

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

**"La aplicación el Esquema Nacional de Seguridad en las Administraciones
Públicas bajo un enfoque práctico"**

Menos es Más

- ES +





- Miguel A. Lubián
- CIES Seguridad (instituto CIES)
- miguel.lubian@institutocies.es

Índice

1. **Objetivo y alcance (subjetivo, objetivo y práctico)**
2. **Determinación de una estrategia**
3. **Implantación de un modelo simplificado (progresivo)**
4. **Priorización de las medidas de seguridad**
5. **Algunas novedades (interpretaciones)**



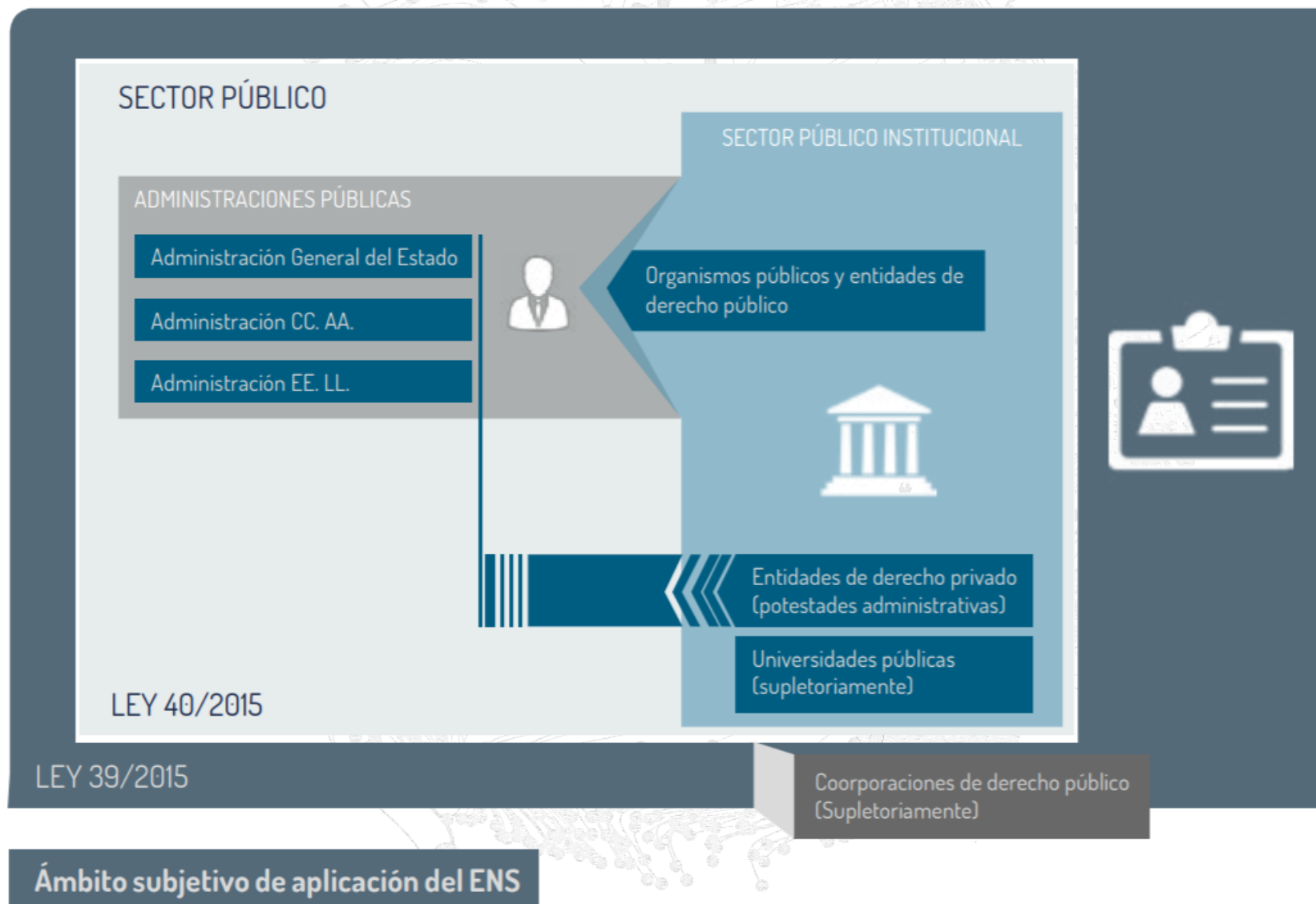
¿Qué aspectos **NO** vamos a tratar?

Por razón de los sujetos o entidades a los que se dirige la norma.

ÁMBITO SUBJETIVO DE APLICACIÓN

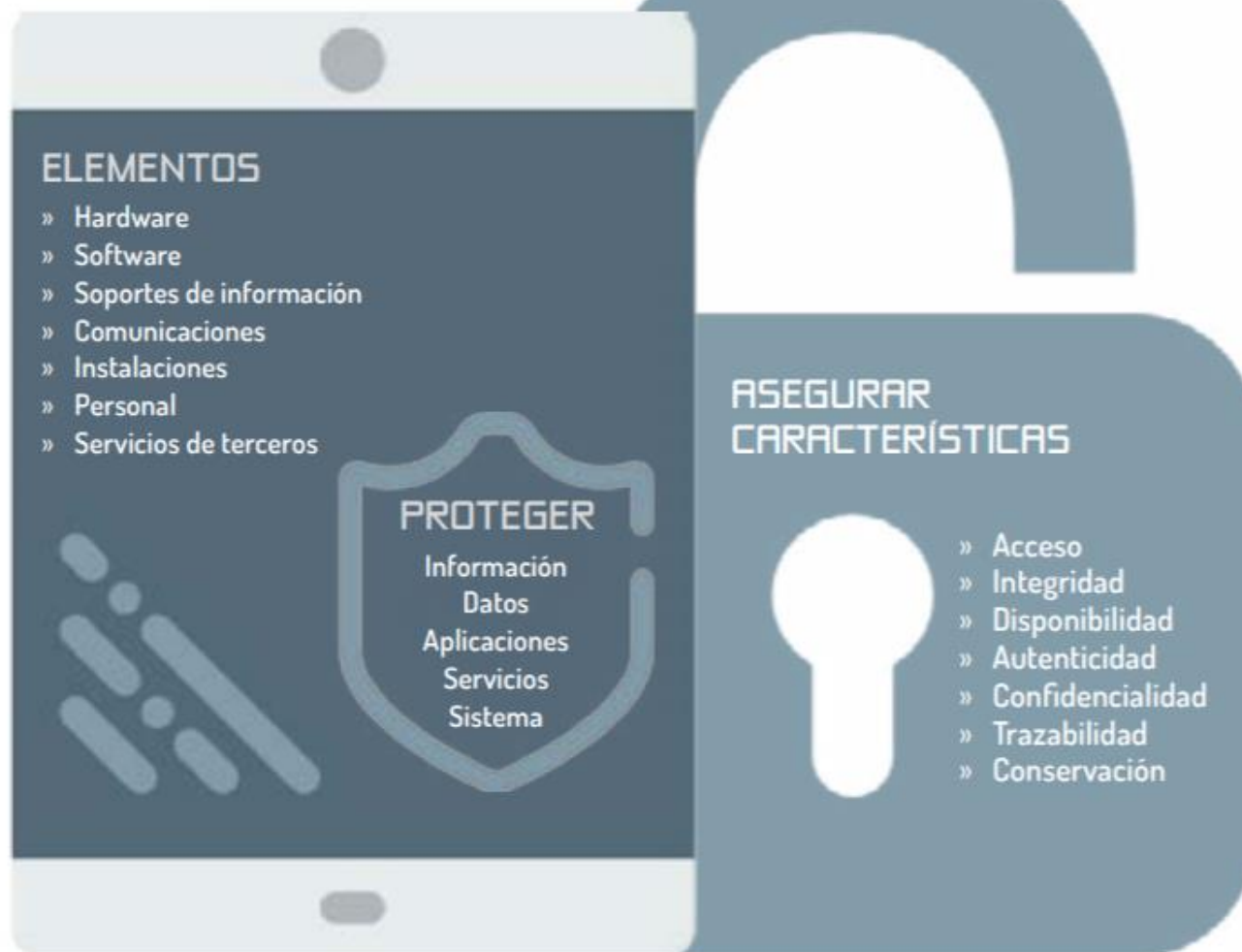
Por razón de las materias que son objeto de su regulación.

ÁMBITO OBJETIVO o MATERIAL DE APLICACIÓN





SISTEMAS Y COMUNICACIONES DEL SECTOR PÚBLICO



ÁMBITO OBJETIVO DE APLICACIÓN DEL ENS

Principios Básicos de Seguridad

"Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios."

Requisitos Mínimos de Seguridad

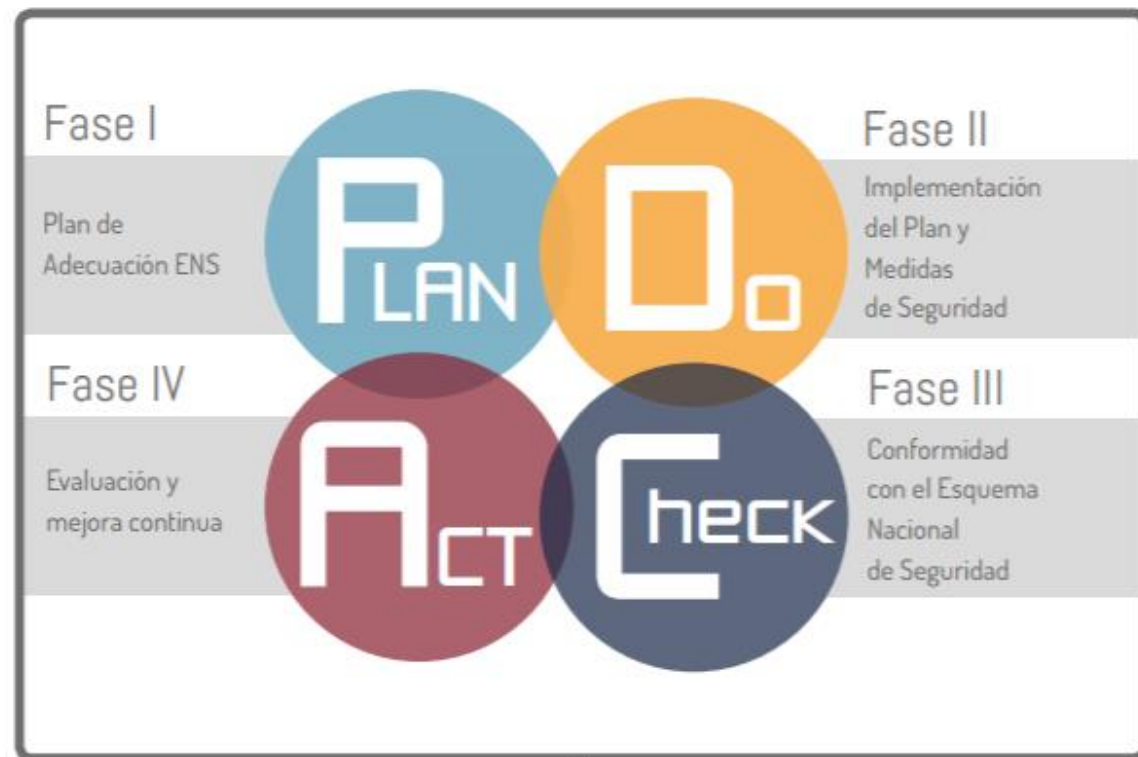
"Exigencias necesarias para asegurar la información y los servicios."

CAPÍTULO II Principios básicos

- ❓ Artículo 4. Principios básicos del Esquema Nacional de Seguridad.
- ❓ Artículo 5. La seguridad como un proceso integral.
- ❓ Artículo 6. Gestión de la seguridad basada en los riesgos.
- ❓ Artículo 7. Prevención, reacción y recuperación.
- ❓ Artículo 8. Líneas de defensa.
- ❓ Artículo 9. Reevaluación periódica.
- ❓ Artículo 10. La seguridad como función diferenciada.

