SOCINFO digital
sociedad de la información

07/10/25

Ciberseguridad, datos e IA,
áreas de alto riesgo/prioritarias para la Sindicatura de Comptes de la CV y la Unidad de Auditoría de Sistemas de Información (UASI)

Antonio Minguillón Roy

Director del Gabinete Técnico

Sindicatura de Comptes de la Comunitat Valenciana

Retos/ Apuesta de la **Transformación Digital** en las AAPP de **la Comunidad Valenciana**

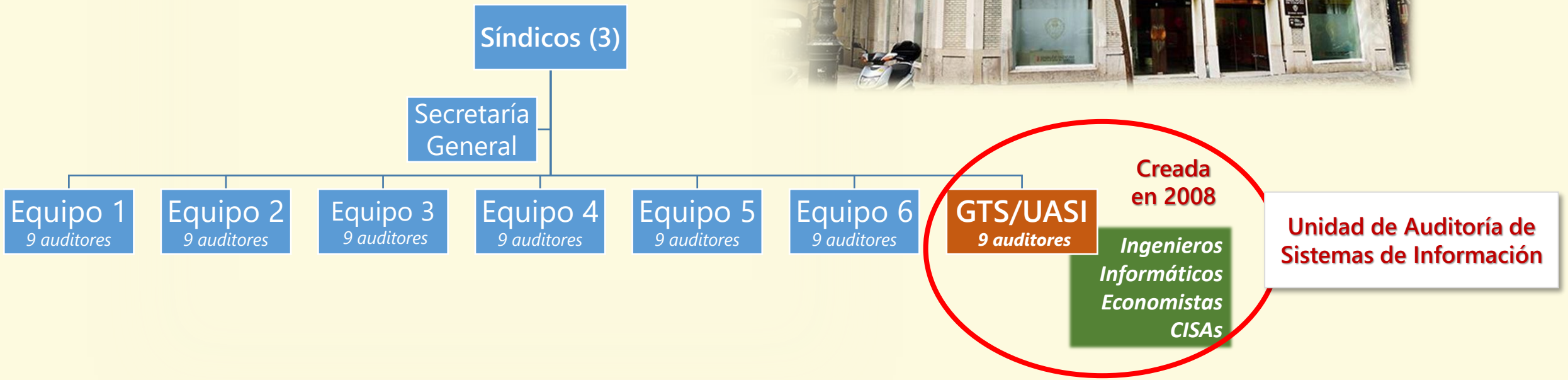
gobierno del dato, ciberseguridad e IA

TREND MICRO™

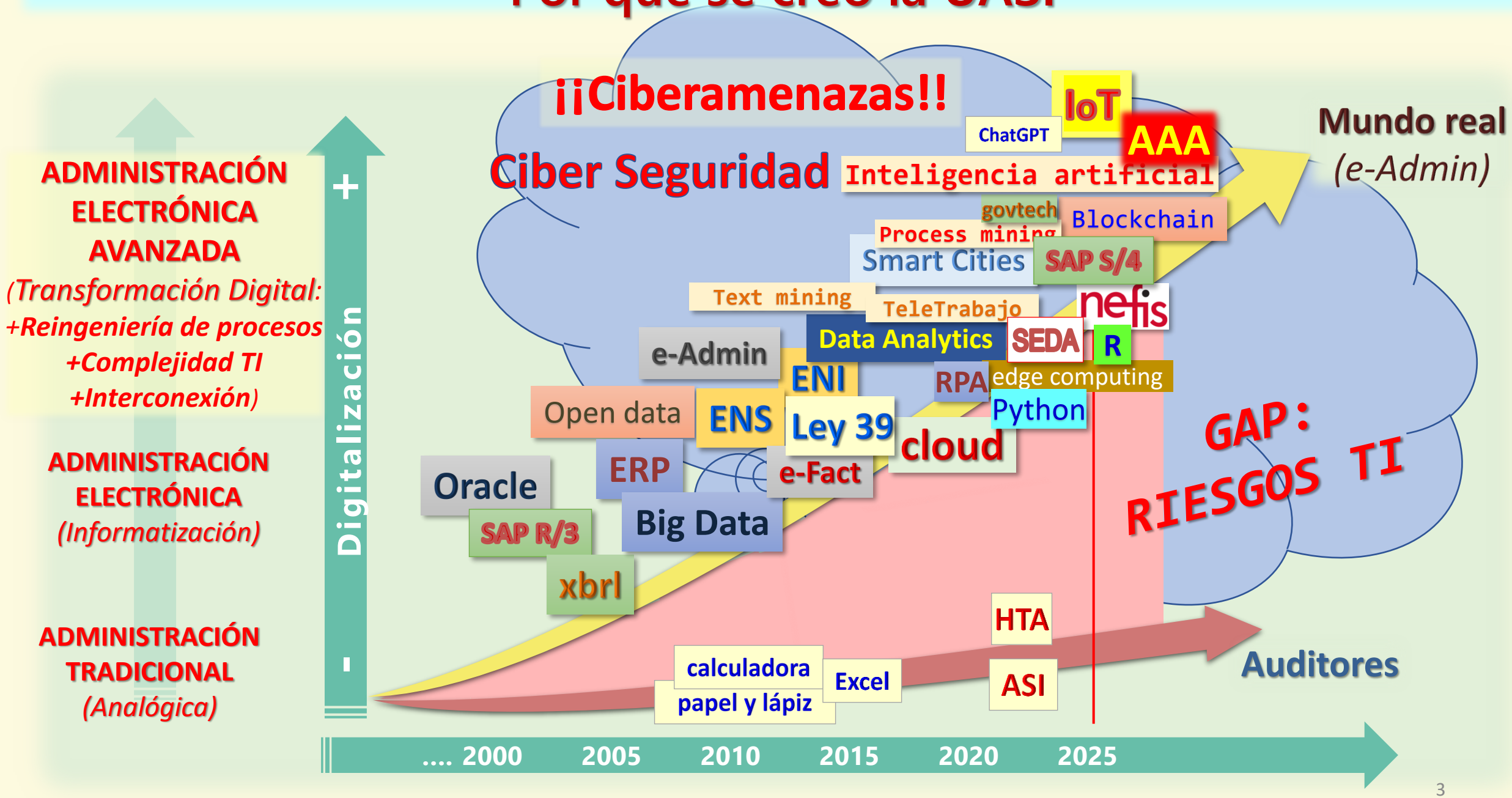
Quiénes somos

Sindicatura de Cuentas de la Comunidad Valenciana

Creada en 1986
actualmente tiene +100 empleados



Por qué se creó la UASI



Qué hacemos

- **Asistencia en las auditorías financieras, de cumplimiento y operativas (50%):**
  - ✓ Revisión de procesos automatizados, evaluación de riesgos TI, identificación y pruebas de CGTI y CPI.
  - ✓ Pruebas masivas de datos.

