HACIA EL USO INTELIGENTE DE LA INTELIGENCIA ARTIFICIAL EN LA AUDITOR-*IA:*
sin Gobierno del Dato, no hay paraíso. Algunas reflexiones para no perecer en el intento.

Lorenzo Pérez Sarrión
Secretario General de la Sindicatura de Comptes de la Comunitat Valenciana.

Revista Auditoría Pública nº 85
Junio 2025. Páginas: 39-49

Resumen: El presente artículo trata de llamar la atención sobre la necesidad de afrontar los riesgos y oportunidades asociados a la utilización de las herramientas de inteligencia artificial (IA) para su incorporación, ordenada y rigurosa, al ejercicio de la función pública auditora por los órganos de control externo (OCEX).

La elaboración de un plan estratégico del gobierno del dato (PEGODA) y la aprobación de unas normas internas -soft law- sobre el uso de la IA en el seno de cada institución, pueden ser el cauce formal adecuado para garantizar una verdadera orientación al dato -a los grandes conjuntos y espacios de datos- de la tarea fiscalizadora del sector público.

En ese proceso, deviene necesario adaptar la estructura organizativa y de recursos de los OCEX mediante una adecuada formación e información de su personal sobre el nuevo contexto que la IA aporta, en un inexcusable entorno de compliance en materia de ciberseguridad, protección de datos y respeto de la propiedad intelectual de terceros.

También resulta inaplazable la incorporación de nuevos perfiles profesionales que den el soporte tecnológico y analítico adecuados a la inevitable evolución de la tradicional auditoría pública.

Los cambios que este nuevo escenario exige aconsejan la revisión y actualización sin demora de los respectivos planes estratégicos de cada OCEX y trazar la oportuna hoja de ruta.

Palabras Clave: Gobierno del Dato. Inteligencia Artificial (IA). Interoperabilidad. Plan estratégico. Sindicatura de Comptes de la Comunitat Valenciana. Órganos de control externo (OCEX). Auditoría pública.

Abstract: This paper attempts to draw attention to the need to deal with the risks and opportunities associated with the use of Artificial Intelligence (AI) tools for their orderly and rigorous incorporation into the exercise of the public audit function by regional public sector audit institutions in Spain (OCEX in its Spanish acronym).

The development of a strategic plan for data governance (PEGODA) and the adoption of internal rules -soft law- on the use of AI within each institution may be the appropriate formal channel to ensure a true data-driven approach to large data sets and data spaces of the public sector audit task.

In this process, it is necessary to adapt the organisational and resource structure of the OCEX through adequate training and information for their staff on the new context that AI provides, in an essential background of compliance in terms of cybersecurity, data protection and respect for the intellectual property of third parties.

The incorporation of new professional profiles that provide the appropriate technological and analytical support for the unavoidable development of traditional public auditing is also urgent.

The changes this new scenario calls for recommend to review and update the respective strategic plans of each OCEX without delay and to draw up the appropriate roadmap.

Keywords: Data governance. Artificial Intelligence (AI). Interoperability. Strategic plan. Audit Office of the Valencian Community. Regional Public Sector Audit Institutions (OCEX in its Spanish acronym). Public auditing.

1. Introducción.

Encontrar los datos. Cuanto más fiables y exactos, mejor. Los datos proporcionan evidencias, imprescindibles para la fiscalización. Los, cada vez mayores, conjuntos de datos disponibles abren nuevos campos para la rendición de cuentas y la auditoría pública. Datos abiertos. Datos confidenciales. Datos protegidos. Datos propios y ajenos, de procedencia diversa. Interoperables. Reutilizables. Necesitamos que los datos sean íntegros, fiables, accesibles, oportunos. Ya no se puede –ni se debe– vivir sin los datos. Hay que trabajar con ellos, sin perdernos en el proceso. Hay que recopilarlos, midiendo y evidenciando su nivel de calidad, relacionarlos y estructurarlos, para un análisis integrado que garantice un ejercicio responsable de la función pública auditora, con respeto a los de carácter protegido, a la confidencialidad y a los derechos de propiedad intelectual.

Por otra parte, la inteligencia artificial (IA) es útil, novedosa y está de moda. No es algo opcional, como tampoco lo fue en su día la conexión a internet, conviene recordarlo. Ha venido para quedarse. Como coloquialmente suele decirse: *no se le pueden poner puertas al campo*. La IA –por cierto, no siempre tan inteligente– es sugerente, subliminal, inmersiva y expansiva. No debe ser un enemigo, sino una aliada del conocimiento humano, también en los trabajos de auditoría. Para ello, el primer paso ha de ser el tomar plena consciencia de ello, y el segundo, adaptar nuestras organizaciones estatutarias a esta nueva realidad. Si no lo hacemos, literalmente nos pasará por encima. Por cierto, nuestro trabajo consiste en auditar un sector público que, no siempre en las condiciones óptimas, está inmerso en esa carrera digital que la IA ha desatado, por lo que habrá que estar preparados para auditar, cómo no, también la IA en los entes fiscalizados. Igualmente, habrá que auditar los algoritmos que la rigen en cada caso, desvelar su opacidad, analizar los riesgos de sus sesgos subyacentes, y hacerlo al margen de cualquier ideología o creencia, con el Derecho Positivo en la mano. ¿Estamos los OCEX preparados para ello?

