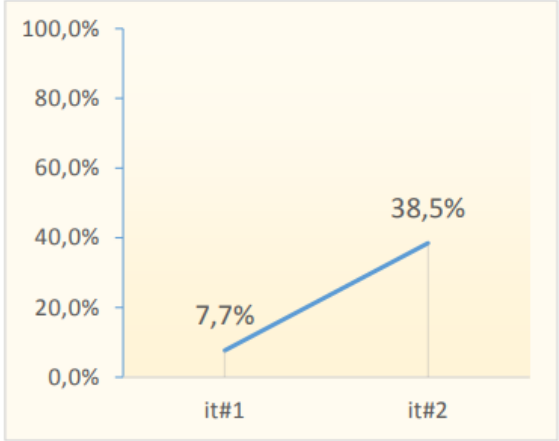


Tabla 8. Progresión del cuerpo normativo sobre la Aplicabilidad

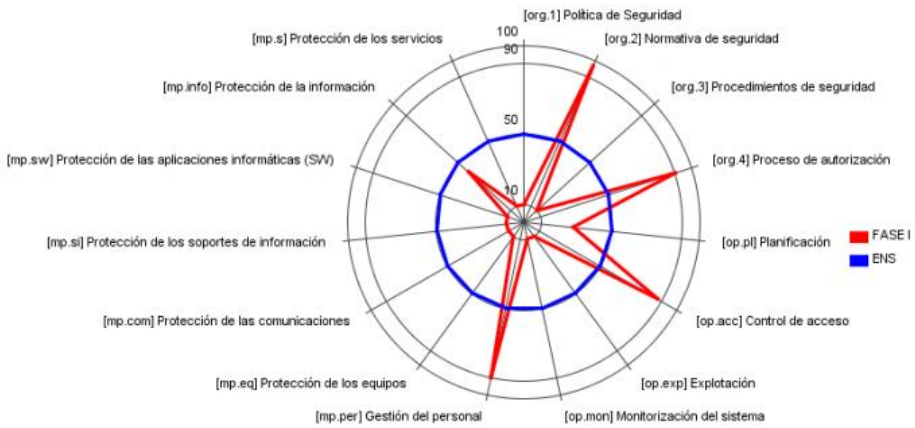


Ilustración 2. Gráfica del AARR en Herramienta PILAR (al completar la Fase I)