CAPÍTULO III Requisitos mínimos

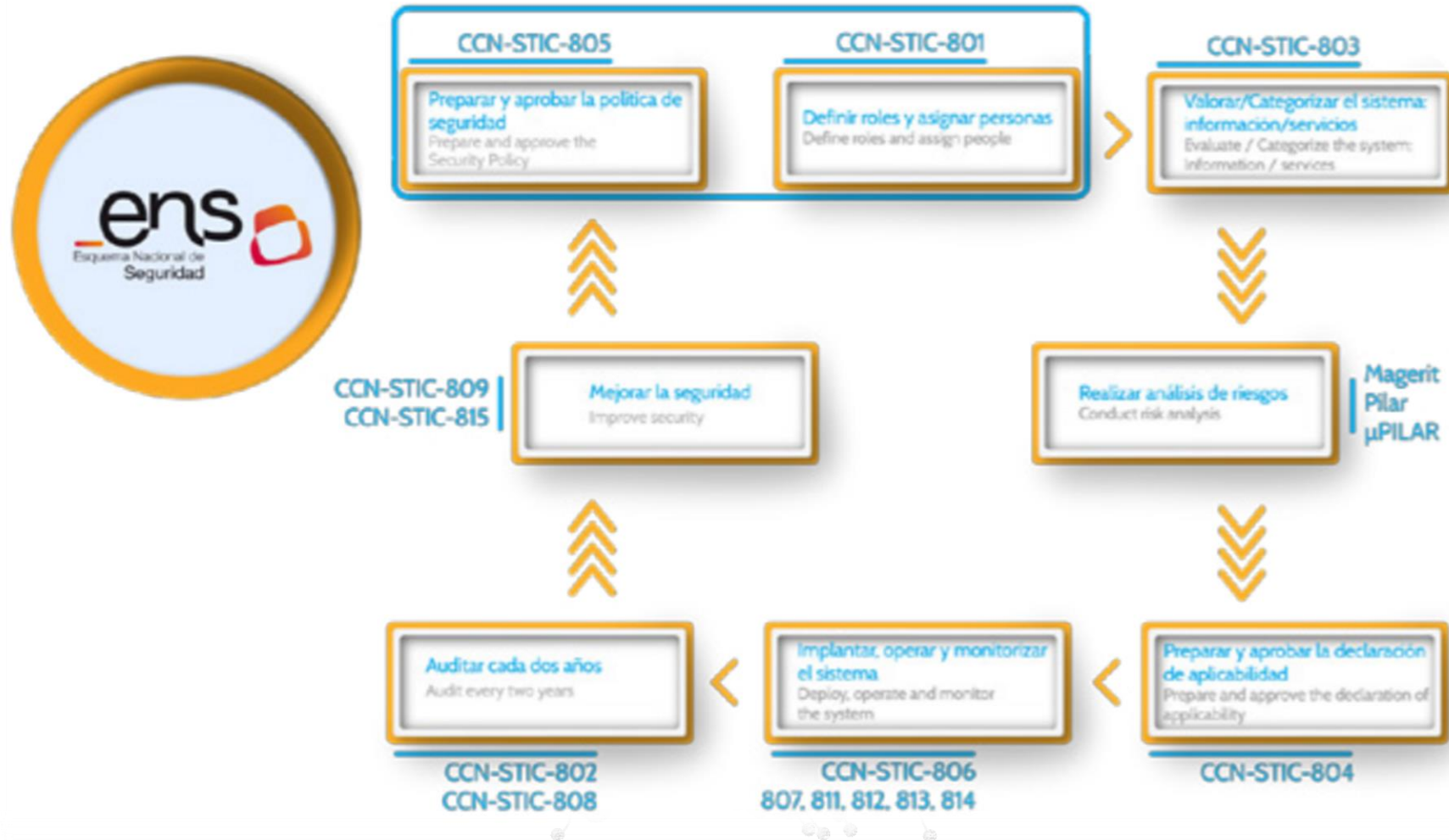
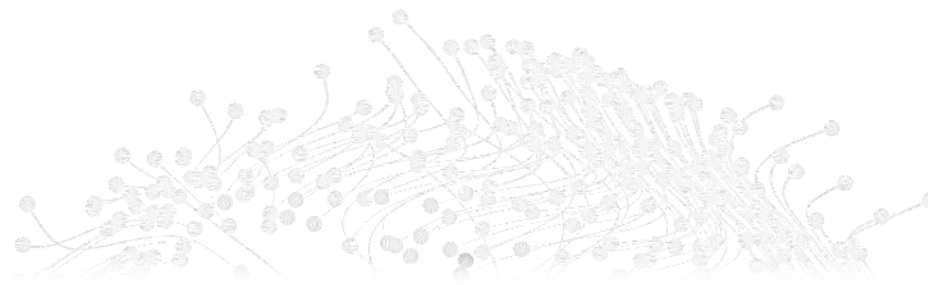
- ❓ Artículo 11. Requisitos mínimos de seguridad.
- ❓ Artículo 12. Organización e implantación del proceso de seguridad.
- ❓ Artículo 13. Análisis y gestión de los riesgos.
- ❓ Artículo 14. Gestión de personal.
- ❓ Artículo 15. Profesionalidad.
- ❓ Artículo 16. Autorización y control de los accesos.
- ❓ Artículo 17. Protección de las instalaciones.
- ❓ Artículo 18. Adquisición de productos de seguridad.
- ❓ Artículo 19. Seguridad por defecto.
- ❓ Artículo 20. Integridad y actualización del sistema.
- ❓ Artículo 21. Protección de información almacenada y en tránsito.
- ❓ Artículo 22. Prevención ante otros sistemas de información interconectados.
- ❓ Artículo 23. Registro de actividad.
- ❓ Artículo 24. Incidentes de seguridad.
- ❓ Artículo 25. Continuidad de la actividad.
- ❓ Artículo 26. Mejora continua del proceso de seguridad.
- ❓ Artículo 27. Cumplimiento de requisitos mínimos.
- ❓ Artículo 28. Infraestructuras y servicios comunes.
- ❓ Artículo 29. Guías de seguridad.
- ❓ Artículo 30. Sistemas de información no afectados.



Herramientas
CCN-CERT



Guías CCN-STIC





GUÍAS CCN-STIC

- Índice de guías >
- Series completas >
- Glosario de Términos (CCN-STIC 401) >
- Serie 800 (ENS) >
- Últimas guías CCN-STIC >

Guías CCN-STIC de Seguridad

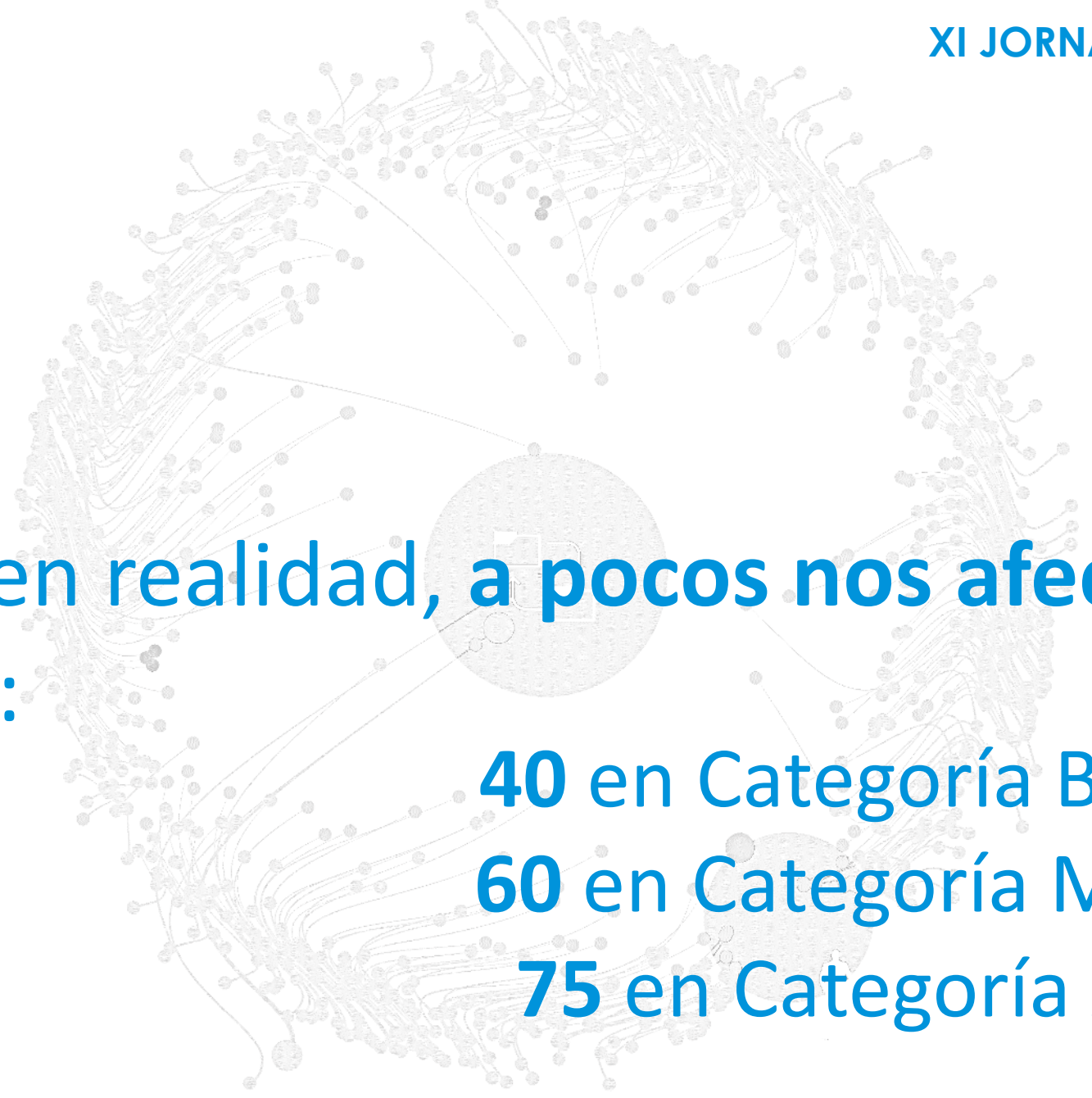
Las Series CCN-STIC son normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional con el fin de mejorar el grado de ciberseguridad de las organizaciones. Periódicamente son actualizadas y completadas con otras nuevas, en función de las amenazas y vulnerabilidades detectadas por el CCN-CERT. El grueso de las Series están especialmente dirigidas al personal de las Administraciones Públicas y empresas y organizaciones de interés estratégico (parte privada del portal) y otras de difusión pública para todos los usuarios. De igual modo, algunas de las series están clasificadas como Difusión Limitada (DL) o Confidencial (C) y por tanto, es necesaria su solicitud al CCN-CERT.

Más información: guias@ccn.cni.es



Cuidado con la Infoxicación: No tenemos que leer las 295 guías publicadas, a fecha de Noviembre de 2017





Aunque en realidad, **a pocos nos afectan las 75 medidas:**

40 en Categoría Básica (53%)

60 en Categoría Media (80%)

75 en Categoría Alta (100%)



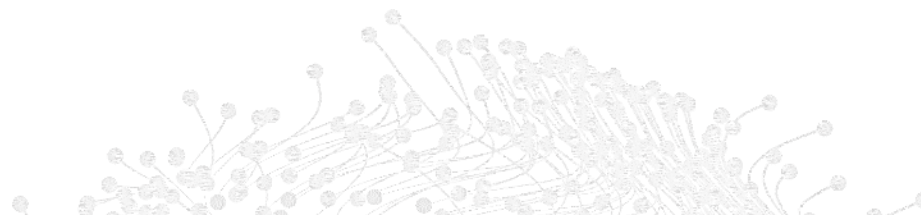
ENS. Valoración de los sistemas



Noviembre 2017

Incluso pueden ser MENOS medidas
pues:

“ Las medidas de seguridad se aplican por dimensión”



Noviembre 2017

CCN-STIC-803

Categoría que se ha asignado al/los sistema(s) de << Nombre de la entidad >> es:

(Categoría): [C(Nivel), I(Nivel), D(Nivel), A(Nivel), T(Nivel)]

Figura 2. Categorización de un Sistema junto a los Niveles en sus Dimensiones de Seguridad.

Ejemplos:

CATEGORÍA BÁSICA: [C(N/A), I(B), D(B), A(B), T(B)]

CATEGORÍA MEDIA: [C(N/A), I(B), D(B), A(M), T(B)]

CATEGORÍA ALTA: [C(M), I(B), D(A), A(M), T(B)]



¿Qué aspectos **SI** vamos a
tratar?



Hablaremos de aplicar el modelo de forma práctica

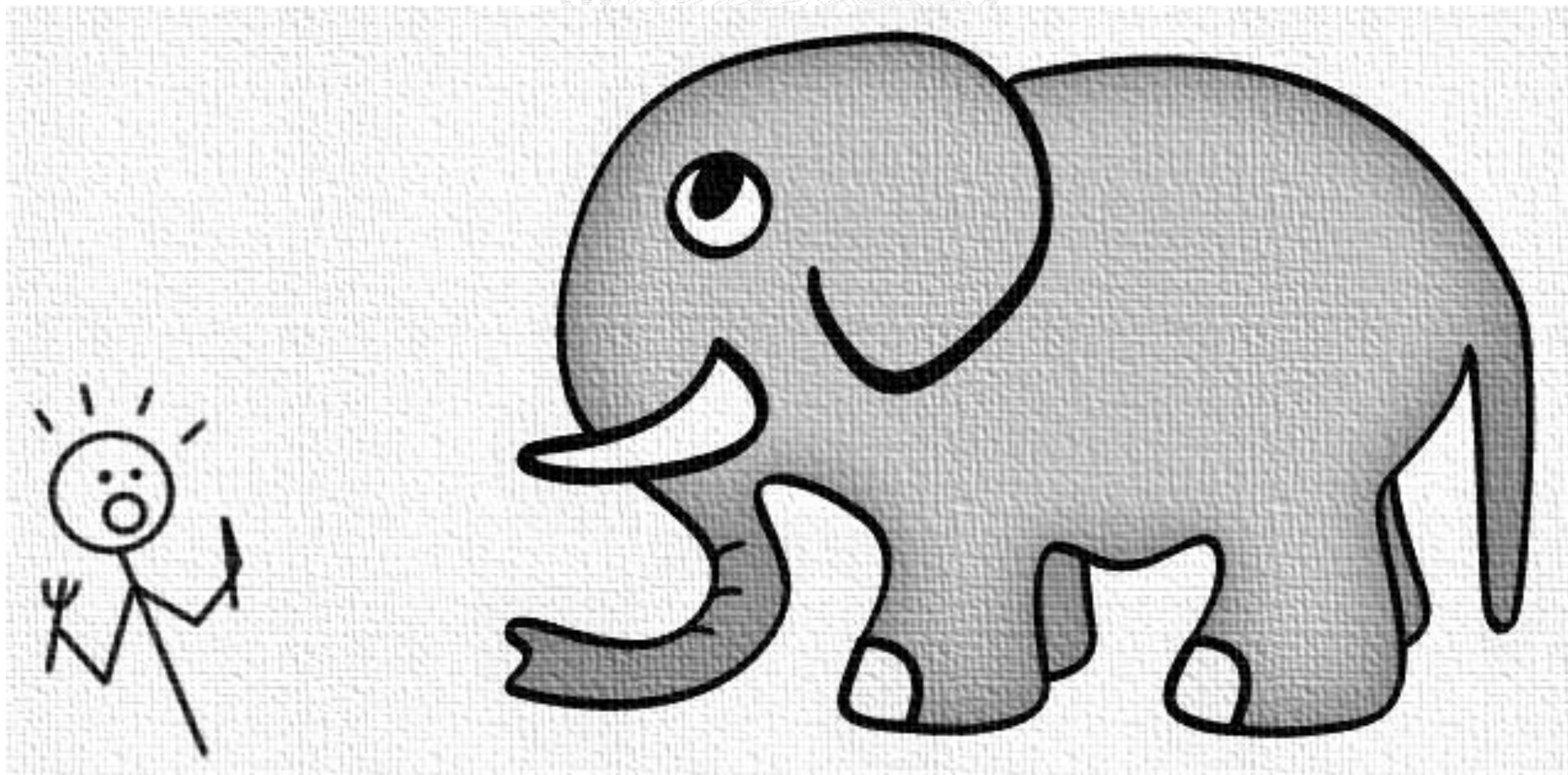
- ES +



¿Cuál es nuestro reto?