- **Realizamos nuestras propias auditorías:**
  - ✓ Ciberseguridad *(>50 informes)*.
  - ✓ Auditorías de control interno, CGTI y CPI *(>35 informes)*.
  - ✓ Gestión de grandes proyectos TI *(3 informes)*.

- **Promover el desarrollo de metodología de auditoría en entornos de Administración Electrónica Avanzada:**
  - ✓ Comisión Técnica de Auditoría de la Sindicatura
  - ✓ Comisión Técnica OCEX

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

Prioridad estratégica / Área de alto riesgo

Ciberseguridad

- **Promover el desarrollo de metodología de auditoría en entornos de Administración Electrónica Avanzada:**
  - ✓ Comisión Técnica de Auditoría de la Sindicatura
  - ✓ Comisión Técnica OCEX

Guía práctica de fiscalización de los OCEX

GPF-OCEX 5331 Gobernanza corporativa, gobernanza de las TI y su auditoría

Guía práctica de fiscalización de los OCEX

GPF-OCEX 5332 Revisión de los CGTI del área B. Gestión de cambios en aplicaciones y sistemas

Guía práctica de fiscalización de los OCEX

GPF-OCEX 5333 Revisión de los CGTI del área C. Operaciones de los sistemas de información

Guía práctica de fiscalización de los OCEX

GPF-OCEX 5334 Revisión de los CGTI del área D. Controles de acceso a datos y programas

Referencia: GPF-OCEX 5330 y Esquema Nacional de Seguridad

Guía práctica de fiscalización de los OCEX

GPF-OCEX 5335 Revisión de los CGTI del área E. Continuidad del servicio

Referencia: GPF-OCEX 5330 y Esquema Nacional de Seguridad

…a de Presidentes de ASOCEX el 26/06/2024

Guía práctica de fiscalización de los OCEX

GPF-OCEX 5311 Ciberseguridad, seguridad de la información y auditoría externa

Referencia: GPF-OCEX 1315, 1500 y 5300

Guía práctica de fiscalización de los OCEX

GPF-OCEX 5313 Revisión de los controles básicos de ciberseguridad

Referencia: GPF-OCEX 5311, Esquema Nacional de Seguridad, CIS Controls.

Documento elaborado por la Comisión Técnica de los OCEX y aprobado por la Conferencia de Presidentes de ASOCEX el 12/11/2018

Guía práctica de fiscalización de los OCEX

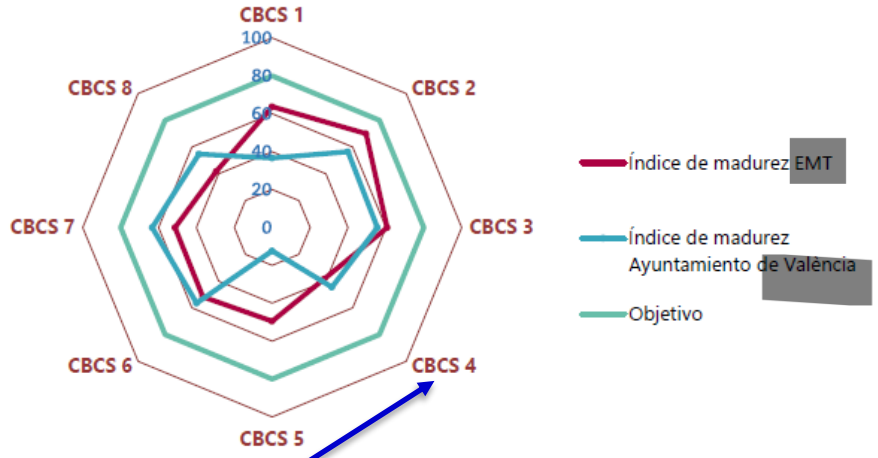
GPF-OCEX 5314 Gobernanza de la ciberseguridad y su auditoría

Referencia: GPF-OCEX 1315 (Revisada), GPF-OCEX 5330, GPF-OCEX 5331 y GPF-OCEX 5313

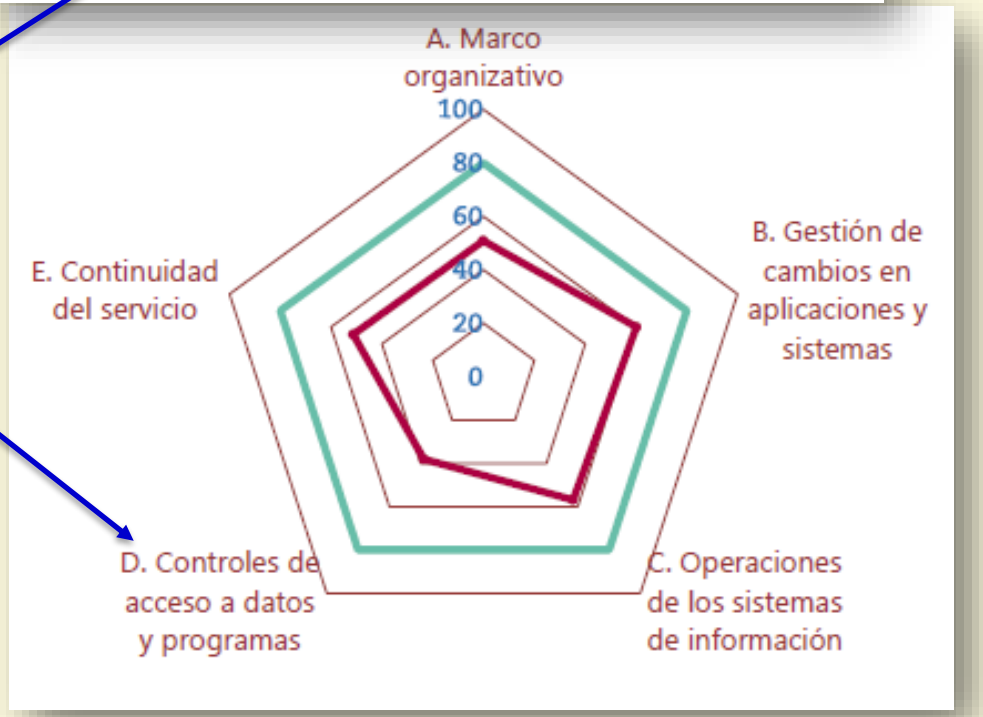
Documento elaborado por la Comisión Técnica de los OCEX y aprobado por la Conferencia de Presidentes de ASOCEX el 19/10/2023.