En este contexto, el presente artículo tan sólo pretende concienciar, una vez más[1], de la inaplazable necesidad de abordar, en el seno de cada OCEX, de acuerdo con sus particulares necesidades, posibilidades y objetivos, una ordenación racional y estructurada de todos los datos con que cuenta, o debe contar, para realizar una auditoría pública moderna, acorde al estado y avance creciente de las innovaciones tecnológicas de este vertiginoso siglo XXI.

Sin Gobierno del Dato, no hay paraíso, podríamos decir, sin riesgo de equivocarnos. Por el contrario, usar en la auditoría las herramientas que proporciona la IA, sin un mínimo marco y procedimiento definidos –Plan Estratégico del Gobierno del Dato (PEGODA) y Normas de uso de la IA– es sinónimo de riesgos en el ejercicio de la auditoría, y comporta un incremento exponencial de vulnerabilidades, no solo en materia de ciberseguridad, sino de protección de datos o de la propiedad intelectual de terceros, pudiendo comprometer, a la postre, las imprescindibles fiabilidad, certidumbre y credibilidad, que deben caracterizar una rigurosa función pública fiscalizadora.

No decidir nada al respecto o mirar hacia otro lado, nunca será una buena decisión.

Tampoco hay un único modelo. Cada organización, en función de su estado de madurez, definido por las competencias y aptitudes, pero también por las actitudes del personal que la conforma, debe alinear sus objetivos con esta nueva realidad de la IA y el relevante papel que corresponde en su seno al uso operativo y consciente de los espacios de datos para la función auditora.

Me referiré pues, a continuación, a las cuestiones que han ido surgiendo alrededor de estas dos realidades en este camino iniciado por la Sindicatura –problemas, dudas e incertidumbres incluidas–, por si el debate puede ser de utilidad a quienes hayan de plantearse su propio PEGODA, su propio código de uso de la IA, desde los cuales afrontar los retos que plantea el nuevo marco tecnológico en la función de control externo de los OCEX.

2. El contexto de cada organización y su propio autodiagnóstico.

Para acometer cualquier plan o proyecto es necesario –además de conocer su marco de referencia específico, legal, o de casos de éxito en su entorno– tener un diagnóstico de nuestra propia organización, para delimitar su alcance, pasos y recursos a utilizar para conseguir los objetivos del plan.

1 El presente artículo puede leerse como una suerte de segunda parte del que ya dediqué a las cuestiones que ahora se exponen: accesible en esta misma revista Auditoría Pública nº 84, *Arquímedes y el iceberg de un OCEX*: https://asocex.es/arquimedes-y-el-iceberg-de-un-ocex/.
También, en el mismo ámbito, con anterioridad, en esta misma revista, Auditoría Pública, nº 80, *Transformación digital y estrategia del dato: El escenario previo necesario para implantar la inteligencia artificial en la auditoría pública:* https://asocex.es/transformacion-digital-y-estrategia-del-dato-el-escenario-previo-necesario-para-implantar-la-inteligencia-artificial-en-la-auditoria-publica/

Citemos algunos aspectos que debemos conocer de nuestra organización antes de embarcarnos en este viaje:

- Cómo estamos en cuanto a sistemas de seguridad, implantados, en curso de implantación y/o programados. ENS[2] (y NIS 2[3]). Ni que decir tiene que los recursos destinados a este campo han experimentado un fuerte incremento. Iniciar el camino de la auditoría y acreditación en el ENS de diversos sistemas en el seno de cada OCEX puede ser una buena práctica de cara a no quedar a la zaga en cuestiones de ciberseguridad en nuestras organizaciones, que requieren una actividad proactiva de seguridad por defecto. En eso andamos en la Sindicatura, inicialmente con un Plan director de sistemas y tecnologías de la información, y después con un Plan de adecuación al ENS, que luego ha incorporado las previsiones, aun no vinculantes, pero recomendables, de las NIS 2: hay que ir adelantando faena.

- Cuál es el grado de madurez del personal en la utilización de aplicaciones, también en herramientas de IA[4]. Detectar carencias, iniciativas de innovación, pero también, y, sobre todo, hacer prevalecer la sensatez y las prácticas seguras, nos marcará las necesidades de información, formación y concienciación necesarias en ese camino.

- La situación de la realidad en materia de interoperabilidad. Se avanza muy lentamente en algo que debe generar un acceso más amplio, racional y seguro a los datos de la actividad de los cuentadantes, facilitando a estos la labor de rendición y normalizando los estándares de control y seguimiento de las fiscalizaciones. ¿Estamos preparados para ello? Es más, ¿somos plenamente interoperables con nosotros mismos? ¿Tenemos plenamente integradas todas nuestras aplicaciones y herramientas? ¿Tenemos un sistema o sistemas que las gobiernen?

Son estos solo algunos aspectos a tener en cuenta y reflexionar en qué estadio nos encontramos. Si bien no es aconsejable pecar de optimista, aunque no estemos plenamente preparados para acometer los cambios necesarios, tampoco podemos permanecer inactivos: los grandes espacios de datos (en apenas una década), y la IA (en los últimos tres años), lo han cambiado todo. La auditoría ya no es –sólo– lo que era, y probablemente nunca vuelva a serlo.

3. La evaluación de riesgos como enfoque sistémico.

Todos los cambios exigen respuestas. No hacer, ni decidir nada, también es una manera –ineficiente, eso sí– de afrontar los problemas. Valorar los riesgos que cada actitud –activa o pasiva– conlleva, puede ayudar a tomar la decisión adecuada, o, cuando menos, evitar males mayores.