Definir la estrategia para...



*“Nada es especialmente
difícil si lo dividimos en
tareas pequeñas.”*

Henry Ford

EL MODELO IDEAL (ESCRITO EN PAPEL)

BUSCA Crear las condiciones necesarias de **CONFIANZA** en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de la información y los servicios electrónicos, que permita a los ciudadanos y a las AA.PP, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

PARA ELLO Debemos establecer la política de seguridad en la utilización de medios electrónicos constituida por los **PRINCIPIOS BÁSICOS Y LOS REQUISITOS MÍNIMOS** para una protección adecuada de la información

MEDIANTE la adopción de medidas de seguridad **EN PROPORCIÓN** a la naturaleza de la información y los servicios a proteger.

Y AFECTA A

TODOS los sistemas de información, con independencia de que exista o no tratamiento de datos personales o que su tramitación sea a través de sede electrónica. También afecta a los **PRESTADORES DE SERVICIO**, públicos y privados.

Esta determinación se encuentra regulado por las Leyes 39 /2015 y 40/2015.

- ES +

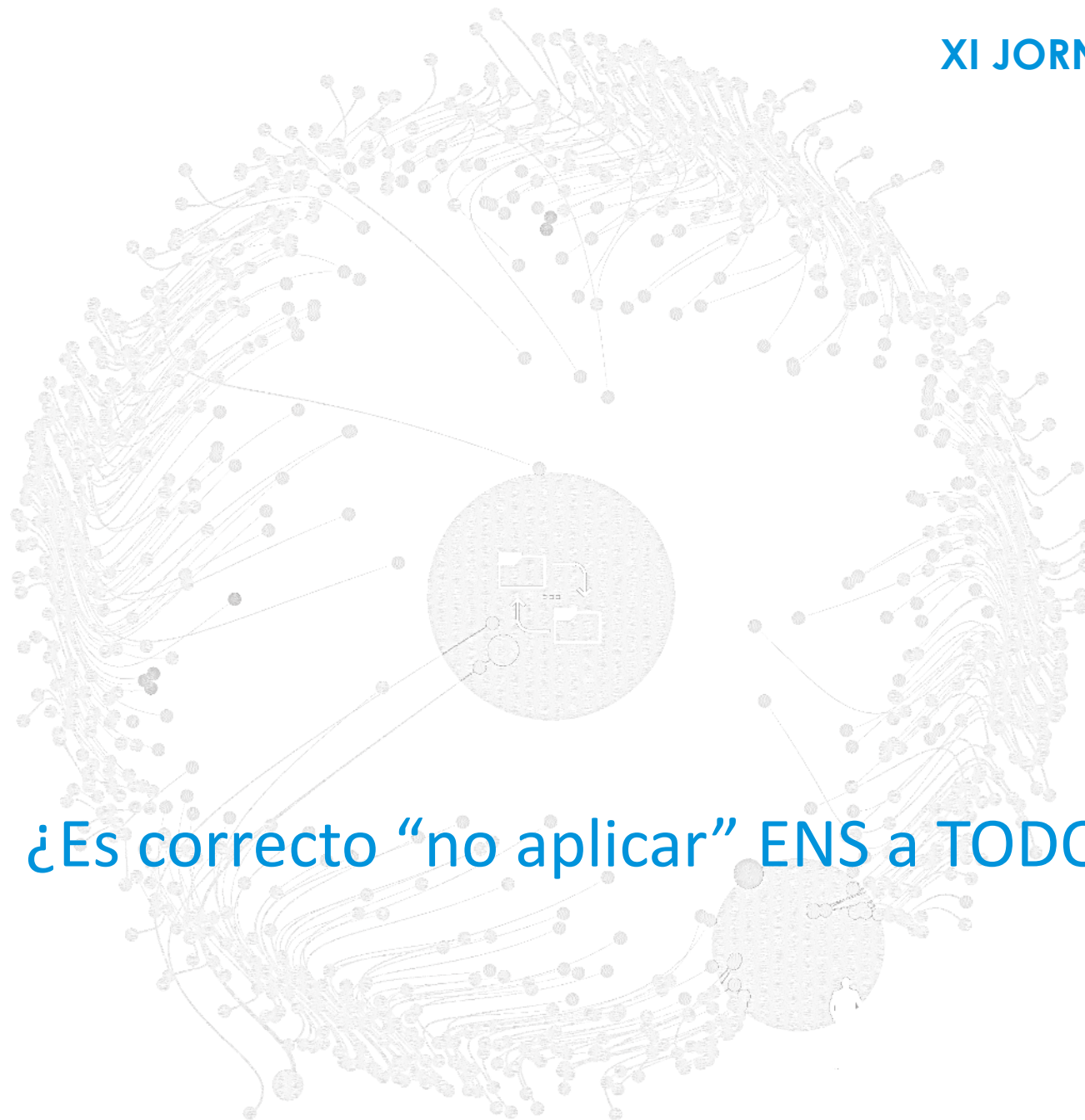
Para ello, empezamos por **olvidarnos** de la palabra ~~TODOS~~

Y nos quedamos con las palabras:

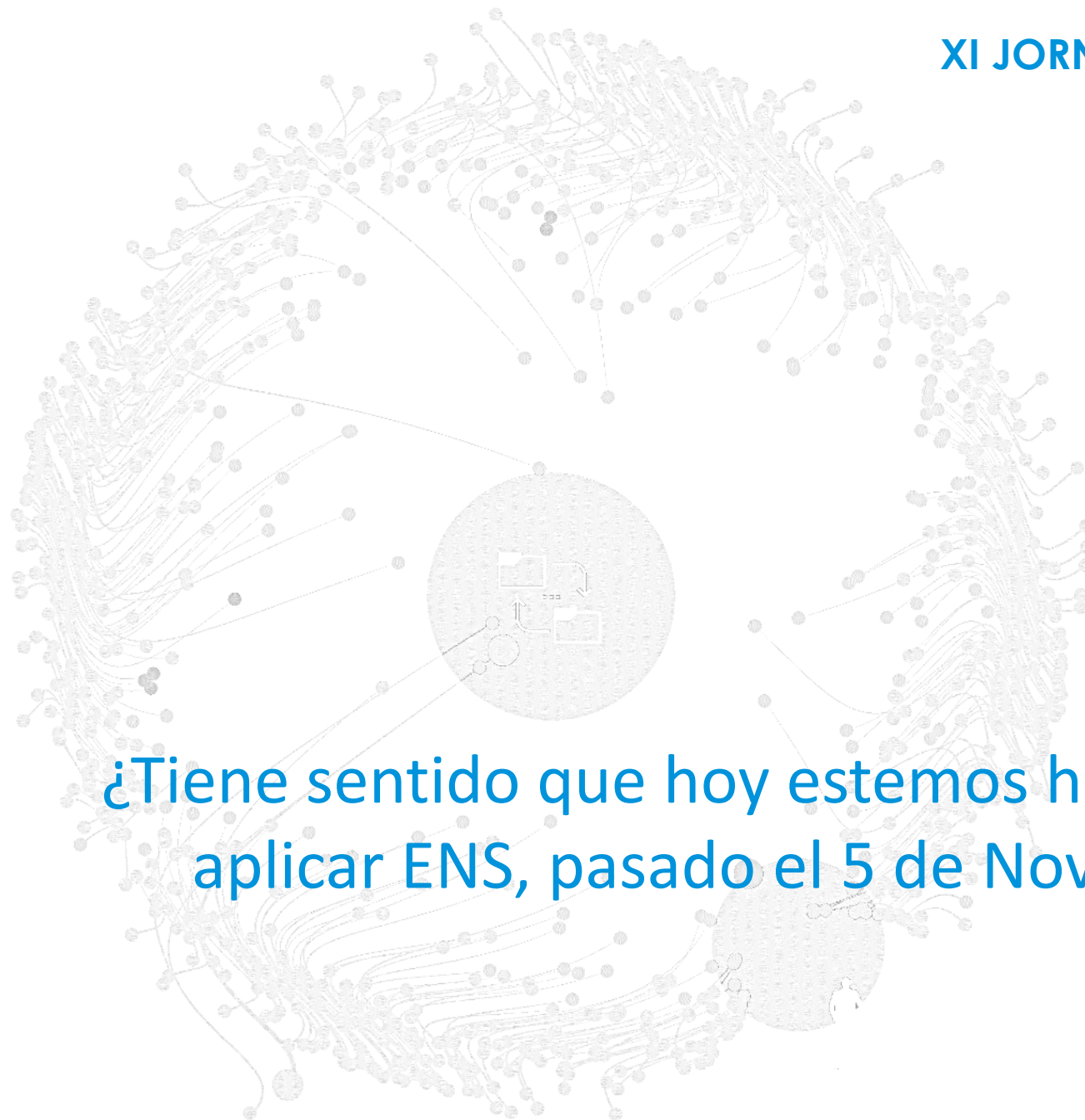
BÁSICOS Y MÍNIMOS (Art. 4 y Art. 11)

PROPORCIONAL (Art. 11)

[*] El Art. 11.3 Los requisitos mínimos se exigirán en PROPORCIÓN a los riesgos identificados en cada sistema.



Miguel,
¿Es correcto “no aplicar” ENS a TODOS los sistemas?



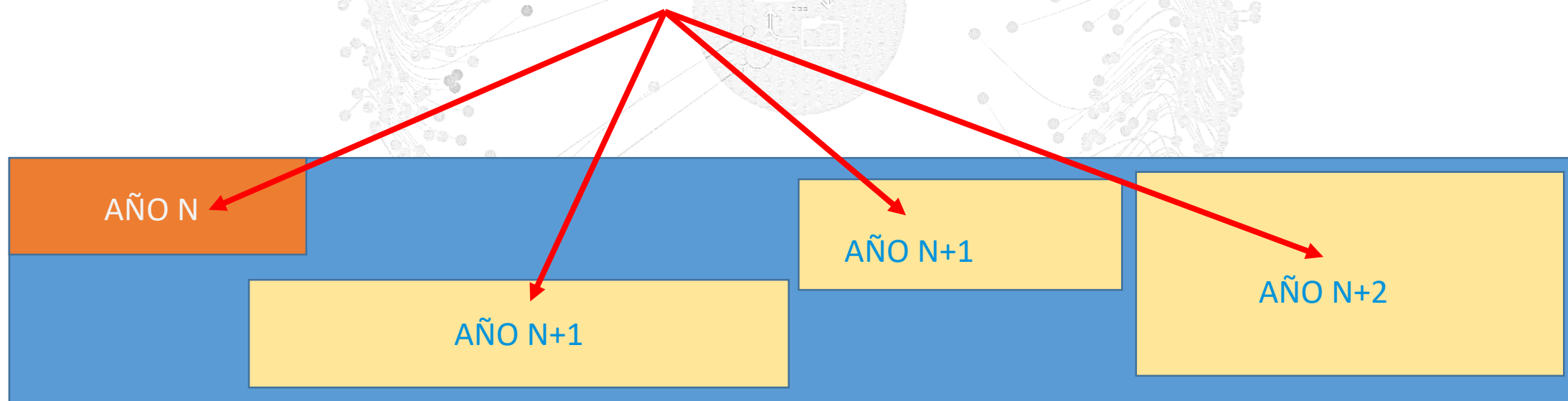
¿Tiene sentido que hoy estemos hablando de cómo aplicar ENS, pasado el 5 de Noviembre de 2017?

