NIS2
Aspectos relevantes para el cumplimiento

Carmen Serrano Durbá

Subdirectora General de Ciberseguridad

GENERALITAT VALENCIANA | ACÍ. ARA.

PLA RECUPEREM VALÈNCIA

Las AAPP en la sociedad

- **Prestadores de servicios ¿esenciales? ¿críticos? ¿importantes?**

  - ✓ No hace falta que alguien nos lo diga o nos designe
  - ✓ Cada vez somos más necesarios para el funcionamiento de la sociedad
  - ✓ Cada vez más dependientes de la tecnología y más vulnerables

- **El ESTADO como garante de los derechos fundamentales y de proporcionar espacio de desarrollo libre del individuo.**

  Obligación o la responsabilidad particular de respetar, promover y garantizar el ejercicio de los derechos humanos, así como de abstenerse de vulnerarlos

NIS2 ¿nos suena algo?

GENERALITAT VALENCIANA

ANNEX I

SECTORS OF HIGH CRITICALITY

10. Public administration		— Public administration entities of central governments as defined by a Member State in accordance with national law
		— Public administration entities at regional level as defined by a Member State in accordance with national law

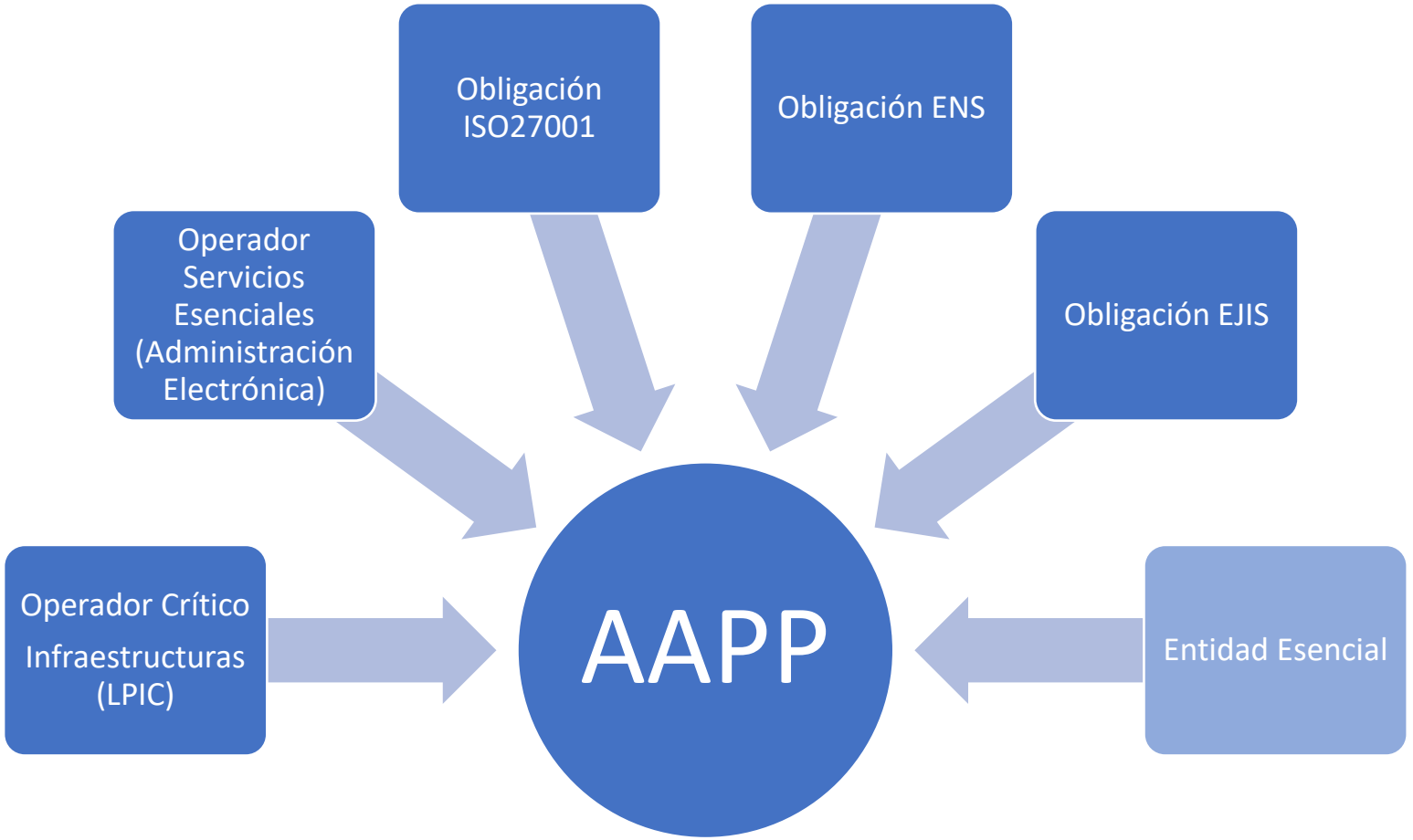
Modelo basado en los riesgos	Medidas técnicas, operativas y organizativas	Gestión de vulnerabilidades	Continuidad de negocio (prestación de servicios)
Gestión de incidentes	Formación y buenas prácticas	Notificación autoridad	Intercambio de información