El acceso a los datos, su gestión, tratamiento y explotación representan riesgos ciertos y concretos, principalmente legales, pero sobre todo de seguridad, que hay que contemplar, antes de decidir como innecesario el disponer de un gobierno de datos en el seno de un OCEX. Las bases de datos, masivas y complejas, son hoy la fuente primordial y casi única de las evidencias de auditoría. No parece cuestionable la necesidad de contar con un inventario preliminar de conjuntos de datos de utilidad para la actividad auditora, so pena de devaluar el alcance de esta y hacerla ineficiente.
Una categorización y catalogación de riesgos, en sus distintos niveles, resulta de ayuda a la hora de abordar la necesidad de disponer de un plan, o de aprobar una norma. También en cuanto a los datos y la IA que, sí o sí, interactúan con la función fiscalizadora. Analizar riesgos y evaluar impactos ayuda, en definitiva, a tomar la "decisión correcta".

En todo caso, se trata de una tarea de reflexión en el seno de cada OCEX, a partir de la cual, afrontar cada uno su propio PEGODA.

---

2 Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. https://www.boe.es/buscar/doc.php?id=BOE-A-2022-7191

3 Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2). Por cierto, directiva pendiente de trasposición española, pese a haber expirado el plazo concedido: https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963

4 Hay diversos test en el mercado especializado. Una referencia (por cierto, *"visión realizada con IA,"* y que al final señala que *"La IA generativa es experimental. Para obtener asesoramiento jurídico, consulta a un profesional"* anuncia la página, en: https://www.google.com/search?q=test+de+madurez+inteligencia+artificial+organizacion&sca_esv=69d96dd121669555&rlz=1C1GCEU_esES1114ES1114&sxsrf=AHTn8zqd_K-GhFL485G1hGjo0W4rokqHag%3A1745786553636&ei=uZYOaJTUJrKI7NYP8823gAM&ved=0ahUKEwjUlljbifmMAxUyBNsEHfPmDTAQ4dUDCBA&uact=5&oq=test+de+madurez+inteligencia+artificial+organizacion&gs_lp=Egxnd3Mtd2I6LXNlcnAiNHRlc3QgZGUgbWFkdXJleiBpbnRlbGlnZW5jaWEgYXJ0aWZpY2lhbCBvcmdhbml6YWNpb24yBRAhGKABMgUQIRigAUibTVCADVjkS3ACeACQAQCYAdoBoAH6J6oBBjAuMzcuMbgBA8gBAPgBAZgCJ6AC9CjCAgoQABiwAxjWBBhHwgIEECMYJ8ICBhAAGBYYHsICCBAAGIAEGKIEwgIFEAAY7wXCAggQABiiBBiJBcICBRAhGJ8FwgIHECEYoAEYCsICBBAhGBWYAwCIBgGQBgiSBwYyLjM2LjGgB66-AbIHBjAuMzYuMbgH4yg&sclient=gws-wiz-serp

4. Sin gobierno de datos no hay paraíso. Definir, elaborar y aprobar un PEGODA: ¿Cómo se hace? ¿Cuál debe ser su contenido?

4.1. Algunas ideas surgidas de los trabajos en curso en la Sindicatura.

Vamos a plantear ahora, sucintamente, algunas cuestiones que surgen en los debates que el proceso de elaboración de un PEGODA propicia y, cuyo mero hecho, ya supone un crecimiento de la respectiva institución en la búsqueda de respuestas adecuadas a la creciente *datificación*[5] en que se desarrolla la actividad de las AAPP, objeto de nuestro control externo, y que, por lo tanto, condiciona nuestras funciones como fiscalizadores públicos:

- Quién y cómo interviene en su elaboración y puesta en marcha. La clave puede estar en promover la participación del personal comprometido, fundamentalmente de los equipos de auditoría, como núcleo duro del negocio de los OCEX. También, los gestores de servicios comunes (secretarías generales), alineados en un objetivo compartido, definido por el PEGODA, obtenido del trabajo conjunto y con el máximo consenso posible en el seno de cada órgano de control externo. Plan que debe incidir, a su vez, en el Plan Estratégico de la entidad.

- Se trata de pautar una regla de comportamiento previsible, constituir una guía o norma común para relacionarse con los datos[6], en sus diferentes orígenes y procedencias, dentro de un marco seguro y controlado, para responder a las necesidades que el uso de la IA nos viene a plantear. Y, por supuesto, manteniendo al respectivo equipo auditor al que se le asigne el trabajo de fiscalización de que se trate, como propietario de los datos usados en el mismo y garantizando, así mismo, su uso y accesos exclusivos por el personal que debe tener acceso a ellos, generando las evidencias oportunas que lo acrediten frente a terceros, con arreglo a las exigencias de las guías de fiscalización vigentes.

- La transversalidad del PEGODA es esencial, y debe estar dirigida a toda la organización, pero fundamentalmente ha de orientarse como utilidad para los servicios y equipos de auditoría en su labor fiscalizadora diaria. El valor de los datos internos y su uso uniforme, siguiendo unas pautas consensuadas y escritas, que vinculen a toda la Institución, debe ser el santo y seña del plan.

- Aparte de los datos internos que ya pueda poseer el OCEX, los datos externos delimitan lo que podríamos denominar la zona perimetral del PEGODA, el camino hacia una interoperabilidad integral, verdadera y plenamente operativa, por parte de las ICEX con todos los repositorios y bases de datos (estructuradas) de las distintas administraciones públicas (AAPP), que contienen datos e información relevantes para el normal ejercicio de la función de control externo sobre el sector público.