- ES +

AMBITO MATERIAL “PROGRESIVO”

Nuestra primera decisión, para abordar el cumplimiento del ENS, es la determinación de un ámbito de aplicación material **PARCIAL Y PROGRESIVO**. **Determinado el ámbito ideal, buscamos un enfoque práctico:**

PRIMERA PROPUESTA Segregar en diferentes subsistemas y buscar la **conformidad progresiva en el tiempo**.



Posicionar FOCO en un subsistema:

- ES +

.El ideal no tiene por qué ser el más importante, sino el **más factible**.

.Estas buscando que **tu organización empiece a interiorizar los procesos de conformidad** (que se acostumbre a someterse a procesos de auditoría)

Esta estrategia NO te dice que dejes de aplicar medidas al resto de elementos.

- ES +

AMBITO MATERIAL “PROGRESIVO”

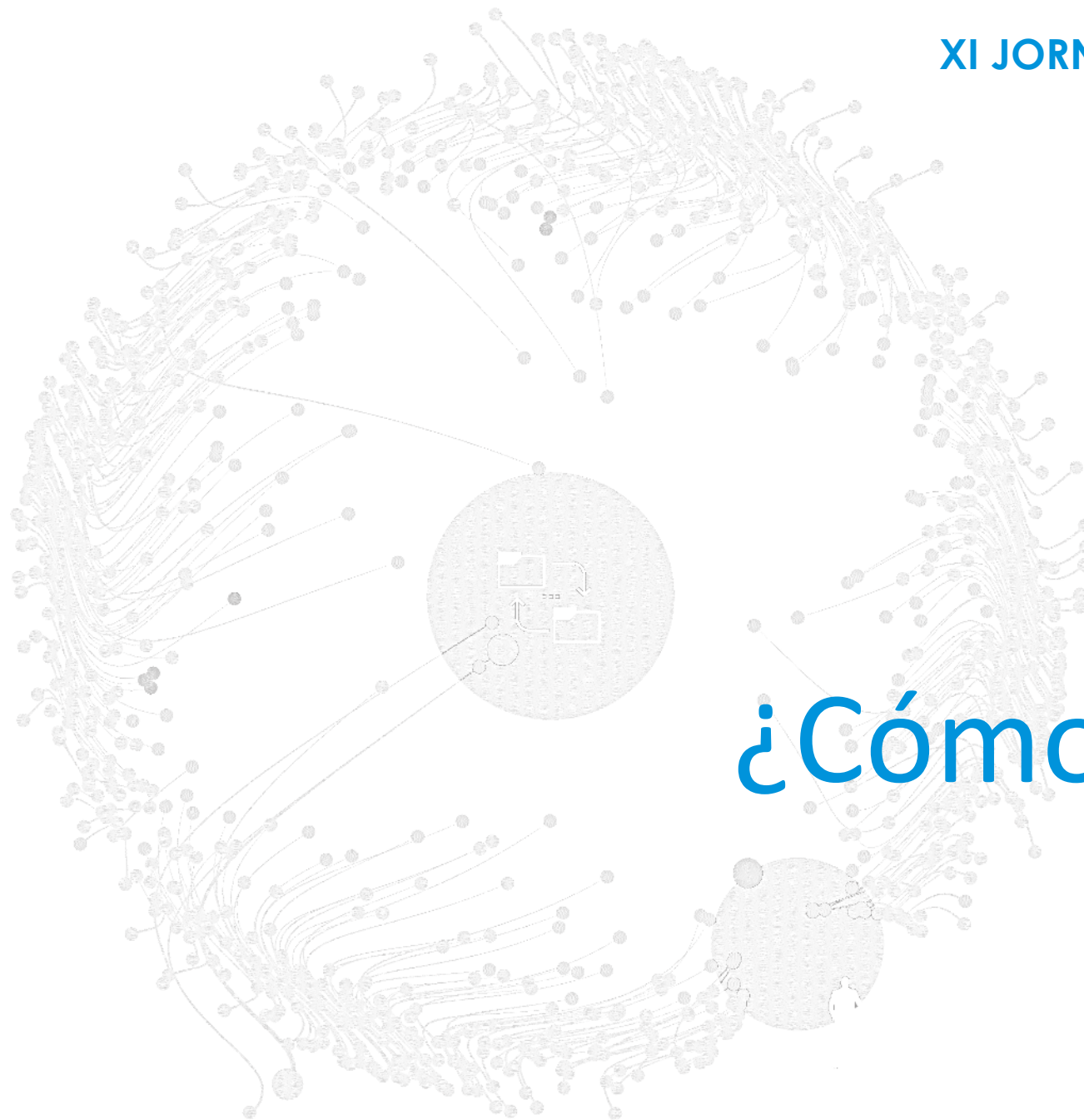
Dentro de la determinación del ámbito de aplicación se encuentran los **operadores del sector privado**

SEGUNDA PROPUESTA Identificar nuestros terceros actuales, analizando si los servicios o las soluciones prestadas están afectados por el Esquema Nacional de Seguridad.



...



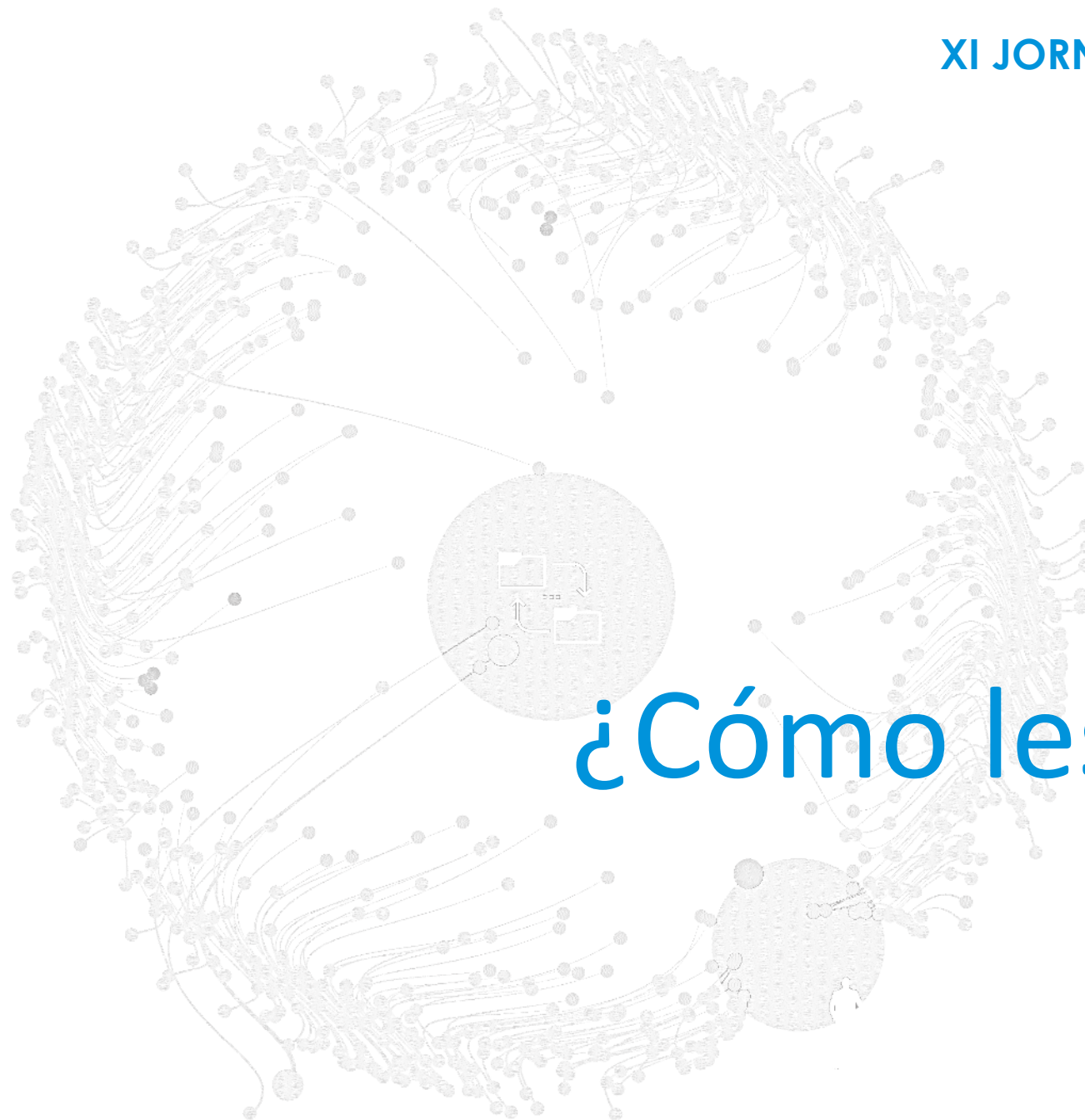


¿Cómo lo hago?



EJEMPLO	DESCRIPCIÓN	¿Requiere pedir Declaración/ Certificación ENS al proveedor?
Sistemas de Ciudades Inteligentes e Internet de las Cosas	Soluciones vinculadas con el desarrollo de productos, servicios o plataformas Smart, incluyendo Sistemas SCADA (<i>Supervisory Control and Data Acquisition</i>), como por ejemplo sistemas de control semafórico, alumbrado inteligente, etc.	Requiere solicitar declaración / certificación El alcance deberá cubrir la prestación completa de la solución y/o servicio. Este tipo de sistemas son especialmente críticos, ya que existe una falta de madurez, en materia de seguridad, en los sistemas industriales.
Empresas de consultoría	Empresas que desarrollan procesos de consultoría, como por ejemplo el desarrollo de un plan estratégico de ciudad, estudios de impacto, etc.	NO precisa declaración ni certificación
Empresas de consultoría y servicios de seguridad	Empresas proveen de soluciones, como por ejemplo soluciones de monitorización de equipos	Requiere solicitar declaración / certificación Requiere certificación que cubra la forma en la que se desarrolla la prestación del servicio. En caso de la existencia de productos de seguridad se deberá analizar la utilización adicional de productos certificados.





¿Cómo les obligo?



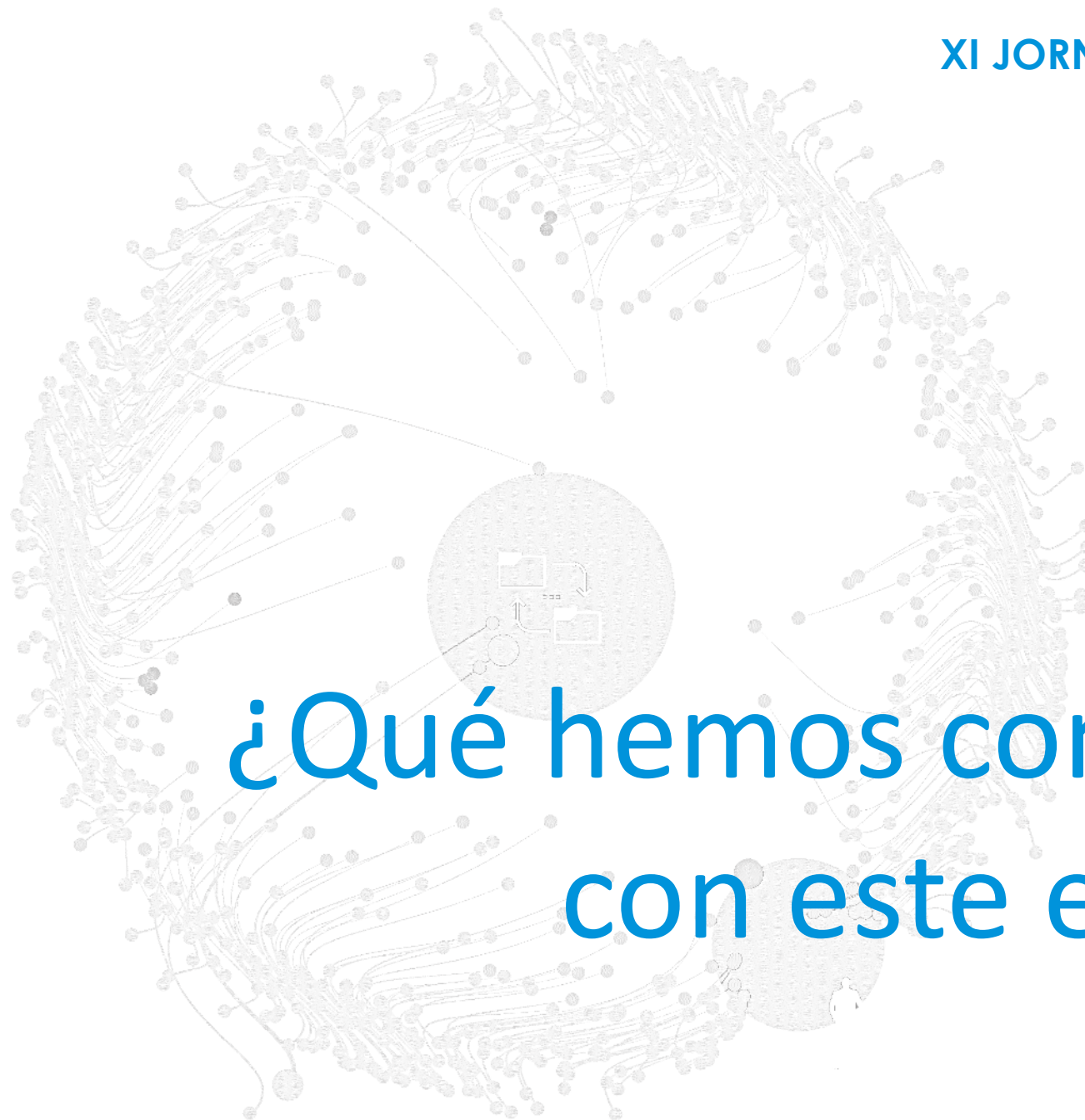
De forma **proporcionada** y
pensando en global...