Las normativas

GENERALITAT VALENCIANA

RGPD	LPDYGDD	ENS (Real Decreto 311/2022)	EJIS
LPIC (Ley 8/2011)	NIS2	CER	LCGC

Las normativas



NIS2: refuerzo

- Refuerza la posición de la Ciberseguridad en la organización
- Refuerzo Ciberseguridad **relaciones con terceros** “Cadena de Suministro”
    - Queda mucho por hacer desde las empresas

- Refuerzo de la **Continuidad de Negocio**
- Implicación de la **dirección como responsable**
    - Art. 43 LCyGC sector público no será objeto de sanción, pero si prevé actuaciones disciplinarias
    - Obligación de formación
    - Oportunidad para conseguir más recursos y presupuesto y de que nos entiendan

NIS2: Gobernanza

GENERALITAT VALENCIANA

NIS2

Artículo 20. Gobernanza.

1. Los Estados miembros garantizarán que **los órganos de dirección** de las entidades esenciales e importantes **aprueben las medidas** de gestión de riesgos de ciberseguridad adoptadas por dichas entidades para cumplir lo dispuesto en el artículo 21, **supervisen** su aplicación y puedan **ser considerados responsables de las infracciones cometidas** por las entidades de dicho artículo.

2. Los Estados miembros velarán por que **los miembros de los órganos de dirección** de las entidades esenciales e importantes estén **obligados a seguir una formación** y animarán a las entidades esenciales e importantes a ofrecer periódicamente una formación similar a sus empleados, a fin de que adquieran conocimientos suficientes y habilidades que les permitan identificar riesgos y evaluar las prácticas de gestión de riesgos de ciberseguridad y su impacto en los servicios prestados por la entidad.

LCGC

Artículo 14. Gobernanza.

1. Los **órganos de dirección** de las entidades esenciales e importantes serán **responsables de aplicar las medidas** para la gestión de riesgos de ciberseguridad incluidas en esta ley, de **supervisar su implantación** efectiva y, en su caso, asumirán la **responsabilidad por su incumplimiento**.
Todo ello sin perjuicio de las normas aplicables en materia de responsabilidad de la administración pública, empleadas y empleados públicos, y los cargos electos o designados.