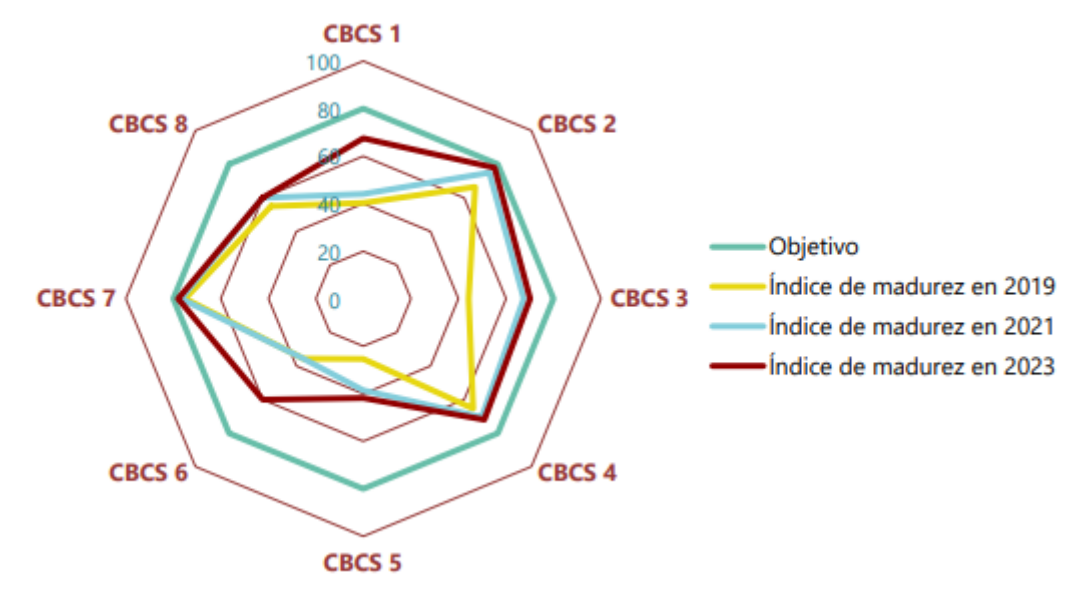
Áreas	Controles principales	Índice de madurez	
A. Marco organizativo	A.1 Cumplimiento de legalidad (CBCS 8)	41,7%	**50,9% (N2)**
	A.3 Formación y concienciación	60,0%	
B. Gestión de cambios en aplicaciones y sistemas	B.3 Gestión de cambios	60,2%	**60,2% (N2)**
C. Operaciones de los sistemas de información	C.1 Inventario de *hardware* (CBCS 1)	63,8%	**56,9% (N2)**
	C.1 Inventario de *software* (CBCS 2)	70,0%	
	C.2 Gestión de vulnerabilidades (CBCS 3)	60,7%	
	C.3 Configuraciones seguras (CBCS 5)	49,5%	
	C.4 Registro de la actividad de los usuarios (CBCS 6)	51,8%	
	C.5 Servicios externos	49,8%	
	C.8 Gestión de incidentes	53,1%	
D. Controles de acceso a datos y programas	D.1 Uso controlado de privilegios administrativos (CBCS 4)	38,6%	**38,1% (N1)**
	D.2 Mecanismos de identificación y autenticación	40,3%	
	D.3 Gestión de derechos de acceso	36,4%	
	D.4 Gestión de usuarios	37,3%	
E. Continuidad del servicio	E.1 Copias de seguridad de datos y sistemas (CBCS 7)	51,3%	**51,3% (N2)**
General			**51,5% (N2)**

Gráfico 3. Comparativa del Índice de madurez de los controles básicos de ciberseguridad de la EMT y del Ayuntamiento de València



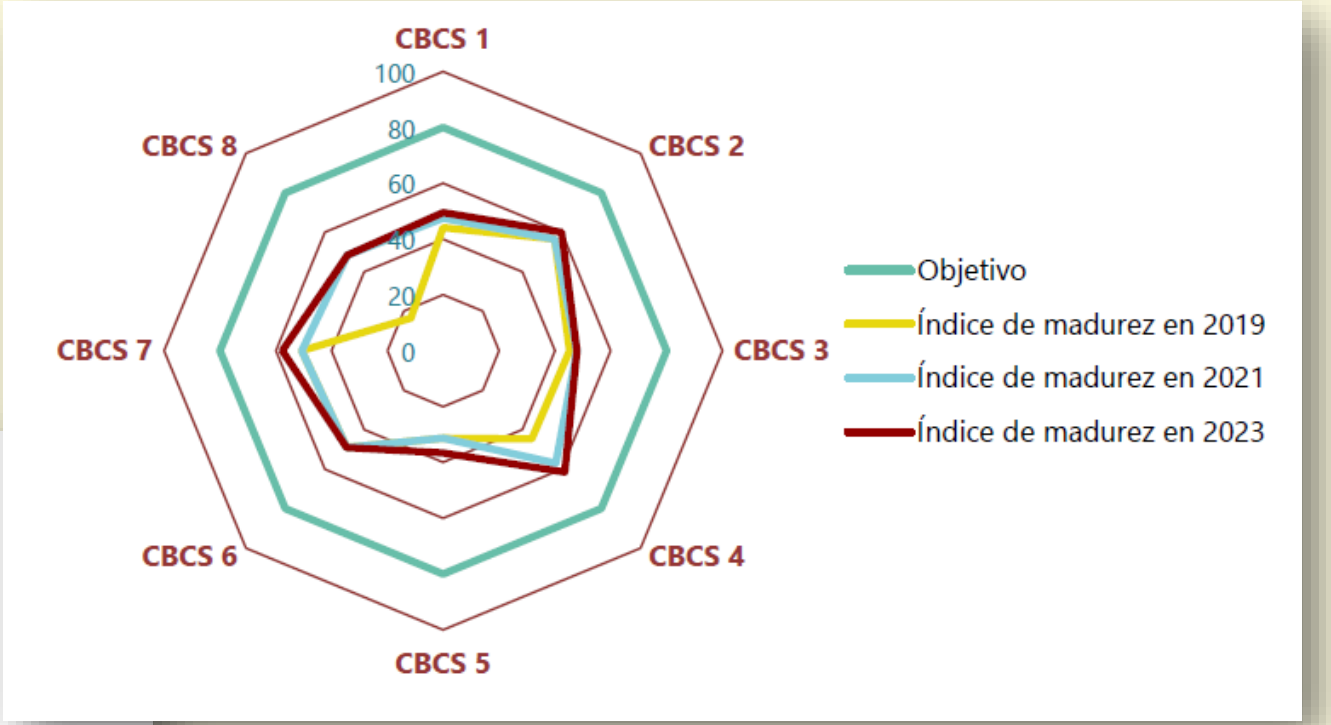
El índice medio de madurez de los CBCS ha sido del 53,4% en la EMT y del 47,5% en el Ayuntamiento de València; en ambos casos la situación de los controles de ciberseguridad es claramente mejorable y no puede considerarse que los sistemas de información estén debidamente protegidos.