FASE II

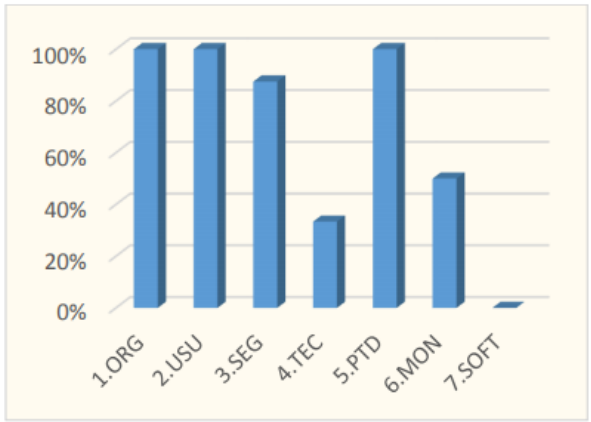


Tabla 10. Cobertura del Cuerpo Normativo – Fase II

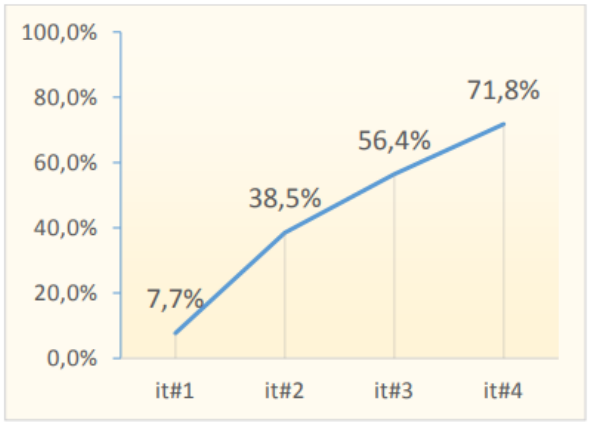


Tabla 11. Progresión del cuerpo normativo sobre la Aplicabilidad

Guía de Seguridad de las TIC
CCN-STIC 883

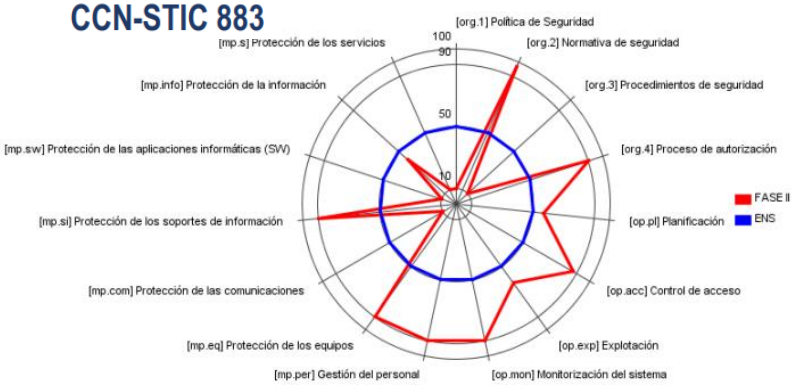


Ilustración 3. Gráfica del AARR en Herramienta PILAR (Fase II)

Cuadro de Mando Integral. Progresión (II)

FASE III

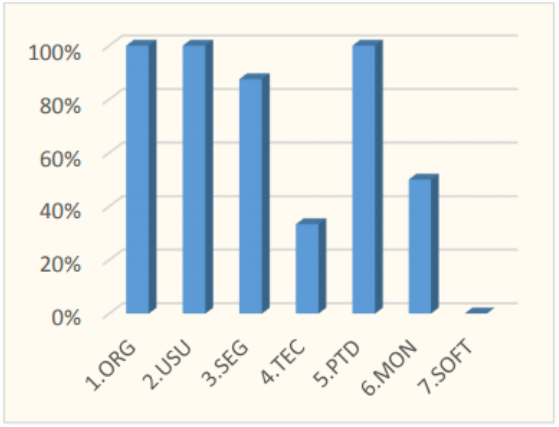


Tabla 12. Cobertura del Cuerpo Normativo – Fase III

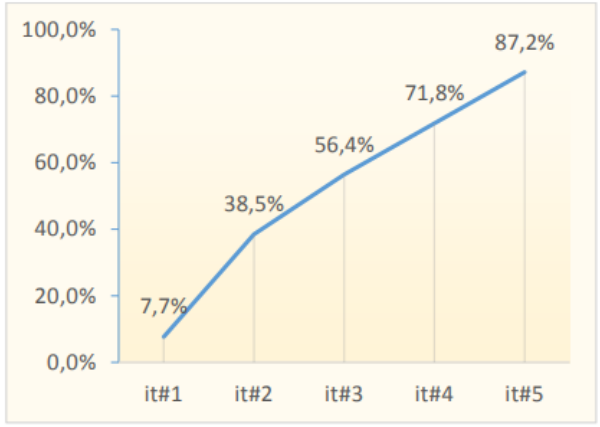


Tabla 13. Progresión del cuerpo normativo sobre la Aplicabilidad

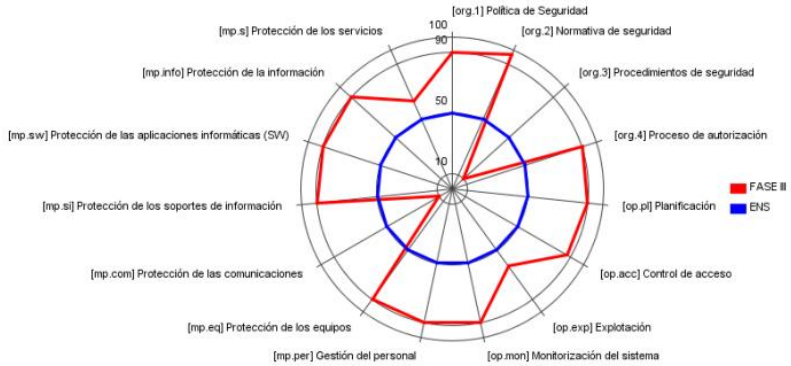


Ilustración 4. Gráfica del AARR en Herramienta PILAR (al completar la Fase III)