¿Sería adecuado, en el año 2017, establecer ENS como criterio de solvencia? ¿Es Proporcional?

“Cumplimiento indirecto:” Todas las Administraciones tendremos que requerir a los proveedores, **de forma gradual**, que nos proporcionen servicios seguros, es decir, conformes a ENS.

Trabajamos en equipo

(Mismo modelo que Listado Unificado de Coordinación de Incidentes y Amenazas)



¿Qué hemos conseguido
con este enfoque?

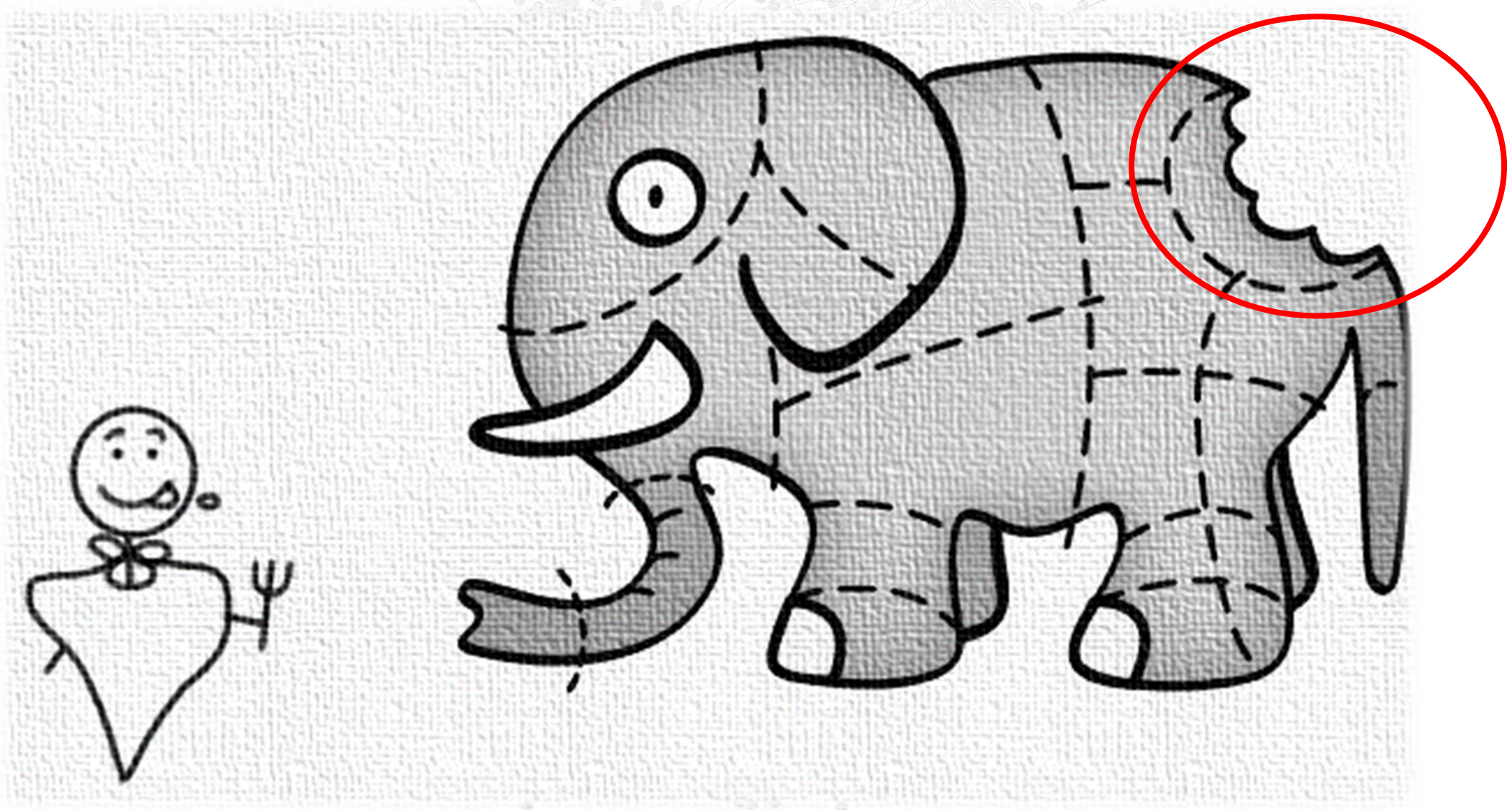
- ES +

¿Qué hemos conseguido?

Tener una estrategia gradual de conformidad (no pienses en lo que te falta, sino en lo que has conseguido)

Gradual, implica trabajar de forma continuada en el tiempo y no a “tirones” (Sensación de avance)

Incrementar el nivel de cumplimiento del sector privado de forma progresiva (conseguir la conformidad de las soluciones o servicios de un operador implica un beneficio para todas las AAPP)





¿Por dónde “seguimos”?

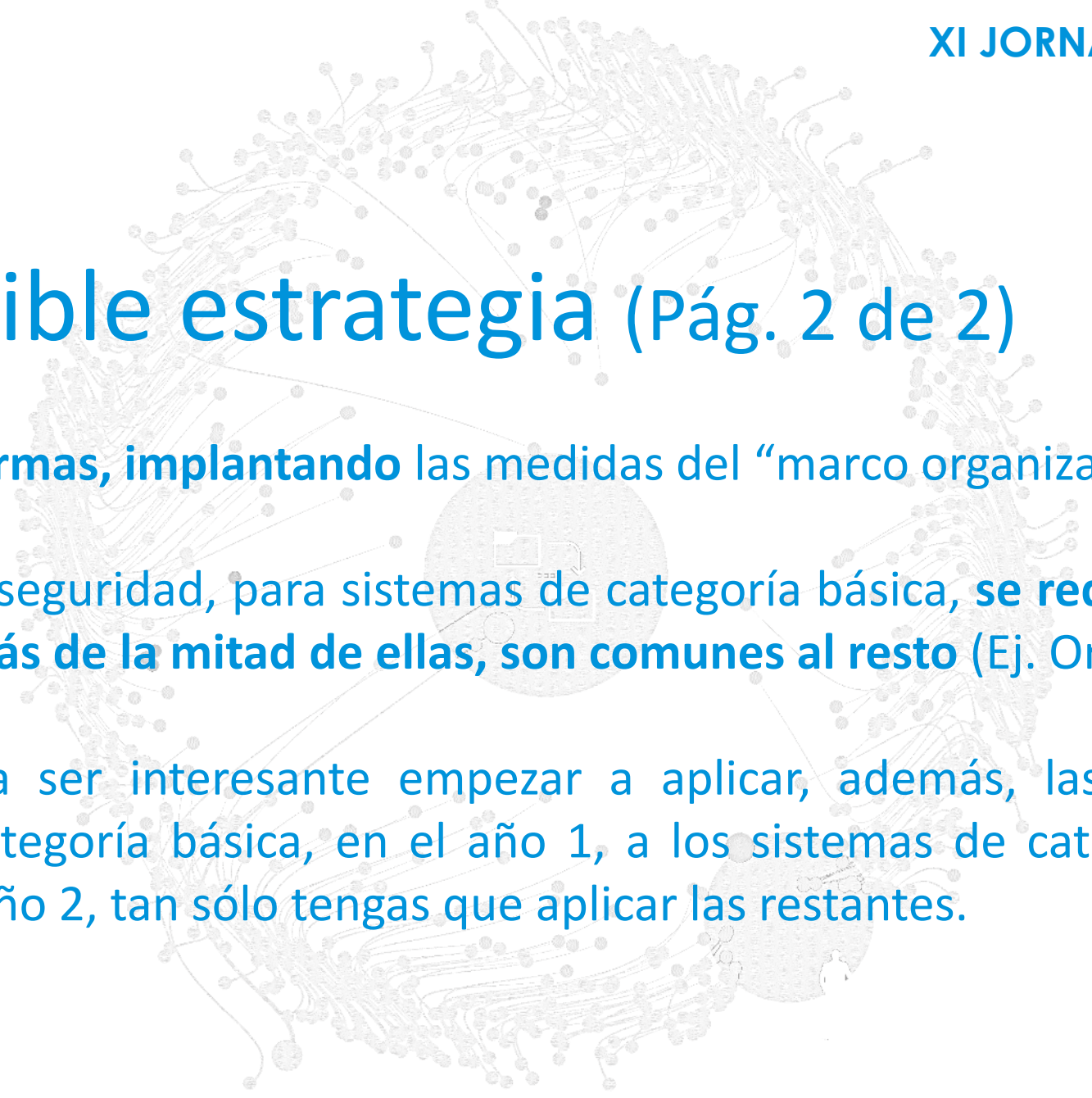
- ES +

Una posible estrategia (Pág. 1 de 2)

Puedes empezar/continuar, por ejemplo, situando el foco en un sistema sencillo, **pero que “requiera” someterse a una auditoría externa** (aunque sea de categoría BÁSICA).

Podría ser interesante, seleccionar sistemas en los que de forma activa estén implicados **terceros (proveedores)**, que ya dispongan de la conformidad con el ENS, de la solución o servicio prestado (te facilitarán muchos controles)

O bien, sistemas sobre los que **ya dispongas de un SGSI**, dentro del sistema de información.

 - ES +

Una posible estrategia (Pág. 2 de 2)

Cimentar las normas, implantando las medidas del “marco organizativo”

Las medidas de seguridad, para sistemas de categoría básica, **se reducen de 75 a tan sólo 40, y más de la mitad de ellas, son comunes al resto** (Ej. Organizativas)

También, podría ser interesante empezar a aplicar, además, las medidas de seguridad de categoría básica, en el año 1, a los sistemas de categoría media, para que en el año 2, tan sólo tengas que aplicar las restantes.

Importante sobre tus terceros

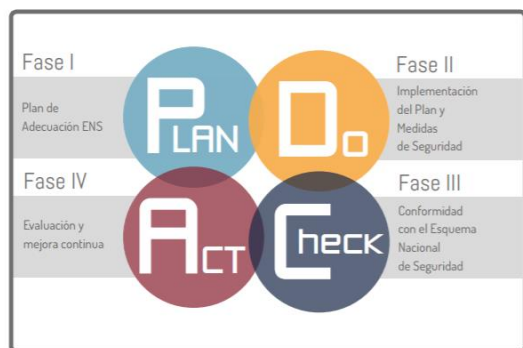
Deberemos de revisar no sólo el alcance en la prestación de los servicios, sino cada una de las dimensiones.

Categoría que se ha asignado al/los sistema(s) de << Nombre de la entidad >> es:

(Categoría): [C(Nivel), I(Nivel), D(Nivel), A(Nivel), T(Nivel)]

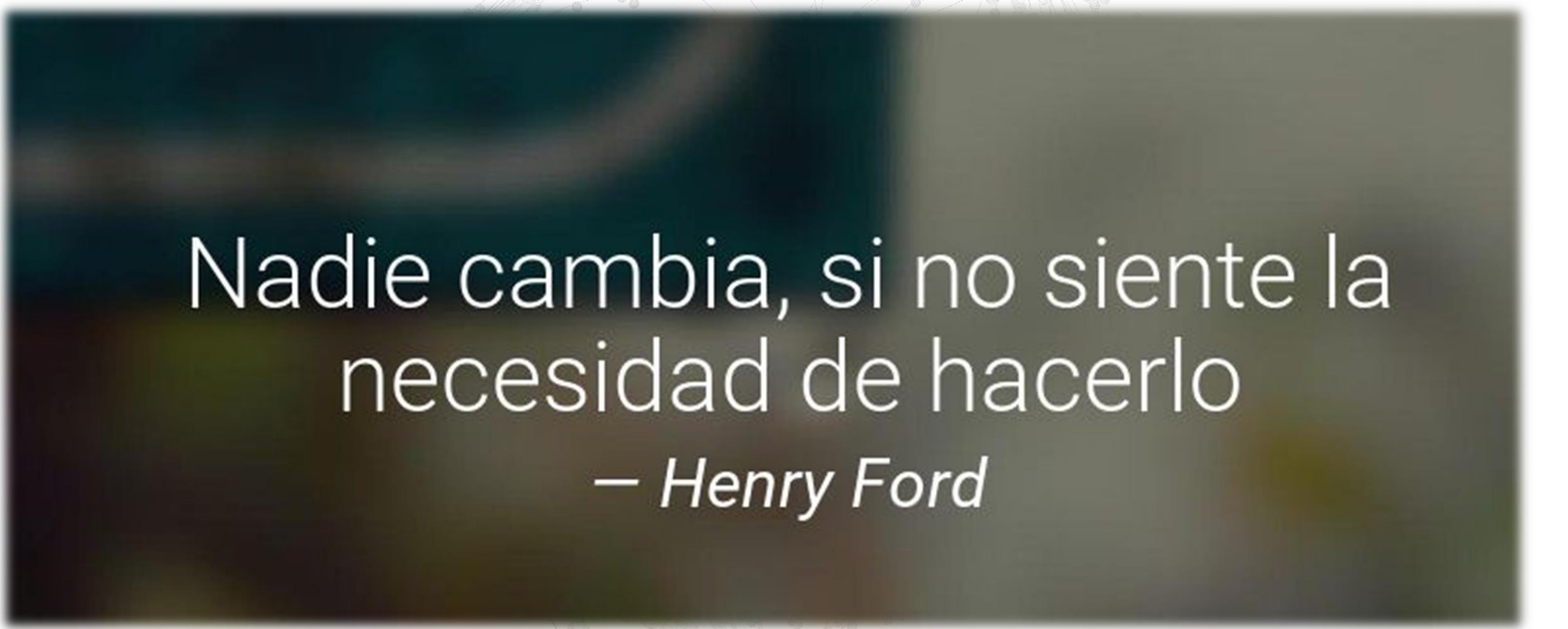
Cuando un sistema contribuya a la prestación de servicios esenciales de terceros o contenga información que pueda poner en riesgo la seguridad de esos servicios esenciales de terceros, deberá determinarse si a las medidas de seguridad requeridas por el Esquema Nacional de Seguridad **deben añadirse medidas adicionales requeridas por las infraestructuras críticas.**