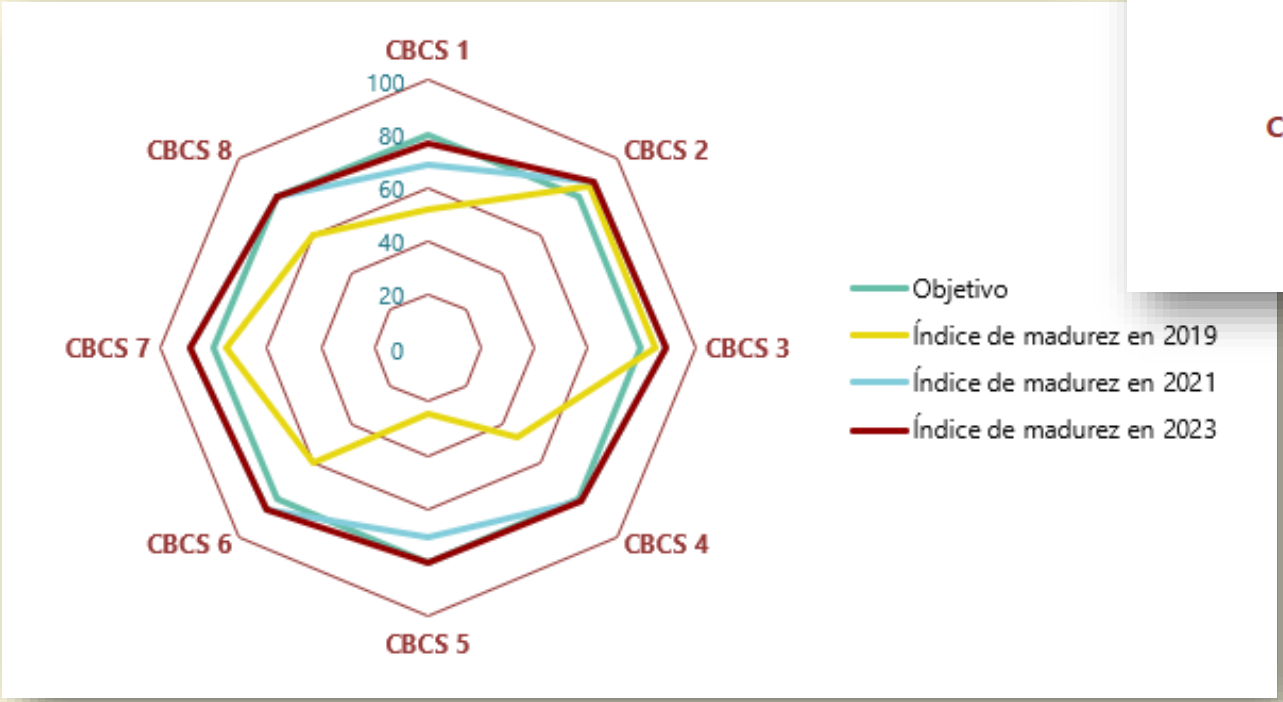




… evolución en el tiempo ….

… y comparación entre entidades ….





Controles Básicos de Ciberseguridad (CBCS)

Análisis de resultados de las auditorías de otros OCEX

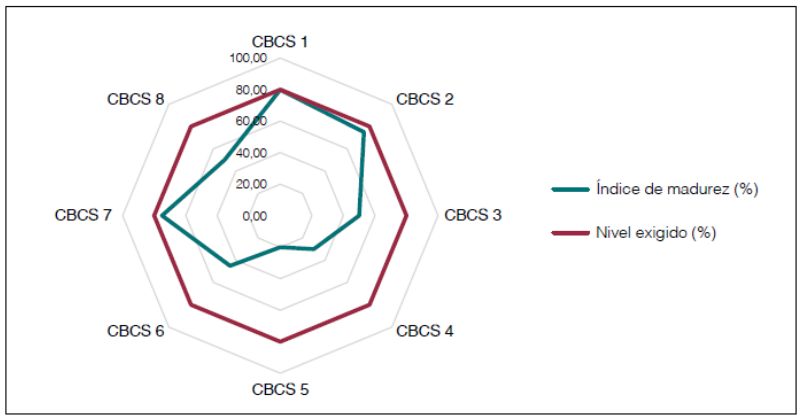
CONSEJO DE CUENTAS
DE CASTILLA Y LEÓN

Ayuntamiento	Índice de madurez
Salamanca	63,2%
Burgos	54,3%
Valladolid	53,6%
Palencia	51,8%
León	37,6%
Ávila	34,5%
A	*39,4%*
B	*19,9%*
C	*17,8%*
D	*16,3%*
E	*11,4%*
F	*4,9%*
G	*3,0%*