No las citaremos todas, pero sí recordar algunas muy valiosas para una fiscalización certera y de calidad, en función de la tipología de cada trabajo: PREEL[7], PCSP[8], BDNS[9], IGAE[10], AEAT[11], TGSS[12], AIREF[13], BE[14], CORME[15], OIRESCON[16], DGT[17], etc.

---

5 https://en.wikipedia.org/wiki/Datafication

6 ¿Por qué no elaborar en el futuro una guía de fiscalización específica sobre los procedimientos a utilizar en el manejo de los datos, a partir de la concepción que subyace en el PEGODA?

7 https://www.rendiciondecuentas.es/es/index.html?locale=es

8 Plataforma de Contratación del Sector Público: https://contrataciondelestado.es/wps/portal/plataforma

9 Base de datos nacional de subvenciones: https://www.pap.hacienda.gob.es/bdnstrans/inicio

10 Base de datos de la Intervención general de la administración del Estadio: https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/BasesDatos/paginas/basesdatos.aspx

11 Base de datos de la Agencia estatal de la administración tributaria: https://sede.agenciatributaria.gob.es/Sede/gobierno-abierto/reutilizacion-informacion/datos-disponibles-catalogo-datos-abiertos-tributaria.html Por cierto, para cuándo poder acceder los OCEX a otros datos que le son útiles para su función auditora del sector público, más allá del catálogo de datos abiertos? Al fin y al cabo, tan solo se trata de revisar el art. 95 de la vigente Ley General tributaria y establecer una previsión para los OCEX, del mismo tenor que la excepción prevista en apartado "g: en el ejercicio de sus funciones de fiscalización" para el Tribunal de Cuentas. O, ¿acaso no son los OCEX homologables al TCU en cuestiones como estas?

12 Base de datos de la Tesorería General de la Seguridad social: https://w6.seg-social.es/PXWeb/pxweb/es

13 Base de datos de la Agencia Independiente de responsabilidad fiscal: https://www.airef.es/es/acceso-a-datos/

14 Bases de datos del Banco de España: https://www.bde.es/wbe/es/areas-actuacion/central-balances/bases-de-datos-y-aplicaciones/bbdd-datos-publicas-informacion-sectores/

15 portal de Datos Abiertos de los Registradores de España: https://opendata.registradores.org/

16 https://www.hacienda.gob.es/es-ES/Oirescon/Paginas/ias.aspx

17 Plataforma de intermediación de datos de la DGT: https://sede.dgt.gob.es/es/otros-tramites/tramites-para-administraciones/plataforma-de-intermediacion-de-datos/

Se trataría de socializar la usabilidad resultante de grandes conjuntos de datos, con una estructuración mínima suficiente que permita su descarga en tiempo real, para una analítica específica según el trabajo de auditoría de que se trate en el respectivo OCEX, mediante los filtrados oportunos, efectuados con las imprescindibles medidas de seguridad (normas de interoperabilidad ENI[18] y, sobre todo, ENS[19]), siempre sobre el dato único como materia prima de consumo por los auditores, y cuyo mantenimiento y otorgamiento de permisos (en función de las competencias atribuidas por las leyes) corresponden al titular del respectivo repositorio o base de datos.

En suma, plantear la eficiencia (economías de escala) *ab initio* y por defecto. ¿O es pedir mucho que las AAPP y los ICEX se pongan de acuerdo en estos aspectos? El sector privado, así puede comprobarse a diario, está dispuesto a lo que sea con tal de *hacerse* con nuestros datos, para ejercitar su –legítima– actividad económica en el mercado global de bienes y servicios. ¿Tiene algún sentido que esta realidad y enfoque no estén plenamente incorporados –a través de una secuencia ordenada– en la planificación estratégica de los OCEX? Una vez más, ahí lo dejo: deberes pendientes tenemos. El PEGODA puede suponer un paso más para estar debidamente preparados ante esa interacción necesaria con bases de datos y repositorios externos[20].

- En ese sentido, el PEGODA ha de contribuir al aprovechamiento de datos que actualmente, o no se tienen, o se pierden. Este proyecto también debe permitirnos dejar de perder datos que, en su mayor parte autogeneramos y que, en la actualidad, no somos capaces de reutilizarlos, analizarlos o aprovecharlos para futuros trabajos.

- Y la pregunta clave: ¿Qué objetivos tenemos con la aprobación de un PEGODA? ¿Para qué ha de servirnos en la auditoría? En mi opinión, se trata de contar con un instrumento de estandarización de procedimientos y forma de estructuración de los datos, que permita avanzar en la transición iniciada desde una auditoría de documentos a otra basada en los datos; una suerte de guía común, al servicio de los equipos de auditoría, para el acceso, gestión, tratamiento, uso, explotación y difusión de los datos utilizados en la labor fiscalizadora, en función de las necesidades de los respectivos trabajos.

- Como valor adicional, nada desdeñable, el PEGODA también ha de proporcionar, en el terreno de la *compliance*, evidencias suficientes de cara a terceros, en lo que se refiere al empleo de buenas prácticas tanto en materia de seguridad –ENS, NIS 2–, interoperabilidad –ENI–, como de protección de datos[21] y confidencialidad.

Igual que los OCEX auditamos, no solo CBCS (controles básicos de ciberseguridad), sino gobiernos de TI (tecnologías de la información) de los entes sujetos al control externo, debemos ser capaces de *predicar con el ejemplo*, acreditando una gestión de datos y sistemas respetuosa con estos principios regulatorios que permitan que podamos también ser auditados acerca de cómo lo hacemos.