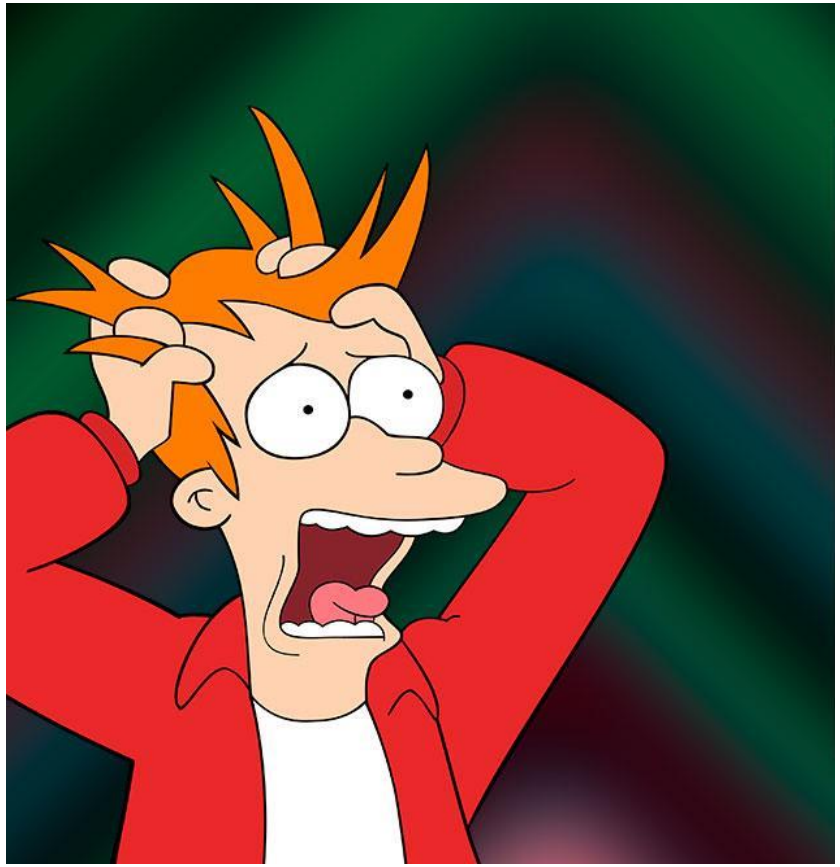
2. Igualmente, **los miembros de los órganos de dirección** de las entidades esenciales e importantes **deberán recibir formación adecuada de forma periódica** al objeto de adquirir conocimientos y destrezas suficientes que les permitan detectar riesgos y evaluar las prácticas de gestión de riesgos de ciberseguridad y su repercusión en los servicios proporcionados por la entidad. Así mismo, los órganos de dirección deberán **organizar periódicamente formaciones similares para sus empleados**.

¿Cómo abordar la NIS2?

- **MAPA: Modelo integrado de cumplimiento**:
  - Diferencial entre normas
  - Identificar afectación de cada Sistema de Información
- **DIRECCIÓN: El ENS .** Hacia la categoría ALTA en sistemas esenciales.
  - Dificultades nuestras y sobre todo de los proveedores
- Necesidad de **identificación servicios esenciales** y sus dependencias:
  - Servicios cuya perturbación podría tener un **impacto significativo en actividades sociales o económicas críticas**
    - No solo la AE
    - Nivel de Disponibilidad ALTO
    - Servicios esenciales **puntualmente**
- El **Perfil de Cumplimiento PCE-NIS2**
- **Certificación** en el ENS

Las notificaciones

- A quien temenos que **notificar** un Incidente:
  - AEPD
  - OCC- CNPIC
  - CCN-CERT
  - INCIBE-CERT
  - Centro Nacional de Ciberseguridad- CERT de Referencia
  - CTEAJE
  - Afectados por los servicios esenciales
  - Afectados datos personales
- Necesidad **ventanilla única y procedimiento unificado**
- **Procedimiento de Gestión de Crisis**:
  - Contención y gestion incidente
  - Coordinación equipos
  - Comités crisis
  - **Comunicación**: dentro, fuera y **notificaciones**



Formación

✓ **Directivos:**

- Los **miembros de los órganos de dirección** de las entidades esenciales e importantes deberán recibir **formación adecuada de forma periódica**.