Ayuntamiento	Índice de madurez
Badalona	51,4%
Mataró	53,1%
Santa Coloma	57,2%

SINDICATURA DE COMPTES DE CATALUNYA

Gráfico 2. Índice de madurez y objetivos de los CBCS

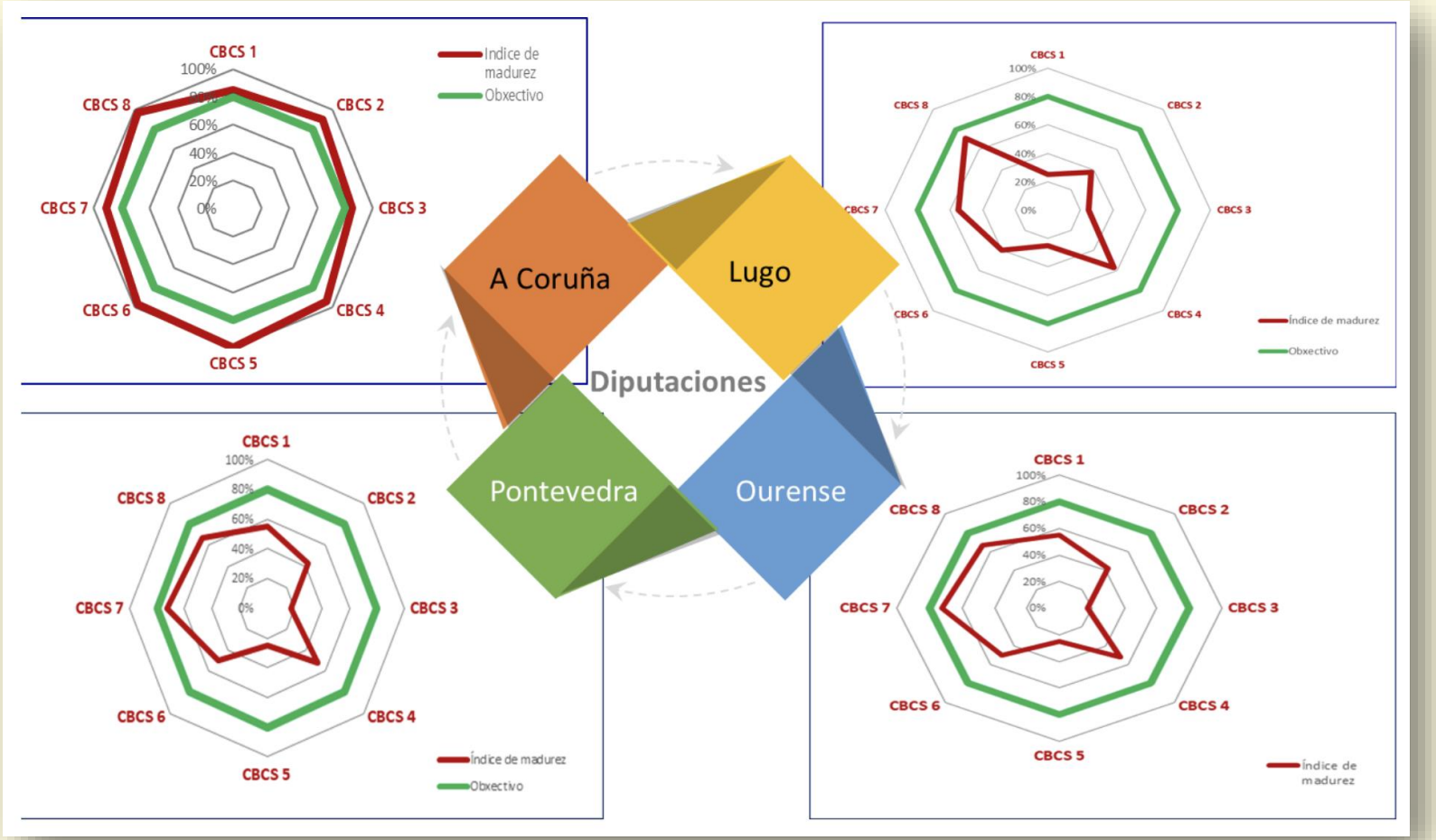


Análisis de resultados de las auditorías de otros OCEX

Consello de Contas de Galicia

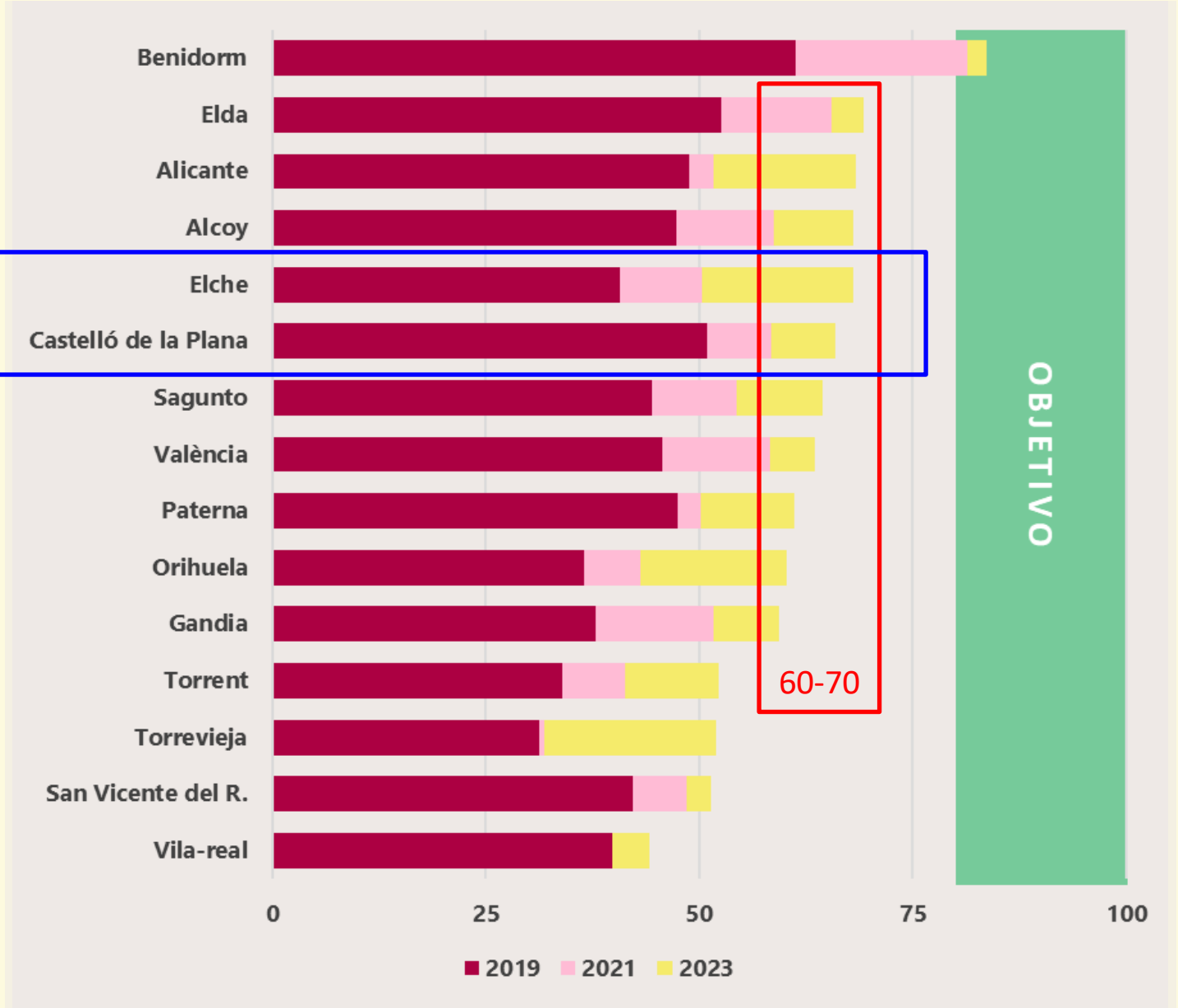
Diputación	Índice de madurez
La Coruña	92%
Pontevedra	53%
Orense	48%
Lugo	42%