- Un gobierno de los datos que así mismo debe orientar una clasificación de estos –de carácter oficial o público– y posibilitar la reutilización[22] de la información que contienen, en las debidas condiciones de *anonimización*[23] en cada caso exigibles.

- El procedimiento estructurado de gestión de los datos, o, si se quiere, sistema de datos, debe ser el corazón del plan. Su finalidad ha de ser la generación de un cauce para una relación operativa con los distintas repositorios y fuentes de datos; debe permitir, respecto de cada fuente de información, actuar con una ficha de sus metadatos y su contenido; las formas de acceso seguro; la gestión y control de accesos y su descarga funcional para el uso que precise el equipo auditor que los utilice, todo ello dejando

18 Esquema nacional de interoperabilidad: https://administracionelectronica.gob.es/ctt/verPestanaGeneral.htm?idIniciativa=eni

19 Guía de Seguridad de las TIC CCN-STIC 813 CIBERSEGURIDAD DE ESPACIOS DE DATOS https://www.ccn-cert.cni.es/es/guias.html

20 https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/aepd-publica-guia-para-ayudar-empresas-y-aapp-cumplir-rgpd

21 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

22 Real Decreto-ley 24/2021, de 2 de noviembre, de transposición de directivas de la Unión Europea en las materias de … datos abiertos y reutilización de la información del sector público, ejercicio de derechos de autor y derechos afines aplicables a determinadas transmisiones en línea y a las retransmisiones de programas de radio y televisión.... https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-17910
Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos. https://www.boe.es/eli/es/rd/2021/03/30/203/con

23 https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/guia-y-herramienta-basica-de-anonimizacion

las evidencias suficientes de una actividad auditora que cumpla, no solo con la exigible integridad e inalterabilidad de los datos consultados, sino también con los marcos regulatorios de confidencialidad, privacidad y seguridad. Importante será, pues, diseñar ese procedimiento de acceso, intercambio y control, desde una adecuada perspectiva de reingeniería de procedimientos, donde la simplicidad de utilización no comprometa los valores a salvaguardar. ¿Existen ventajas de no hacerlo, de dejar espacio a la improvisación en algo tan trascendental en el proceso de elaboración de las auditorías?

- En último término, un PEGODA también puede ayudar a salvar el vacío existente en cuanto a la falta de unas Normas técnicas sobre el tratamiento y preservación de la información (datos), en aras a propiciar una operativa garantista de la información obtenida de las bases de datos de consulta necesaria para ejercer la función fiscalizadora, ya residan en los repositorios primarios de sus propietarios –cuentadantes–, o en los depósitos secundarios en que se alojan a través de los numerosos y a menudo diversos y solapados (tediosos, si escuchamos a los responsables de la intervención de las entidades fiscalizadas), procedimientos de rendición.

- Insistiremos una vez más, pues, en demandar una interoperabilidad real y efectiva entre los datos que poseen las diferentes AAPP para mejorar los estándares de auditoría, permitiendo pasar de los tradicionales muestreos a la analítica de grandes conjuntos de datos. El PEGODA puede ser un camino, aún parcial, para lograr ese objetivo.

4.2. ¿Cuál podría ser el contenido del PEGODA?[24]

En realidad, el propio PEGODA no puede concebirse sin una política de gobierno del dato (PGD) que lo inspire y justifique. Plan y política (del dato) son elementos complementarios.

Ante la ausencia de una cultura del dato consolidada, el PEGODA puede proponer un modelo propio de datos estándar, con vocabularios para codificar las variables con las que trabajamos: generar un proceso de acceso y uso de la información, que actualmente no es uniforme ni está sistematizado, superando los accesos, gestionados puntualmente de forma ad hoc, según las necesidades concretas de cada momento y usuario, y sin un procedimiento claramente definido, lo que no alimenta, precisamente, la eficiencia. Tener o no tener PEGODA Y PGD puede marcar un salto cualitativo en la manera de hacer las cosas.

- **Contenido de la PGD:**

  La PGD debe evaluar el uso actual y futuro de los datos, dirigiéndolo para asegurar que los datos satisfacen los objetivos de la entidad, y monitorizando su cumplimiento.

  También es propicio que incorpore, adaptándolos

24 Al momento de redactar este artículo, están en curso los trabajos de redacción del PEGODA en la Sindicatura, por lo en este apartado tan solo se apuntan algunas previsiones y orientaciones que han surgido en el seno del grupo de trabajo creado al efecto, y, por lo tanto, deben ser tomadas como propuestas iniciales, pendientes del proceso participativo con el personal de equipos a través de la Comisión Técnica de Auditoria (CTA).

a su propia realidad, los principios de gobierno del dato, detallados en la norma UNE 0077 (Gobierno del Dato)[25], que competen al órgano de gobierno del dato del OCEX acerca de: responsabilidad, estrategia, adquisición, desempeño, conformidad y comportamiento humano.

Así mismo, la PGD debe asegurar los requerimientos de los datos y su gestión en cuanto a: disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, cumplimiento, responsabilidad, transparencia y privacidad desde el diseño y por defecto.

Otro elemento fundamental es, para cualquier organización, la determinación de roles y responsabilidades concretas, en relación con los datos, de cuantos actores intervienen en este ámbito: desde el Consejo de Gobierno del Dato a la Oficina del Dato y su director, los usuarios finales, pasando por el responsable y administrador de seguridad, responsable de sistemas o delegado de protección de datos.