- ES +



ALGUNAS IDEAS

(Recorrido simplificado sobre
algunas fases del ENS)



Nadie cambia, si no siente la
necesidad de hacerlo
— *Henry Ford*

Prepara al personal: Usuari@s

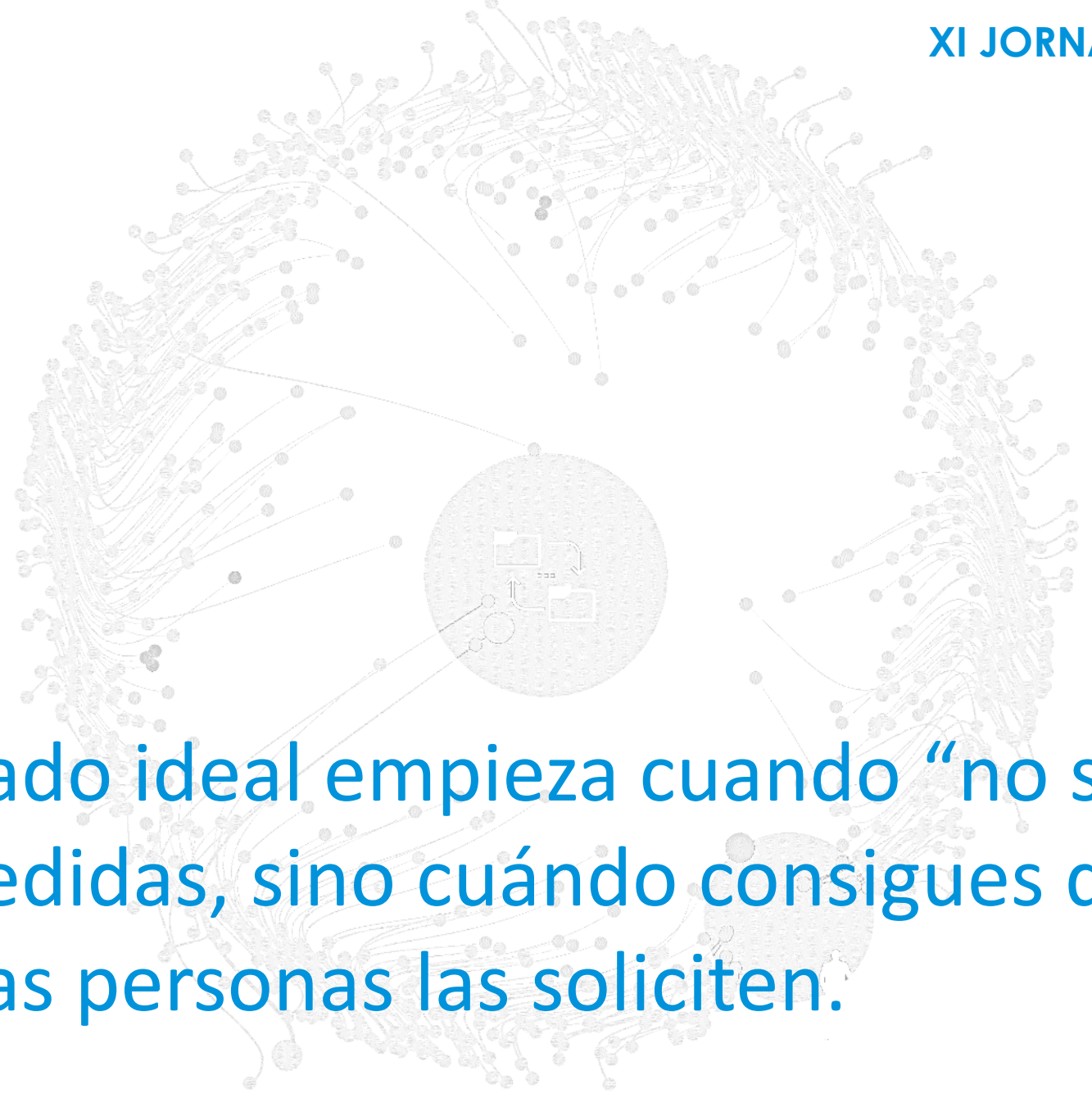
Empieza **creando necesidad**, a través de cursos de sensibilización continuados (Crear Demanda)

Enseña a que los propios usuarios **vean, en primera persona, los riesgos y comprendan** la necesidad de aplicar medidas.

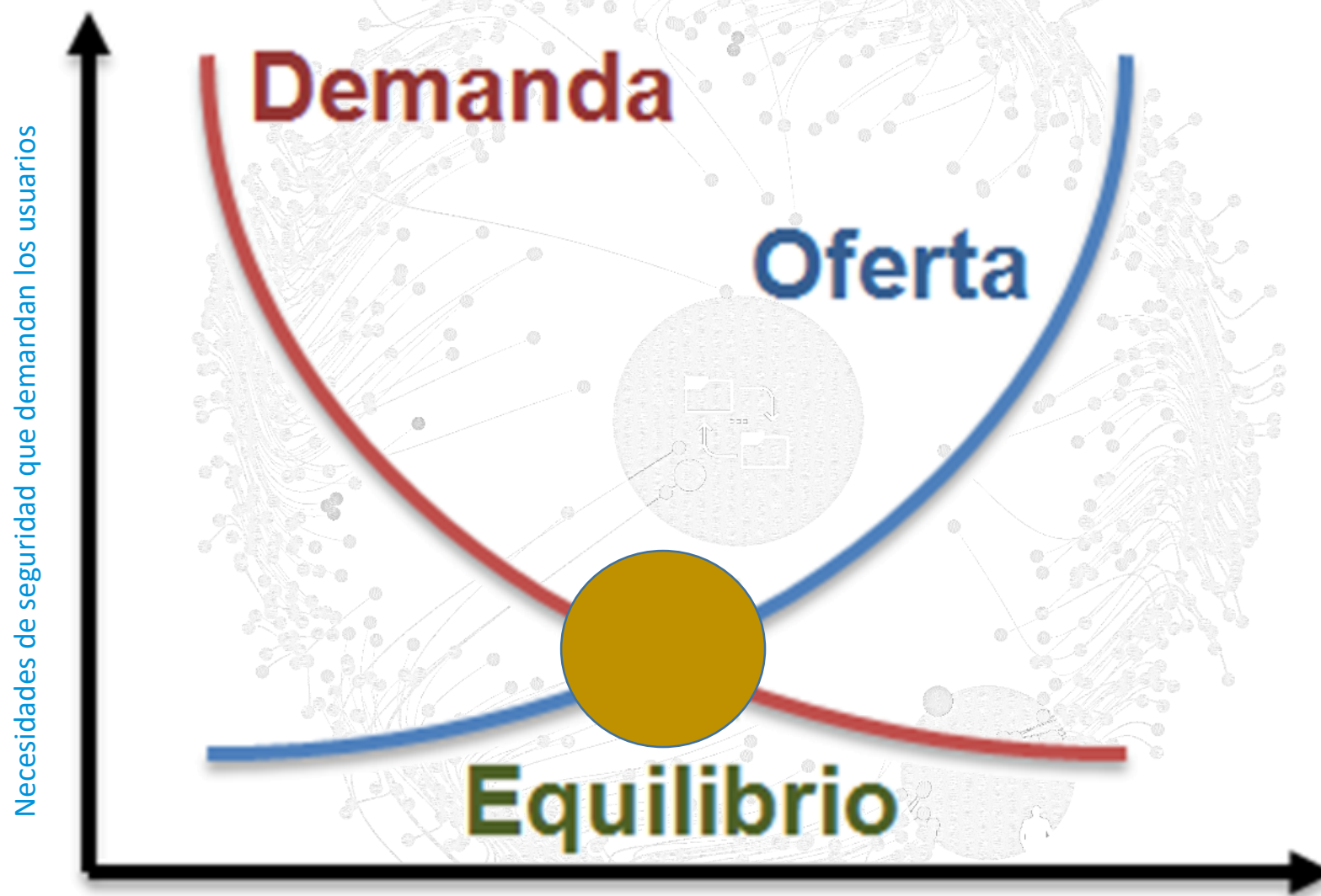
Siempre que **quites algo, da algo a cambio** (Ej. Gestor de credenciales)

Busca medidas de seguridad sean **viables/ sencillas** de aplicar

Mixed Alpha AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz		Class of Attack					
Password		Class of Attack					
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	2,704	Instant	Instant	Instant	Instant	Instant	Instant
3	140,608	14 Secs	< 2 Secs	Instant	Instant	Instant	Instant
4	7.3 Million	12½ Mins	1¼ Mins	8 Secs	Instant	Instant	Instant
5	380 Million	10½ Hours	1 Hour	6 Minutes	38 Secs	4 Secs	Instant
6	19 Billion	23 Days	2¼ Days	5½ Hours	33 Mins	3¼ Mins	19 Secs
7	1 Trillion	3¼ Years	119 Days	12 Days	28½ Hours	3 Hours	17 Mins
8	53 Trillion	169½ Years	17 Years	1½ Years	62 Days	6 Days	15 Hours
9	2.7 Quadrillion	8,815 Years	881 Years	88 Years	9 Years	322 Days	32 Days



El estado ideal empieza cuando “no se imponen”
las medidas, sino cuándo consigues que las
propias personas las soliciten.



Tu oferta de medidas de seguridad para cubrir su necesidad

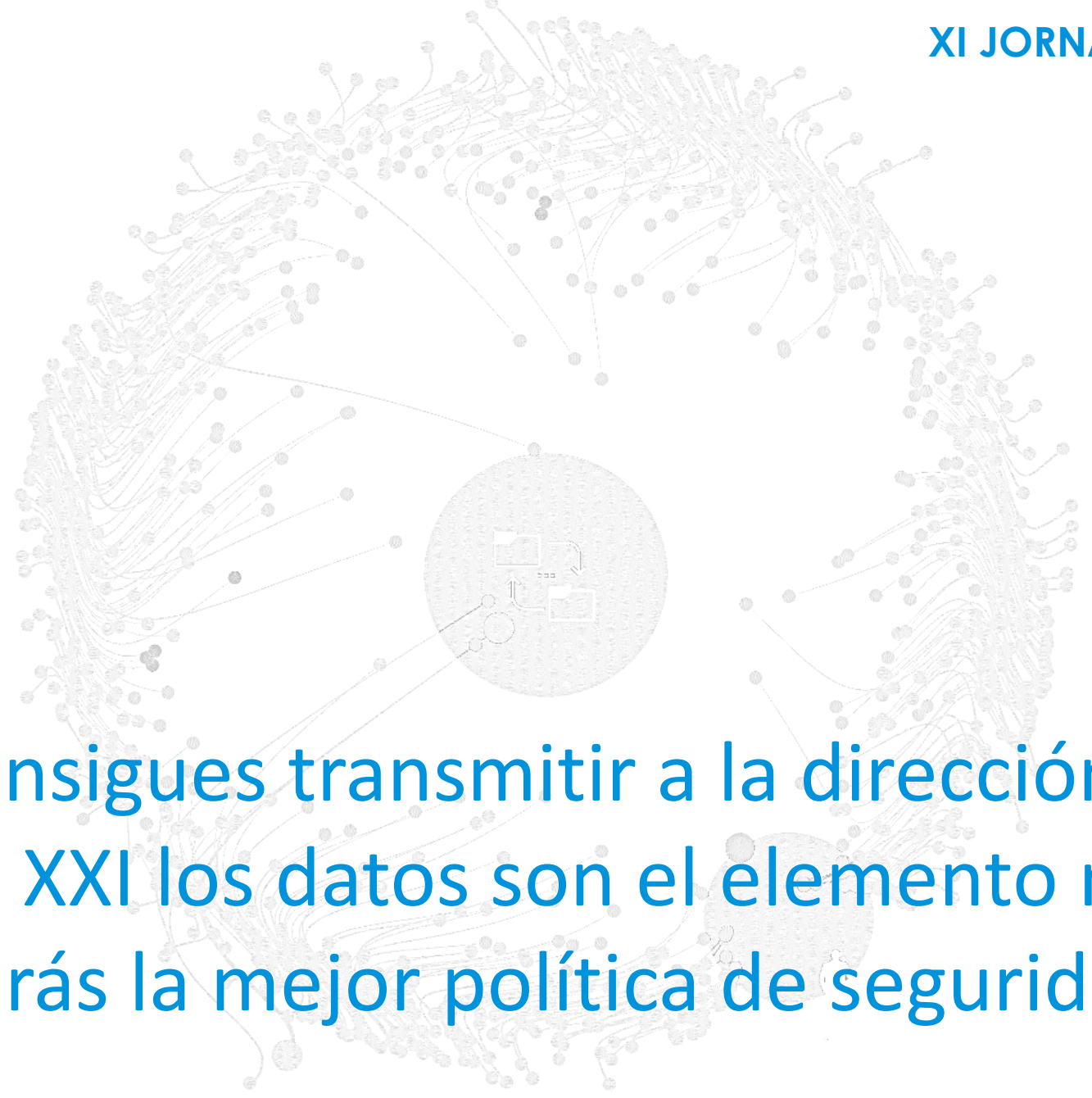
Prepara al personal: Comité de seguridad