Ayuntamiento	Índice de madurez
La Coruña	56%
Orense	50%
Vigo	57%



Qué decimos en los informes de auditoría de los CBCS

Índice de Madurez de los CBCS de los 15 mayores ayuntamientos de la CV



4. CONCLUSIONES

Bajo índice de madurez de los controles de ciberseguridad

Se requiere mayor concienciación y más recursos dedicados a la seguridad de la información

Insuficiente gobernanza de la seguridad de la información

La EMT dispone de una *Política de seguridad de la información* (PSI), que **no ha sido aprobada** como requ
requisitos

La situación de los controles de acceso privilegiado debe ser mejorada

Existen graves deficiencias en los controles relacionados con los usuarios administradores de los sistemas, departamentos
"sistemas descer

Insuficiente grado de adecuación a la normativa de ciberseguridad

La revisión del cumplimiento de legalidad en materia relacionada con la ciberseguridad ha puesto de manifiesto un nivel insatisfactorio de adecuación a la normativa de

Priorización de las recomendaciones

Con objeto de que puedan establecerse acciones basadas en criterios de coste/beneficio, el siguiente gráfico 2 se muestra la clasificación de las recomendaciones según los terios combinados de riesgo potencial a mitigar y coste de su implantación.

áfico 2. Riesgos que se atienden y coste de implantación de las recomendaciones

!!!!!!!!!

CUARTA CONCLUSIÓN

Las entidades auditadas, en general, no tienen establecida una adecuada gobernanza de la ciberseguridad, tal como exigen tanto la normativa como un sistema de control interno bien establecido.

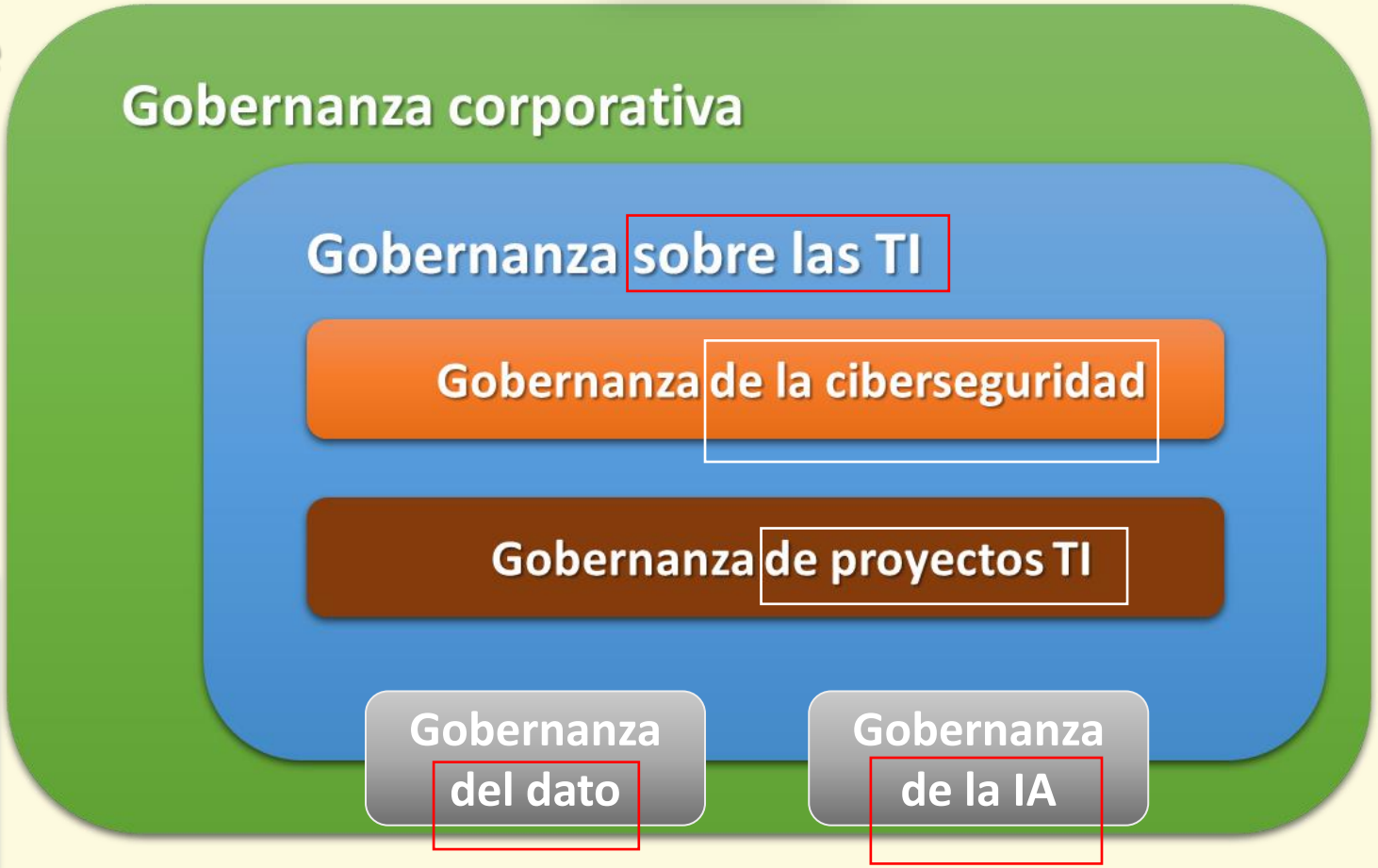
Los órganos superiores de las entidades (alcalde o alcaldesa en el caso de los ayuntamientos; presidente o presidenta en el caso de las diputaciones) son los **responsables** de que existan unos controles adecuados sobre los sistemas de información y las comunicaciones, y su implicación, compromiso y liderazgo constituyen, posiblemente, el factor más importante para la implantación exitosa de un sistema de gestión de la seguridad de la información que garantice la ciberresiliencia de la entidad. Se debe actuar de manera urgente para solventar las carencias identificadas en esta materia en cada una de las entidades, ya que afectan de manera negativa al estado de su ciberseguridad.