Un reparto de papeles en el que el auditor debe figurar como "propietario" de los datos que utiliza su equipo en los trabajos, que no deben salir más allá del respectivo perímetro de tareas, a cuyo fin, el PEGODA y la PGA pueden ser aliados inestimables para garantizarlo y evidenciarlo.

Deben recogerse, así mismo, las previsiones oportunas para asegurar las distintas fases del ciclo de vida de los datos: recopilación, almacenamiento, uso, mantenimiento y eliminación.

La PGD, por fin, debe prefijar, proactivamente, las medidas del ENS que resulten necesarias de acuerdo con la clasificación de los sistemas, más las adicionales que se requieran tras el análisis de riesgos realizado, dirigidas al control de accesos, el cifrado o anonimización necesarios, la seguridad física, las copias de seguridad y la concienciación de cuantos intervienen de una u otra forma en el ciclo de vida del dato.

- **Contenido del PEGODA:**

Aparte de lo apuntado en el punto anterior (4.1), teniendo en cuenta las normas UNE 0078 (Gestión del Dato)[26] y 0079 (Gestión de la calidad del dato)[27] parece adecuado que el PEGODA, por su parte, se refiera a:

- La Gobernanza de datos, estableciendo procedimientos claros para su gestión, concretando los roles y responsabilidades para la calidad, seguridad y privacidad de los datos.

- La Calidad de los datos, implementando procesos de validación, medición y limpieza, así como indicadores de seguimiento y control periódicos.

- La infraestructura necesaria, referida a los conjuntos de datos, con el fin de modernizar los sistemas de almacenamiento y procesamiento de datos, ajustándola a las necesidades que vayan demandando los cambios tecnológicos y creando, para ello, un Sistema Integral –o procedimiento estructurado– de Gestión de los Datos que ha de permitir centralizar la gestión del uso de todos los datos que el OCEX precise para realizar sus funciones de una manera segura, eficaz y eficiente.

- La integración e implementación de las herramientas de análisis de datos y visualización que se decidan por el consejo de gobierno del dato.

- Las garantías precisas para la seguridad y escalabilidad de los datos.

- La explotación de datos necesaria, que permita al personal del OCEX un análisis avanzado de datos, utilizando *big data*, *machine learning* o inteligencia artificial, en las condiciones que se autoricen (en las respectivas normas de uso de la IA), de todos los datos necesarios para el correcto desempeño de sus funciones.

- El establecimiento de cuadros de mando, paneles de control e informes personalizados, o autogenerados, referidos al uso y explotación de datos.

- Las previsiones de automatización de procesos de trabajo en aquellos ámbitos donde sea aconsejable y mejore la eficiencia en los informes y trabajos de auditoría.

- La promoción de la cultura del dato, a través de la formación del personal en el uso de los datos y de las herramientas de *big data* o IA necesarias.

- La demanda de los recursos necesarios, tanto propios de la organización, como de colaboradores

25 https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0071116

26 https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0071117

27 https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0071118

externos, para asegurar el cumplimiento de los objetivos fijados por el respectivo PEGODA, de acuerdo con el cronograma programado.

5. La regulación del uso de la IA[28] en los OCEX y el libre albedrío de su personal[29].

Siguiendo el esquema que hemos propuesto en estas reflexiones, lo primero es tener un gobierno del dato, como acabamos de apuntar; lo segundo (por desgracia, en algunos casos nos puede encontrar sin tenerlo todavía preparado) es cómo afrontar el uso de la IA en los trabajos de auditoría en un OCEX. Algunas reflexiones para abordar, sin demasiados riesgos, esta óptica novedosa:

- El PEGODA prevé la incorporación de la IA, pero no es suficiente. Hace falta regular, pero sobre todo concienciar y propiciar buenas prácticas, para minimizar riesgos latentes detectados en el análisis previo.

- La seguridad debe ser la incuestionable premisa: seguridad de inicio a fin, *Ian to Ian*.

- En cuanto al procedimiento del uso de la IA en las auditorias: recordar el escepticismo profesional y la supervisión humana como principios innegociables para permitir entrar a la IA en el negocio de la auditoría.

- A la hora de prever una normativa de esta naturaleza, se han de considerar las limitaciones intrínsecas que la IA debe comportar por su uso directo en la elaboración de Informes de auditoría, ya que se trata, en definitiva, de herramientas analíticas, que no proporcionan evidencias suficientes, y no pueden obviar la supervisión humana para validar sus datos o conclusiones. En todo caso, el auditor responsable debe comprobar la adecuación del uso de la IA que se haya utilizado en cada trabajo, y así deberá constar en los papeles de trabajo.

- Algunas dudas e incertidumbres que surgen en el proceso de reflexión sobre el uso de la IA en la fiscalización: ¿qué fuentes de conocimiento entrena la IA generativa en el ámbito de la auditoría? Debemos valorar el posible riesgo de que los datos del OCEX puedan alimentar, a través de las herramientas que tenemos contratadas en cada momento, el propio sistema de IA del que nos servimos, no solo nosotros, sino también terceros.

- ¿Qué directrices deben contener esas normas de uso de la IA? Los mensajes y procedimientos deben ser claros y precisos, para generar en el personal los comportamientos homogéneos y documentados que minimicen riesgos y que, a su vez, no afecten negativamente al contenido de los trabajos en que se haya utilizado.