La mejor política de seguridad, simplemente es aquella que consigue el **compromiso** de la alta dirección. **Ese es el objetivo, que incorporen la seguridad como elemento clave en su hoja de ruta.**

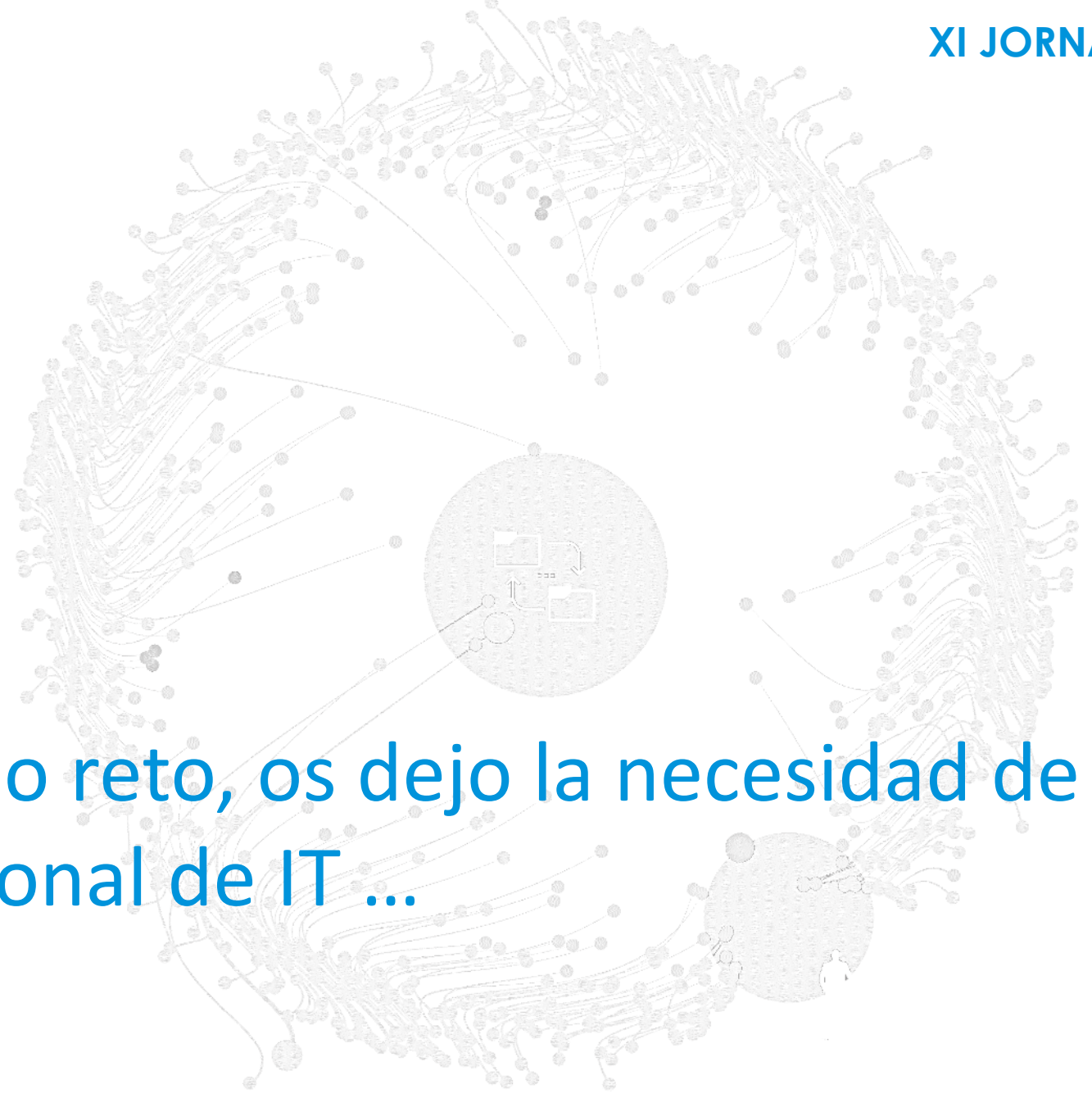
La informática **no debe ser una caja negra para ellos**, pues deben de conocer /comprender los riesgos que asume la organización.

No eres el fin, sino el medio. Muchas cosas no se deciden en informática, sino en el Comité o a través de el Comité. Luego, la dirección ratifica / apoya las medidas.

Debemos de hablar en un **idioma común** (Negocio, ciudadanía...)



Si consigues transmitir a la dirección que en el siglo XXI los datos son el elemento nuclear, tendrás la mejor política de seguridad.



Como reto, os deixo la necesidad de preparar al personal de IT ...

La dificultad de determinar la categoría de los sistemas



Guía de Seguridad de las TIC
CCN-STIC 803



Anexo II: Valoración de sistemas en Entidades Locales

ANEXO II: Valoración de los sistemas en EE.LL.



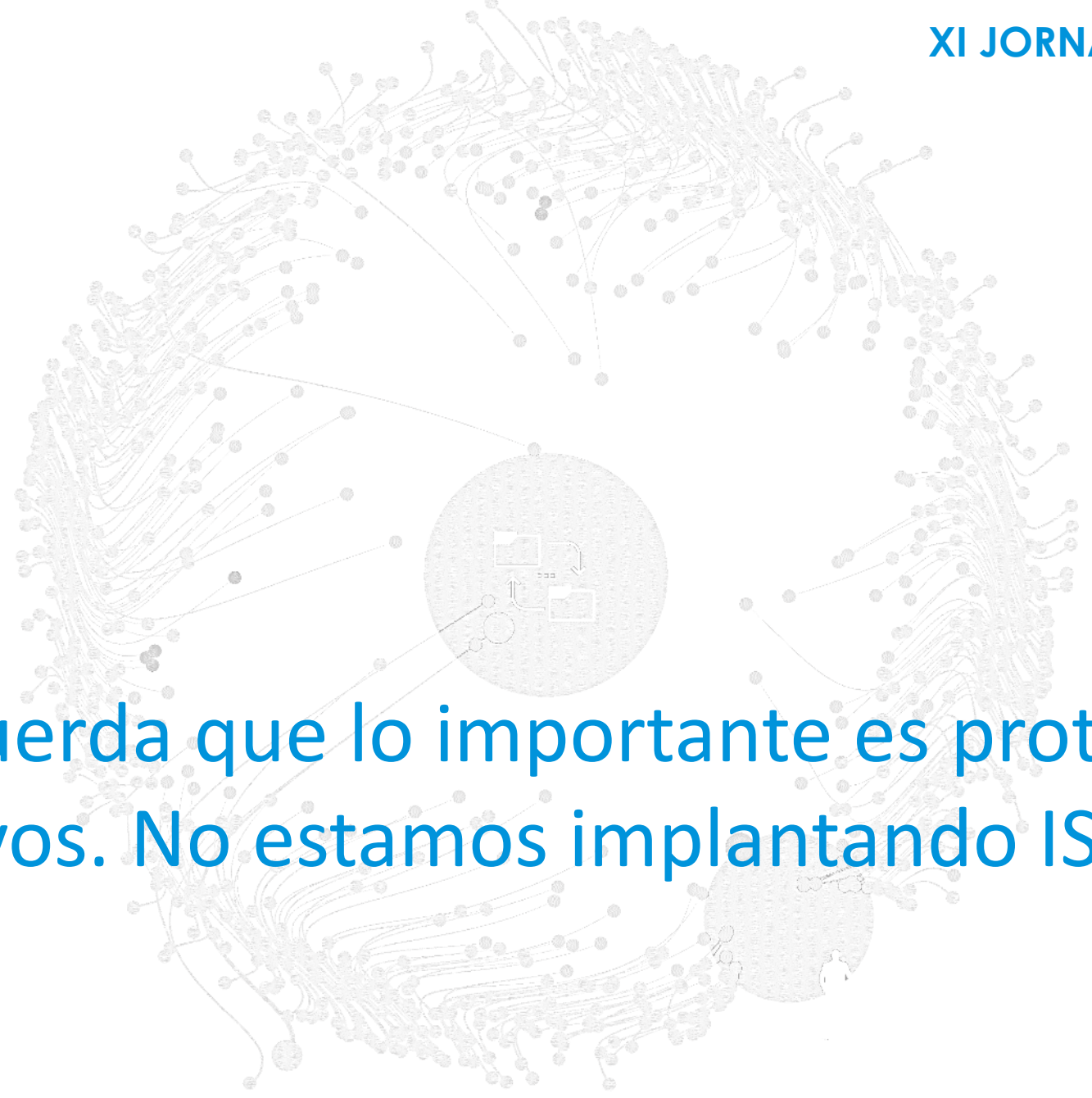
TIPO DE INFORMACIÓN ¹	DESCRIPCIÓN	D P ²	LOPD	C	I	A	T
	derivada.						
FEMP_I_33 Policía Local - Administrativa	Incluye la información necesaria para la gestión operativa de la Policía Local.	SÍ	M	M	M	M	M
FEMP_I_34 Policía Local - Comunicaciones	Comunicación a través de emisores y otros canales de información sensible relacionada con actuaciones policiales.	SÍ	A	M/A	M	M	M
FEMP_I_35 Policía Local – Fines Policiales	Incluye la información necesaria para la gestión operativa de la Policía Local.	SÍ	A	M/A	M	M	M
FEMP_I_36 Protección Civil	Registro de beneficiarios de servicios de protección civil, así como de afectados por servicios sanitarios y preventivos en acontecimientos públicos. Gestión del Voluntariado, su formación y divulgación.	SÍ	A	M	M	M	M

Aplicar medidas por dimensión

Categoría que se ha asignado al/los sistema(s) de << Nombre de la entidad >> es:

(Categoría): [C(Nivel), I(Nivel), D(Nivel), A(Nivel), T(Nivel)]



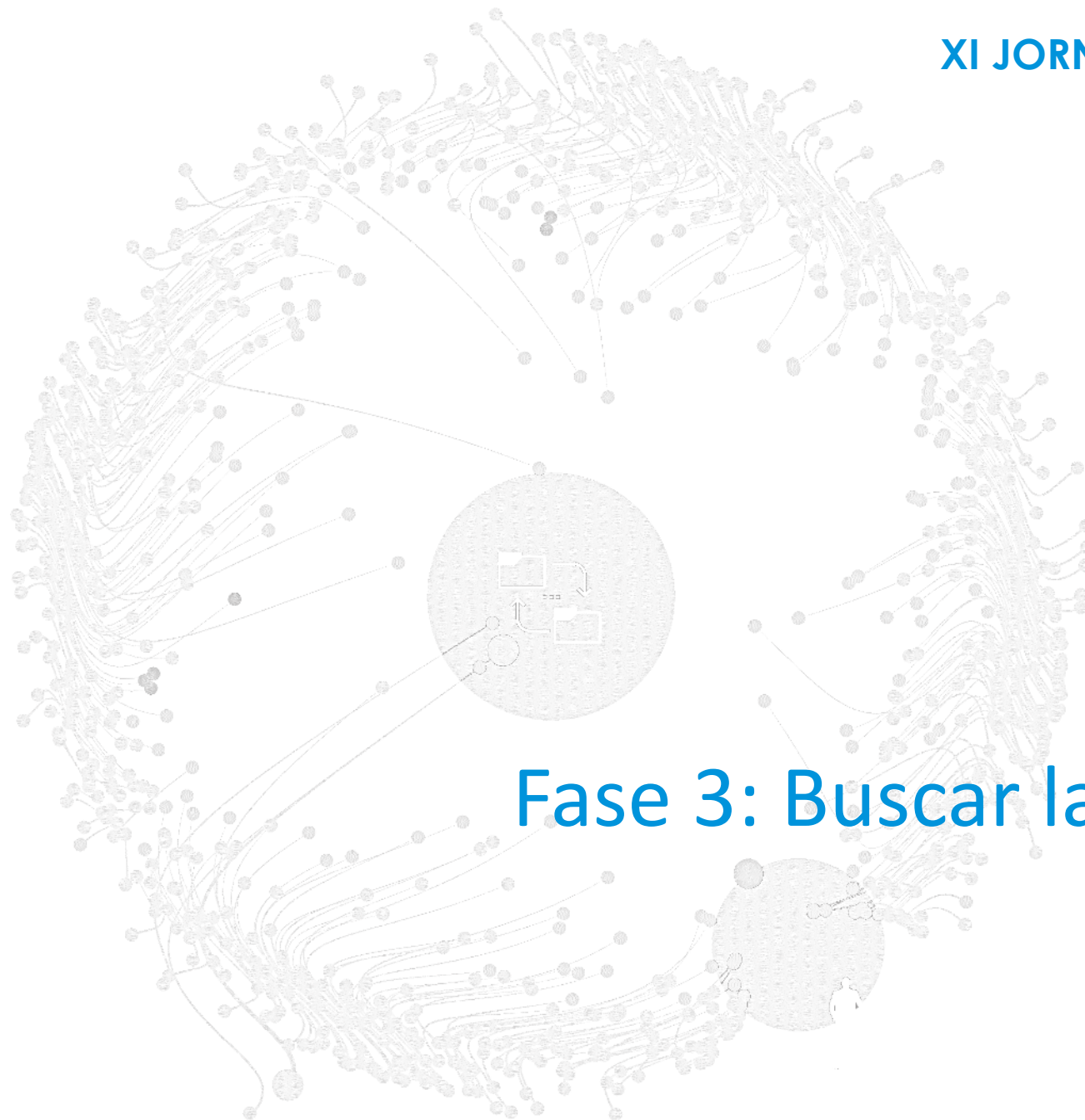


Recuerda que lo importante es proteger los activos. No estamos implantando ISO 27001