No hay alineación entre los objetivos y prioridades de la alta dirección/órganos de gobierno y el departamento TI/seguridad

Gobernanza de la Ciberseguridad

Es el proceso de establecer y mantener un marco de referencia, y apoyar la estructura y los procesos de gestión para garantizar la confidencialidad, autenticidad, disponibilidad, integridad y trazabilidad de los datos.

La Gobernanza, primer componente de un sistema de control interno (COSO)

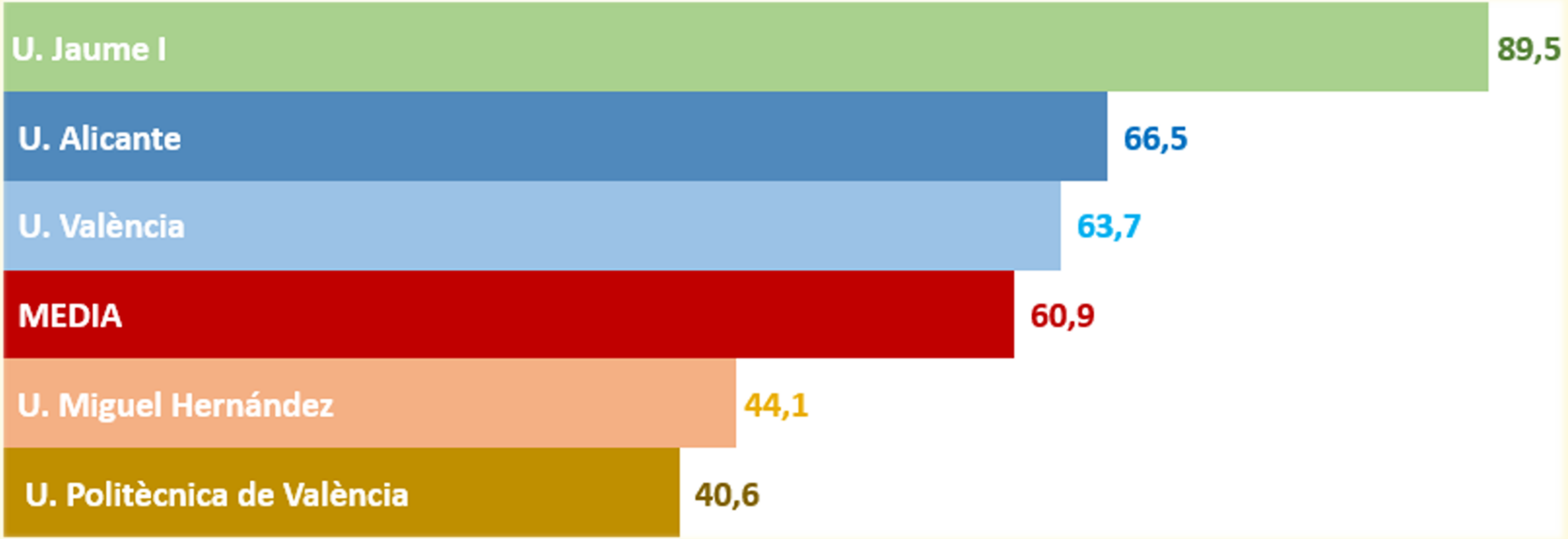


Las normas internacionales de auditoría (NIA) requieren que el auditor conozca este primer componente del sistema de control interno

La Gobernanza de las TI es un componente esencial de la Gobernanza corporativa

La Gobernanza de la ciberseguridad es un componente esencial de la Gobernanza TI

Indicador global de la Gobernanza TI+Ciber en las Universidades de la Comunidad Valenciana



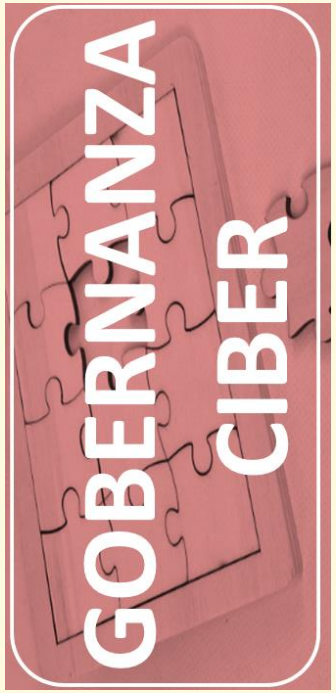
OJO!!!!! Auditar la gobernanza de ciberseguridad NO ES LO MISMO que auditar medidas/controles concretos para evaluar el nivel o estado de la ciberseguridad de la entidad.

Actualmente tenemos en marcha una auditoría sobre la gobernanza de la ciberseguridad de las 60 entidades que forman el SPI de la GV.

Debilidades más significativas observadas

- Inexistencia de comités de gobierno de las TI, que operen de manera eficaz y que cuenten con la involucración de los órganos de gobierno.
- Carencia de planes estratégicos de TI y de ciberseguridad, que estén aprobados por los órganos de gobierno, de forma que cuenten con su compromiso en la consecución de los objetivos planteados y aseguren la disponibilidad de los recursos necesarios.
- Procesos de gestión de riesgos de TI no formalizados o inexistentes.
- Marco normativo TI (políticas, normas y procedimientos TI), en general, limitado y poco estructurado.
- Indicadores para la gestión TI inexistente.

Aspectos más significativos



- La ciberseguridad no es un área o sección del departamento de informática. La ciberseguridad debe estar en la agenda de los órganos de gobierno.
- El COMSEGTIC debe tener un funcionamiento efectivo.
- Organización de la ciberseguridad. Incompatibilidades.
- ENS, herramienta indispensable.
- Política de seguridad, es una declaración de intenciones. No se puede quedar en papel mojado.
- Formación y concienciación, elementos clave de la estrategia de ciberseguridad. A TODOS los colectivos y a TODOS los niveles.
- Recursos. Tecnología + personas.