Así pues, aportamos nuestra modesta experiencia en la materia:

5.1. Primero abordar el **Análisis de riesgos:**

En el caso de la Sindicatura, antes de las propias Normas, para su justificación, elaboramos un análisis de riesgos del uso de las propias herramientas de IA, Sucintamente: En primer lugar, se han analizado los procesos de gestión y tratamientos de datos personales de la Sindicatura (SC). Ninguno de ellos cumple los requisitos para ser considerado un tratamiento de alto riesgo del artículo 6 del RIA, ya que no está previsto utilizar la IA para procesos de selección y contratación de personas, ni para tomar decisiones de índole laboral (Anexo I y III).
Después, se han analizado los riesgos sobre:

- los derechos de las personas derivados del uso de datos personales gestionados por la SC.

- los datos confidenciales o restringidos gestionados por la SC.

- los derechos de propiedad en datos e información gestionados por la SC.

- riesgos específicos derivados del uso de herramientas de IA: Responsabilidad, respeto a los derechos humanos, transparencia, trazabilidad, equidad y no discriminación, sesgos, incumplimiento normativo.

Los riesgos se han agrupado en dos bloques y asignado probabilidades de ocurrencia en función de las medidas de protección existentes en cada tipo de sistema de IA, considerando dos tipos:

- Sistemas de IA contratados por la SC en los que el proceso de contratación garantiza que existan cláusulas contractuales de protección de datos adaptadas al RGPD y LOPDGDD, así como garantías de que el proveedor aplica las medidas de protección de TI en sus sistemas de información establecidos por el ENS.

28 A tener en cuenta el REGLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (en adelante RIA): https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81079

29 Sin perder de vista el respectivo Código Ético de cada OCEX. El de la Sindicatura, accesible en https://www.sindicom.gva.es/codigo-de-etica

- Sistemas de IA no contratados por la SC. No disponen de los controles de protección de los anteriores.

En ambos casos, se han valorado los posibles riesgos de: fuga de datos, tratamiento de datos inadecuado, de acceso no autorizado, de falta de transparencia, y de sesgos algorítmicos o generación de información incorrecta o falsa.

Finalmente, se ha evaluado el impacto en cada bloque.

5.2. En segundo lugar, abordar el **contenido de las Normas**: A partir de este análisis, se ha establecido la regulación contenida en las Normas de uso de la IA, estableciendo:

- Prohibiciones de uso.

- Casos de uso permitidos de IA en la SC con uso limitado.

- Supervisión humana y registro de la actividad. La norma subraya este aspecto, clave en el uso de la IA en la auditoría: Cuando se obtengan resultados derivados del uso de la IA de acuerdo para ser utilizados en los procesos de gestión o fiscalización de la SC, esos resultados deberán ser previamente revisados y verificados por las personas responsables del proceso o fiscalización. Se establece un procedimiento y formalidades específicas para ello.

- Elaboración de una norma que regule los usos correctos de IA en la Sindicatura[30].

La aprobación de estas normas nos ayuda así mismo a plantearnos otras cuestiones relevantes, como la necesidad de abordar un procedimiento estándar de anonimización de datos, que no demore el uso de las herramientas de IA que estén autorizadas, pero que garantice su uso con garantías.

En todo caso, somos conscientes de que esta primera aproximación reguladora, de urgencia si se quiere, ante la vis expansiva de las herramientas IA y su fácil e imperceptible deslizamiento en los propios trabajos de auditoría, debe ser objeto de constante seguimiento y supervisión, que inevitablemente dará lugar a adaptaciones en la regulación futura, en función de la propia dinámica e interacción de IA en las fiscalizaciones y la experiencia que se vaya acumulando.

5.3. Por último, –o, mejor, en primer lugar– y para el debate: **Algunas reflexiones adicionales sobre la IA en la nueva *"Auditor-IA"***:

- ¿Qué IA utilizar en la auditoría pública? ¿Sabemos lo que queremos, o lo que necesitamos?

- Si las herramientas no son transparentes, si no conocemos los algoritmos que las sustentan, ¿las compramos sin más, por capítulo 2, sobre una base intuitiva?

- ¿O nos proveemos de nuestras propias herramientas de IA?

- Además, habrá que valorar previamente, como en todas las soluciones y desarrollos tecnológicos que precisemos, las previsiones de los arts. 157 y 158 de la Ley 40/2015.

- Es más, dada la especificidad de las funciones de los OCEX y el TCU, ¿Y si consorciáramos[31] el desarrollo conjunto de la IA que verdaderamente necesitamos los OCEX?

- De esta manera, el intercambio de conocimiento que precisa la IA generativa se crearía desde el propio *know how* y experiencias auditoras, lo que podría suponer un punto de partida para construir una IA *ad hoc* en la auditoría pública.

- Por último, ¿estamos capacitados para auditar el uso adecuado de la IA por los entes que fiscalizamos?, ¿Queremos, o debemos hacerlo? ¿Contamos con cualificación suficiente para desvelar y auditar los algoritmos que están detrás de esas herramientas utilizadas?

Entre todos deberemos conformar respuestas y soluciones a estos retos y problemas.

6. Alineación del PEGODA con el Plan Estratégico de la Entidad.

Trazando líneas de futuro. Los planes estratégicos no son documentos inamovibles. Conviene revisarlos periódicamente para acompasar la acción y organización de cada OCEX a su entorno, como instrumentos esenciales para encauzar el futuro.