FASE IV

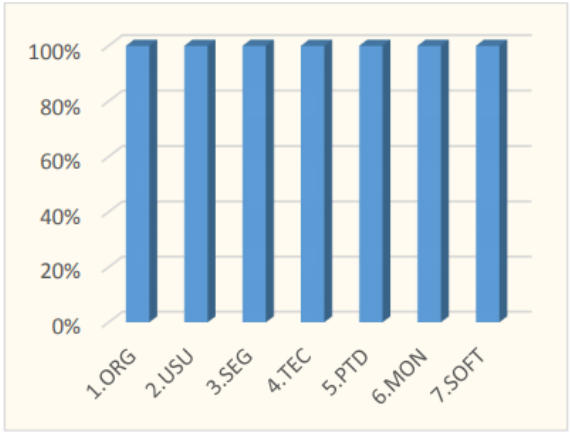


Tabla 14. Cobertura del Cuerpo Normativo – Fase IV

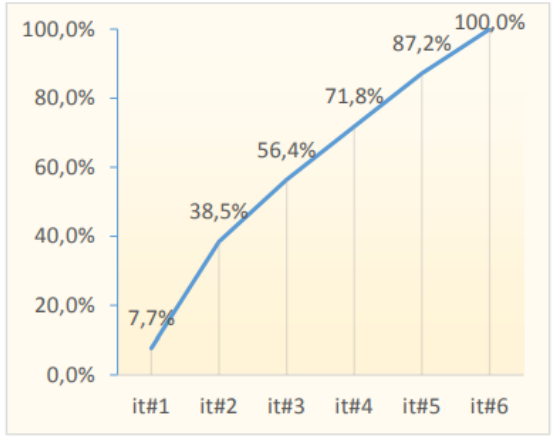


Tabla 15. Progresión del cuerpo normativo sobre la Aplicabilidad

Guía de Seguridad de las TIC
CCN-STIC 883

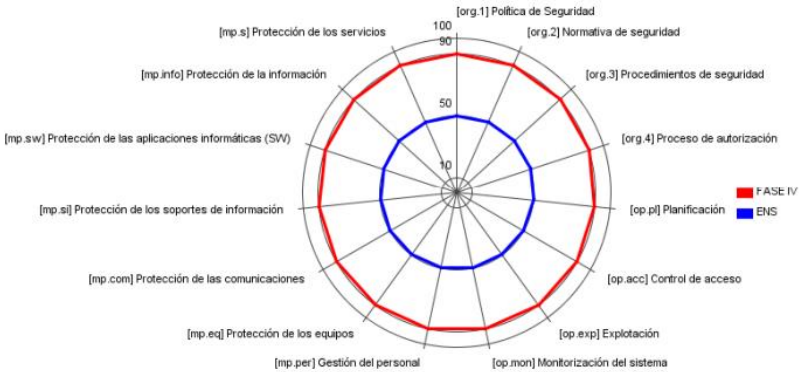


Ilustración 5. Gráfica del AARR en Herramienta PILAR (al completar la Fase I)

centro criptológico nacional

Resultado

Ayuntamiento de Utebo	UTEBO (ZGZ)	18.4 k		Sede Electrónica
	CUARTE DE HUERVA (ZGZ)	12.5 k		Sede Electrónica
AYUNTAMIENTO DE JACA	JACA (HU)	12.9 k >55.0 k		Sede Electrónica
M.I. AYUNTAMIENTO DE EJEA DE LOS CABALLEROS	EJEA DE LOS CABALLEROS (ZGZ)	16.5 k		Sede Electrónica
ALCAÑIZ AYUNTAMIENTO	ALCAÑIZ (TER)	16.0 k		Sede Electrónica

Si piensas que la tecnología puede

resolver todos tus problemas de seguridad,

está claro que no entiendes

ni los problemas y ni la tecnología.

Bruce Schneider - 2004

Muchas gracias

David López Rodríguez
CEO de Cibergob
dlopezr@cibergob.es