Conclusiones y

95 Concluimos que la comuni
(IOUE) no ha alcanzado un nive
trabajo demuestra que las IOUE
y, dado que suelen estar interc
privadas en los Estados miembr
pueden exponer a otras a ciber

III Constatamos que no siempre se aplicaban buenas prácticas esenciales de ciberseguridad, como algunos controles esenciales, y que los gastos en ciberseguridad en varias IOUE son insuficientes. En algunas IOUE tampoco existe una buena gobernanza de la ciberseguridad: en muchos casos, no existen estrategias de seguridad informática, o estas no están respaldadas por la alta dirección, las políticas de seguridad no siempre se formalizan y las evaluaciones de riesgos no abarcan todo el entorno informático. No todas las IOUE disponen de medidas re
ciberseguridad sujetas a una garantía independiente.

96 Constatamos que no siempre se aplicaban buenas prácticas, como algunos controles esenciales. Una buena gobernanza de ciberseguridad es esencial para la seguridad de los sistemas de información e informáticos, pero esta aún no aplica en algunas IOUE: en muchos casos, no existen estrategias y planes de seguridad informática o estos no están respaldados por la alta dirección, las políticas de seguridad no siempre se formalizan y las evaluaciones de riesgos no abarcan todo el entorno informático. El gasto en ciberseguridad es desigual, ya que algunas IOUE no gastan lo suficiente en comparación con homólogas de tamaño similar (véanse los apartados *21* a *33*, y *37* y *38*).

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

Prioridad estratégica / Área de alto riesgo

Datos, datos, datos … e IA

FIRMADO POR
El Secretari General de la Sindicatura de Comptes de la Comunitat Valenciana Lorenzo Pérez Sarrión 04/06/2025 19:17

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

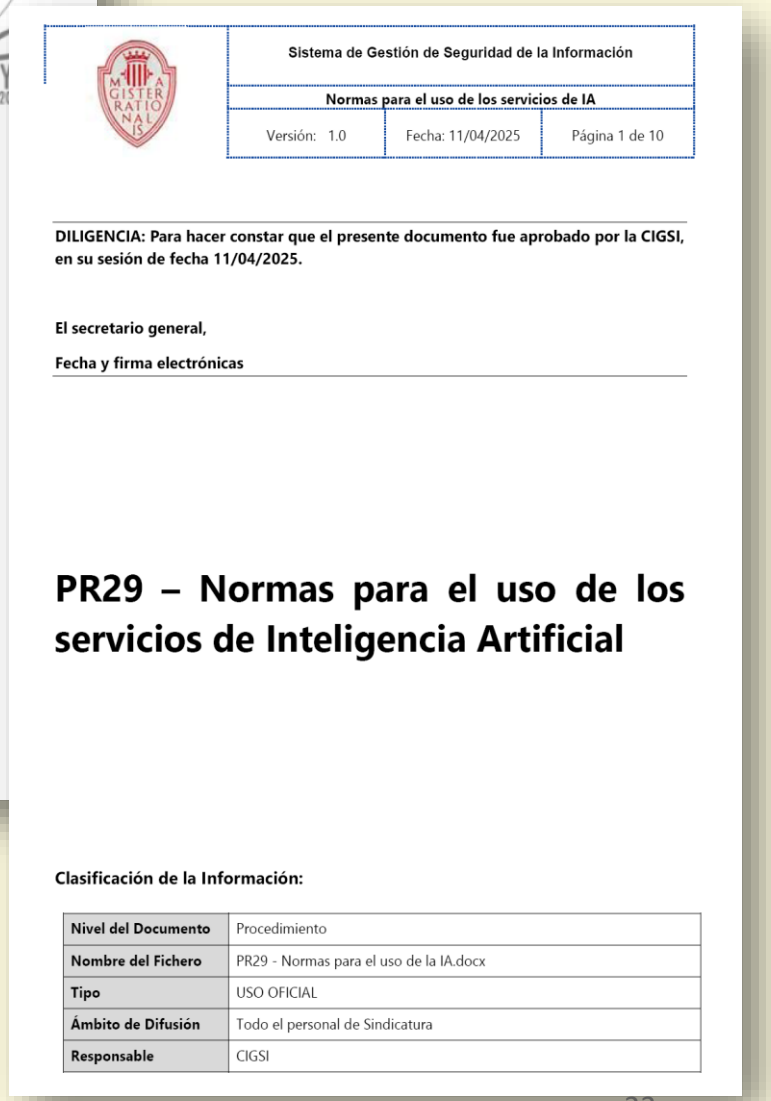
CIGSI
Expedient 2010121N

ACTUALIZACIÓN ESTRATÉGICA: GOBIERNO DEL DATO, DATOS ABIERTOS E INTELIGENCIA ARTIFICIAL (PEGODA)

1. ANTECEDENTES Y SITUACIÓN ACTUAL

La Sindicatura de Comptes de la Comunitat Valenciana (en adelante la Sindicatura) es una institución estatutaria independiente a la que le corresponde realizar el control externo de la gestión económico-financiera del sector público valenciano, función que desarrolla con la máxima iniciativa y responsabilidad, y goza de total independencia funcional tanto del Consell de la Generalitat como de las Corts Valencianes. Esto significa que la Sindicatura decide, dentro de su ámbito de actuación, qué entidades va a auditar, qué tipos de auditorías realizará y cómo las ejecutará.

Crear la oficina del dato (datos públicos)
Potenciar el uso de la IA



Sistema de Gestión de Seguridad de la Información

Normas para el uso de los servicios de IA

Versión: 1.0	Fecha: 11/04/2025	Página 1 de 10

DILIGENCIA: Para hacer constar que el presente documento fue aprobado por la CIGSI, en su sesión de fecha 11/04/2025.

El secretario general,

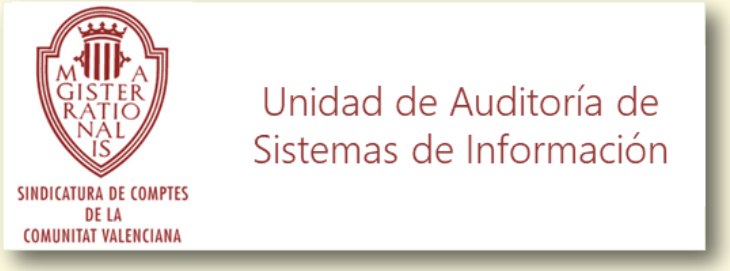
Fecha y firma electrónicas

PR29 – Normas para el uso de los servicios de Inteligencia Artificial

Clasificación de la Información:

Nivel del Documento	Procedimiento
Nombre del Fichero	PR29 - Normas para el uso de la IA.docx
Tipo	USO OFICIAL
Ámbito de Difusión	Todo el personal de Sindicatura
Responsable	CIGSI

Gracias por su atención



Antonio Minguillón Roy
aminguillon@sindicom.es