✓ **Responsable de seguridad** de la información:

- En las entidades esenciales, el responsable de la seguridad de la información, su **persona física representante** en caso de ser un órgano colegiado **y su sustituto**; independientemente de los requisitos de capacidad técnica y formación, deberán ser personal **acreditado por el Ministerio del Interior**. En el caso de tratarse de entidades esenciales que también tengan la consideración de críticas conforme a la ley XXXXXXX, esta obligación será **asimismo extensiva al resto de personal encargado de realizar las labores de ciberseguridad** previstas en esta Ley.

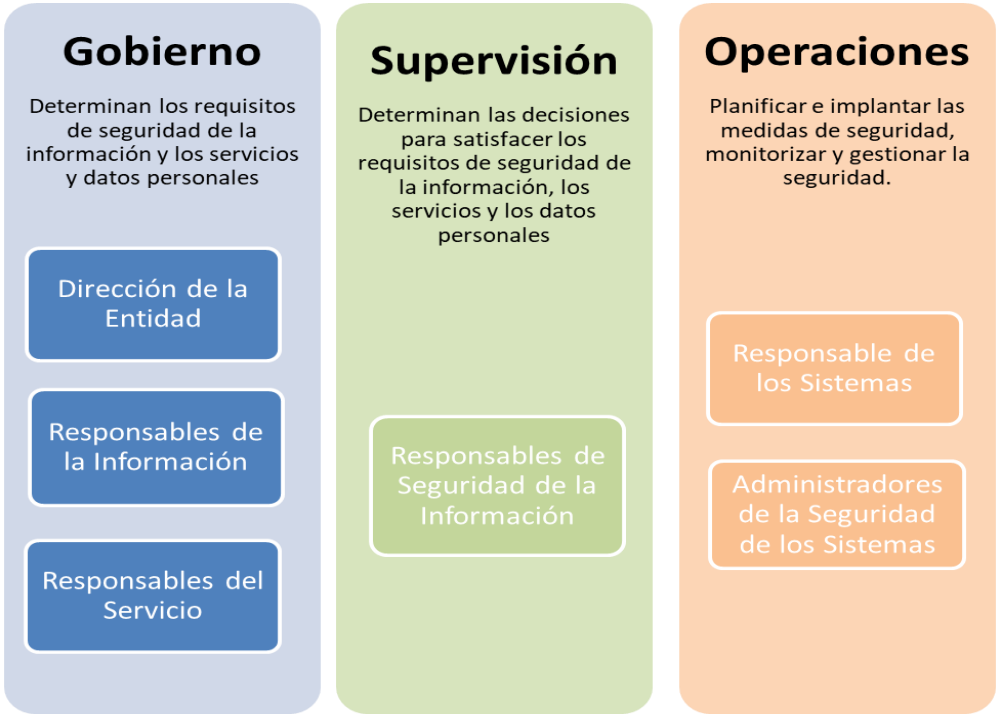
✓ **Personal Administración General.** ENS, NIS2, Ciberseguridad:

- Intervenciones
- Contratación
- Abogacías

La importancia de la Gobernanza

GENERALITAT VALENCIANA

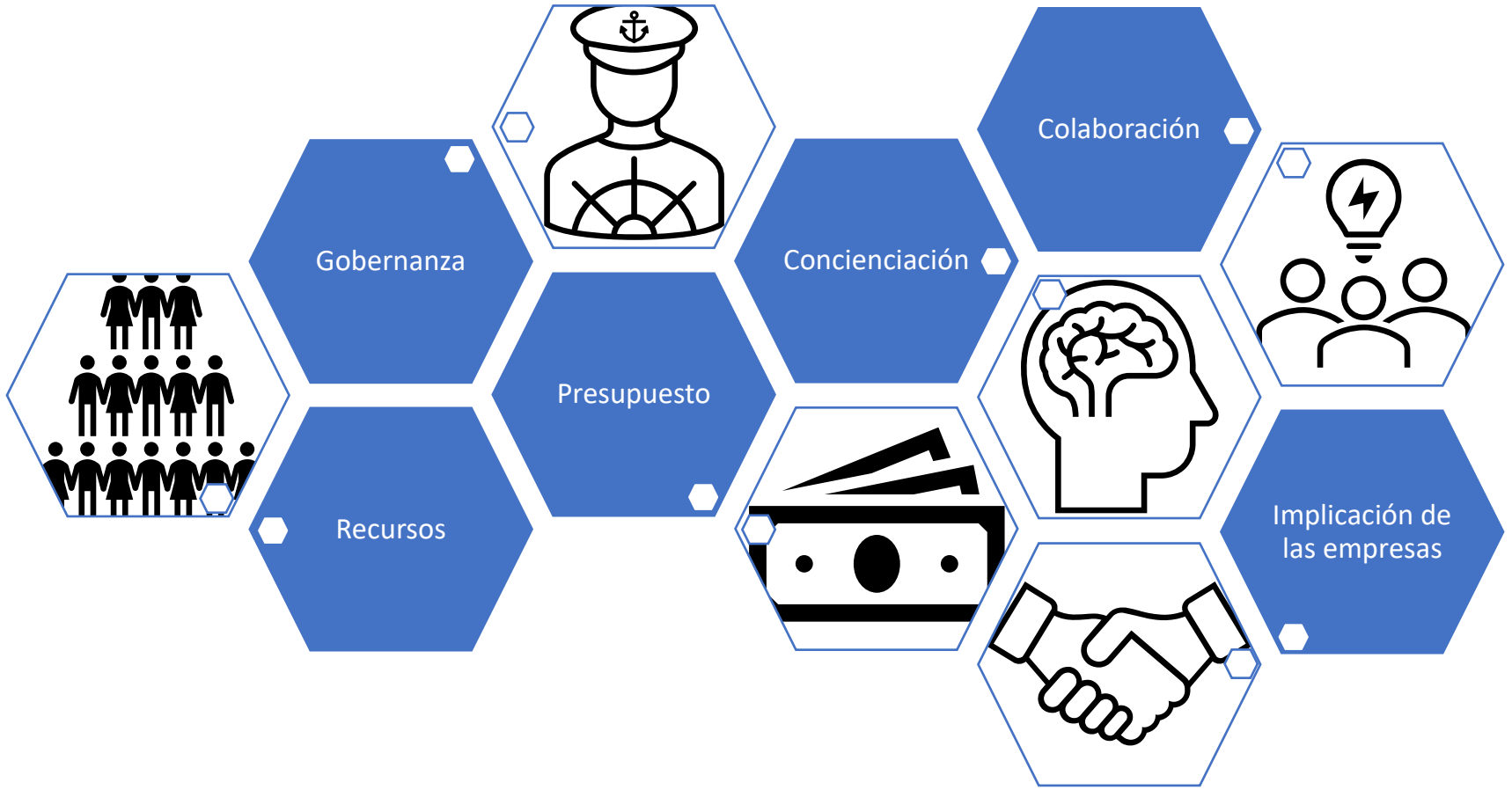
- Verdadera **implicación de la dirección**:
  - Ciberseguridad y cumplimiento en los comités de dirección
  - **Formación** dirección
  - Identificación y categorización necesidades
  - Presupuesto y recursos prioritario
- Que el ENS salga de los departamentos TIC:
  - Responsables de las unidades directivas,
  - Servicios de Contratación,
  - Servicios Jurídicos,
  - Intervenciones
  - **Formación específica** para estos colectivos



Nueva Política de Seguridad: **Nivel de gobierno**. Para cada sistema de información, el Responsable de la Información y el Responsable del Servicio, junto a la Dirección de la entidad, ejercen la responsabilidad legal y la especificación de los requisitos de seguridad.

“Conseguir un elevado nivel común de ciberseguridad en toda la Unión”

GENERALITAT VALENCIANA



GENERALITAT VALENCIANA

¡¡Muchas GRACIAS!!