30 No accesible en general, no es un documento público, sólo de uso interno por el personal de la Sindicatura. Para más información, se puede contactar con el autor de este artículo lperez@sindicom.es

31 Ya disponemos de experiencias similares positivas: PREEL, FISCALICEX, FISCONEX…

Si el dato es la materia prima de la auditoría (los grandes espacios y conjunto de datos) y, por ello precisamente proponemos la incorporación de su gobierno y organización en un plan estratégico propio que guie la evolución en la metodología de trabajo de la función fiscalizadora, parece razonable plasmar esta realidad al más alto nivel de cada OCEX, mediante su incorporación expresa en el respectivo Plan Estratégico, para orientar la trayectoria a seguir en el seno de cada OCEX.

Esa revisión debe llevarse a cabo mediante un proceso participativo, abierto al personal de cada organización, que incorpore e integre la visión de quienes conocen, por su trabajo diario, el ejercicio de la función fiscalizadora. También debe plasmar adecuadamente el compromiso de la alta dirección en alinear y presupuestar los recursos necesarios (humanos, tecnológicos y presupuestarios) para alcanzar los objetivos que el propio plan estratégico recoja.

7. A modo de resumen.

Por concluir:

- Y todo esto de la IA y los PEGODAs en la auditoría, incluso la revisión del propio Plan Estratégico de la institución –se podrá preguntar algún IA-dato-escéptico–, además de lo que hemos tratado de exponer sintéticamente, ¿viene a cuestionar los fundamentos de la auditoría?
  La respuesta debe ser negativa, pues precisamente las premisas de escepticismo profesional y supervisión humana por defecto hemos dejado claro que deben ser la perspectiva para su utilización en los trabajos de auditoría.

- Y ¿para qué sirve?

Es innegable que, con la pujanza y expansión de los datos y la IA, la auditoría pública ya no va a ser la misma tal y como la conocíamos. Por ello, debemos prepararnos y adaptarnos: en definitiva, resiliencia. Si no, la realidad se nos echará encima.

- Con todo esto, ¿va a cambiar la forma de relacionarnos con nuestros entes fiscalizados?

Efectivamente. De hecho, ya venimos experimentando ese cambio. ¿Quién no ve esa alianza necesaria entre el control interno y el externo? Ciertamente, no se trata de caer en el síndrome de Estocolmo, a la hora de relacionarnos con los entes fiscalizados, pero sí debemos comprender el rol de estos en el ejercicio de esa otra función pública, la de gestionar las respectivas parcelas de los intereses generales (competencias), en un razonable marco de rendición y cumplimiento. Por ello, todo nos debe conducir a facilitar lo que podríamos definir como una *auditoría ecuánime*[32], fiscalizaciones que deben gravitar sobre un equilibrio que garantice, de forma razonable, que cada AP cumple con los objetivos que le marca su respectiva normativa reguladora en el ejercicio de las funciones públicas encomendadas, ya sea como prestadoras de servicios o actividades llevadas a cabo con fondos públicos; y que acredite que lo hacen de forma económica, eficaz y eficiente.

Los datos, ciertos, únicos, objetivos e inalterables, deben ser el foco de atención que sustentan esos trabajos de auditoría. Saber cómo acceder con garantías a los grandes conjuntos de datos, sin duda reforzará el contenido y rigor de los trabajos de auditoría y, por ende, la confianza en las instituciones de control.

Complementariamente, si implantamos de forma inteligente la IA en los OCEX, esta puede ser una aliada inestimable para los responsables de ejercer la función pública de control externo en el sector público.

- Entonces, ¿basta con aprobar un PEGODA, incluso revisar el propio plan estratégico?
  Sin duda, no serán pasos suficientes, pero sí necesarios, pues también resulta preciso adaptar y adecuar la estructura de los recursos de nuestras organizaciones para este cambio de época, algo más que una época de cambios. Es imprescindible seguir ahondando en un proceso continuo de formación y concienciación que fomente y propicie las aptitudes y actitudes requeridas para ello entre el personal de los OCEX.

  También es inaplazable la Incorporación de nuevos perfiles profesionales, con preparación suficiente en el campo tecnológico y de la analítica, acordes con este nuevo escenario que los datos y la IA nos plantean. La colaboración público–privada puede facilitar, así mismo, a costes razonables, la incorporación de talento especializado en sectores muy concretos, imprescindibles en la fiscalización moderna, donde no siempre es fácil llegar con los recursos tradicionales

32 El diccionario de la lengua española de la RAE define ecuánime: 1. adj. Que tiene ecuanimidad. imparcial, objetivo, neutral, ponderado, equilibrado, desapasionado, equitativo, recto, honrado, sereno, justo, sosegado, mesurado, razonable.

de reclutamiento del empleo público.

En definitiva, como se comentaba en el último Congreso Nacional de auditoría de 2024 –creo recordar que la cita era de Daniel Innerarity–, en la actualidad existen espacios de ruptura, como también ámbitos de inevitable imprevisibilidad, y en ese escenario, la IA siempre tendrá un papel complementario respecto del conocimiento de las personas.

Aplicado a nuestro campo –la auditoría pública– podríamos añadir, para concluir, que la cultura ética y la responsabilidad pública son valores incuestionables que deben acompañar el uso de la IA, y que, para ello, antes debemos tener claro cómo gobernamos, de forma segura, responsable y garantista, los datos con los que ahora trabajamos, y otros conjuntos de datos a los cuales todavía no llegamos, en ese ejercicio de auditoría en pleno proceso de cambio.

También por ello deberemos rendir cuentas, o ser debidamente auditados.