INTERACCIÓN ENTRE HERRAMIENTAS

- 1 Sistema de Alerta Temprana en Internet
- 2 Sistema de Alerta Temprana en la red Sara
- 3 Detección de APT
- 4 Análisis dinámico de ficheros
- 5 Multiantivirus
- 6 Análisis y gestión de riesgos
- 7 Auditoría de cumplimiento ENS/STIC
- 8 Informe de estado de seguridad en el ENS
- 9 Inspección de dispositivos de red
- 10 Entornos clasificados
- 11 Gestión de ciberincidentes
- 12 Investigación de ciberincidentes y compartición de inform
- 13 Almacenamiento en la nube
- 14 Plataforma de retransmisión (streaming)



Fase 3: Buscar la conformidad



Nombre	Razón social	Enlace web	Estado Acreditación ENS	Estado Acreditación STIC (DL)
AENOR Internacional S.A.U.	AENOR Internacional S.A.U.	www.aenor.com	ACREDITADA (21/04/2017)	-
Audertis Audit Services, S.L.	Audertis Audit Services, S.L.	www.audertis.es	EN PROCESO	-
BDO Auditores, S.L.P.	BDO Auditores, S.L.P.	www.bdo.es	EN PROCESO	-
Ingeniería de Sistemas para la Defensa de España (ISDEFE)	Empresa pública de consultoría e ingeniería	www.isdefe.es	-	EN PROCESO
LEET Security, S.L.	LEET Security, S.L.	www.leetsecurity.com	EN PROCESO	-
LGAi Technological Center, S.A.	LGAi Technological Center, S.A.	www.appluscertification.com/es	EN PROCESO	-
Lloyd's Register Quality Assurance España, S.L.	Lloyd's Register Quality Assurance España, S.L.	www.lrqa.es	EN PROCESO	-
Eurocertificación	Eurocert Certification Spain S.L.	Desconocida	EN PROCESO	-
Cámara Certifica	Certificación y Confianza, Cámara S.L.U.	camaracertifica.es/	EN PROCESO	-

En esta fase, someteremos nuestros sistemas de información a un proceso de auditoría, considerando que:

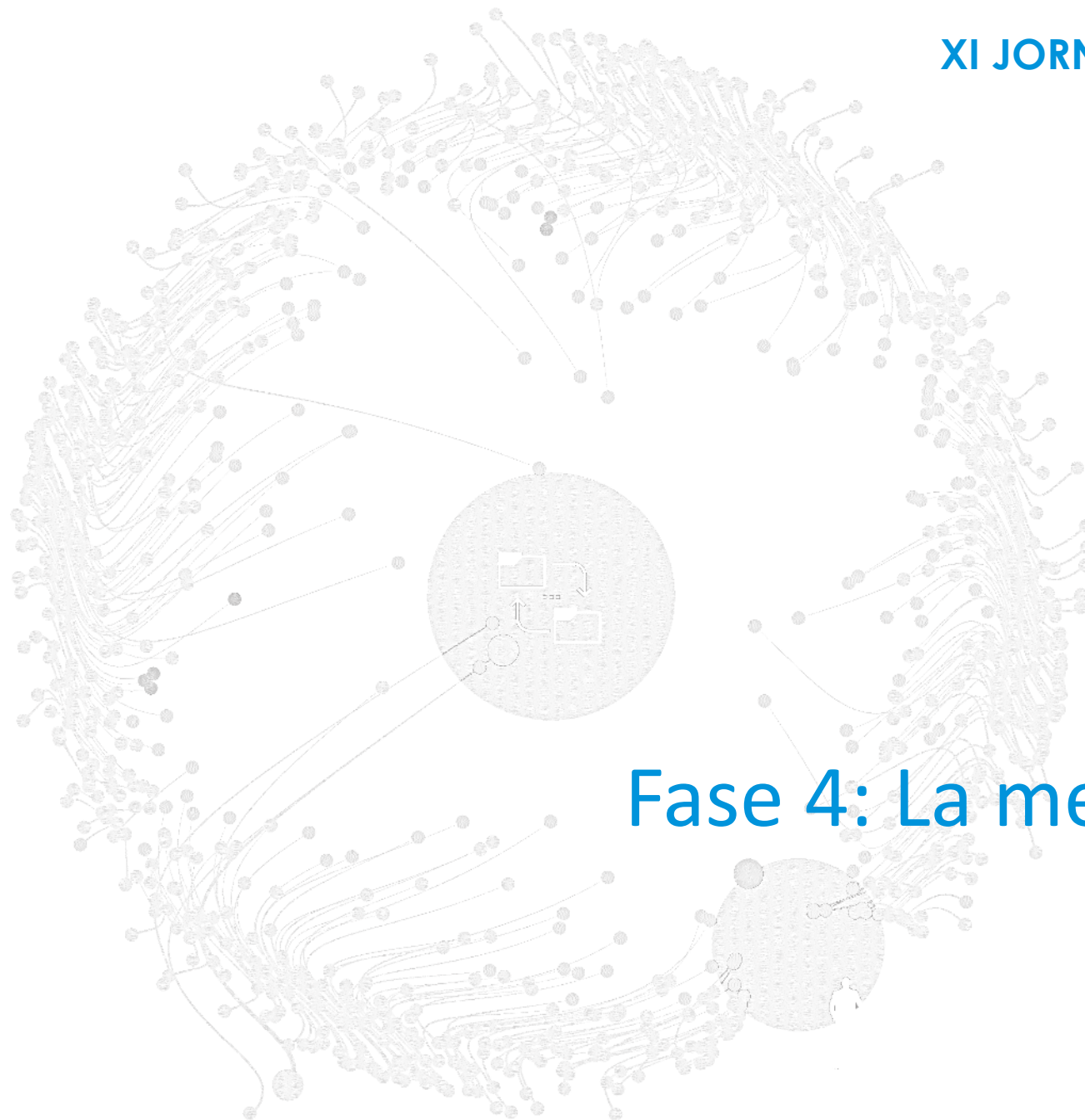
En función del alcance (sistema de información a certificar) el número de jornadas de auditoría **variará**. Quizás, los sistemas de categoría media requieran como mínimo de 3-4 jornadas

Hay una gran diferencia con otros estándares de seguridad, como ISO 27001, pues la evaluación de conformidad **se hace conforme a 17065 y no conforme a 17021**.

Nos encontramos ante una **evaluación de cumplimiento normativo (0 | 1)**

Los procesos de **revisión son cada 2 años**, ¿Demasiado tolerante?

Publicidad conforme a la ITS. ¿La conformidad de los operadores del sector privado serán publicadas en las páginas de las entidades de certificación?



Fase 4: La mejora continua

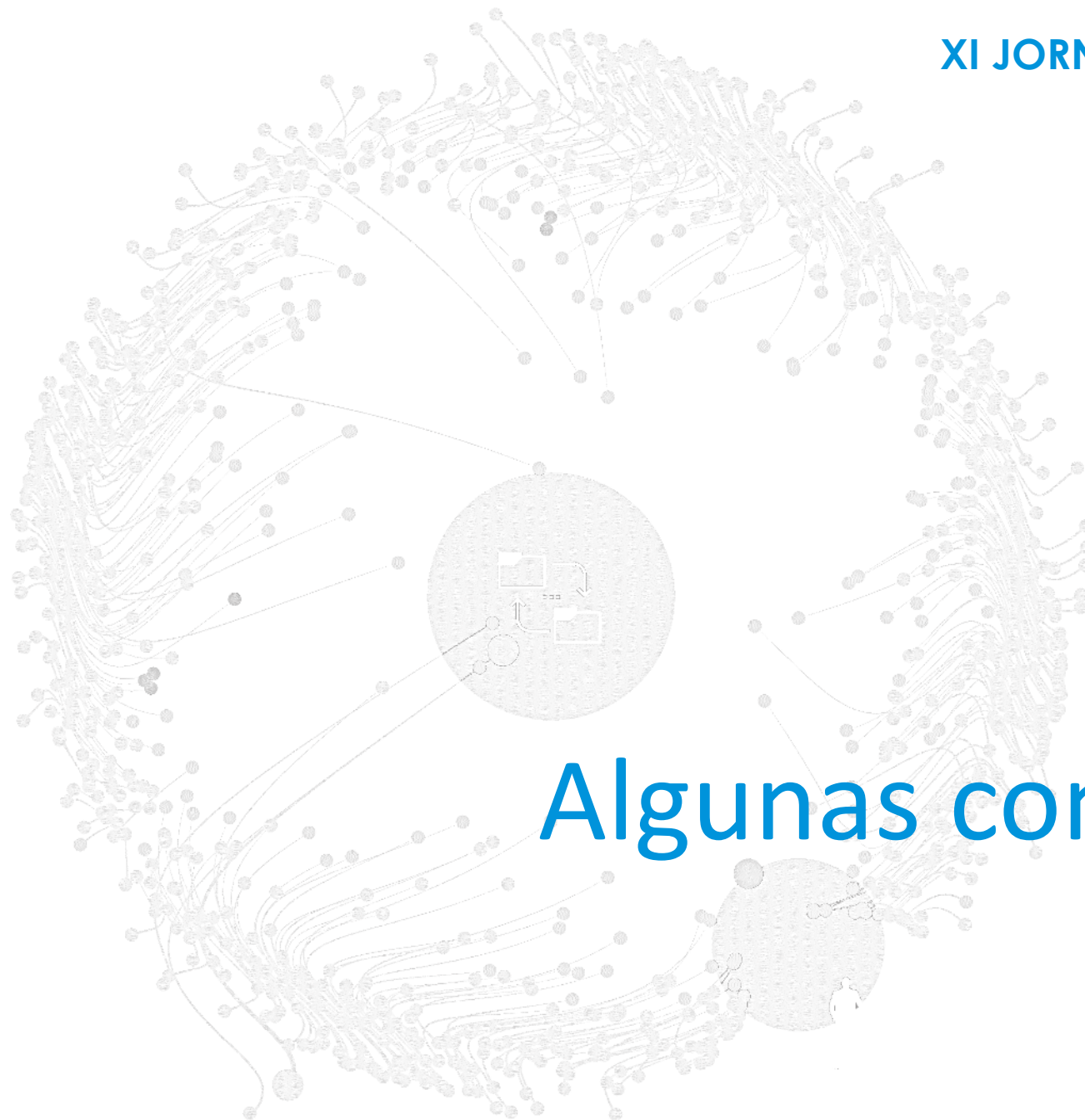
En el primer año

- > Tendremos establecidas las medidas comunes a todos los sistemas, con independencia de la categoría (29 medidas de seguridad comunes a todos los sistemas)
- > Tendremos un SGSI reducido
- > Habremos aplicado 11 medidas de seguridad, adicionales las 29 anteriores, para sistemas de categoría básica. En total, 40 medidas.

En sucesivos años:

- + Introducir nuevos subsistemas en el modelo
- + Aplicar nuevas medidas, para categoría MEDIA, además de incrementar la intensidad de las 11 medidas anteriores





Algunas conclusiones

Conclusiones

Las Declaraciones o Certificaciones de Conformidad con el ENS **se realizan sobre los sistemas de información**, a diferencia de la ISO 27001 que se realiza sobre los sistemas de gestión. **Necesitamos aplicar medidas de seguridad técnicas**

- **ES +** La visión es que la botella está medio llena. Cada año nos queda algo menos por hacer. Buscamos una estrategia de conformidad gradual, **ampliando el alcance en los procesos bienales (revisión de la certificación)**

Necesitamos **incrementar el nivel de conformidad de los prestadores de servicio**, a través de los procesos de licitación. ¿Por qué los prestadores consiguen la conformidad de forma más ágil? Necesidad vs Obligación

Que utilicemos un servicio o solución, proporcionado por un proveedor externo, que disponga de la conformidad con el ENS, no implica que nuestro sistema, en su totalidad, sea conforme con el ENS.

La seguridad se trabaja los 365 días de año. En nuestro último “Assessment” los metadatos de los documentos tenían todos la fecha del día anterior. **La seguridad de la organización es un proceso interno, integral y continuo**

La formación y concienciación son elementos clave, que deben ser desarrollados a través de planes anuales, alineados con la estrategia (oferta y demanda).

➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

➤ Síguenos en

