

ESPECIAL

“Tecnoregulación en Prospectiva”

DE **Tecnología & Sentido Común**



ESPECIAL

AGOSTO
2025

¿Quién dijo que la cartera europea de identidad digital garantizase el anonimato?

08

La Directiva NIS2 sigue pendiente de transposición

12

Llega el desarrollo parcial, aunque ciberamplio, de la Directiva NIS2

20

Llegó el primer paquete de actos de ejecución de la Cartera Europea de Identidad Digital

24

Representación de instrumentos financieros mediante tecnología de registros distribuidos

28

La bolsa o la ViDA

16

Luchando contra la suplantación de identidad telefónica y por SMS

32

En tiempo de descuento para la implantación de Veri*Factu

36

Caminando hacia la Cartera Europea de Identidad Digital: llega MiDNI

40

Acuerdo sobre algoritmos criptográficos post-cuánticos

44

Nuevas herramientas y procesos digitales en el Derecho de sociedades: el efecto eIDAS (parte 1)

48



ESPECIAL “Tecnoregulación en Prospectiva”

DE **Tecnología & Sentido Común**



EQUIPO TYSC

Javier Peris - El Governauta

Manuel Serrat - Futuro y Seguridad

Nacho Alamillo - Tecnoregulación en Prospectiva

Juan Carlos Muria - Diario de una Tortuga Ninja

Marlon Molina - Es Tendencia

Ricard Martínez - Ojo Al Dato

Marcos Navarro - Ai Futuro

Víctor Almonacid - La Nueva Administración

Alex Aliaga - Radio Security

Marta Martín - Mentas Divergentes

PUBLICIDAD Y CONTRATACIÓN

Carmen Usagre

carmen.usagre@businessandcompany.com

Teléfono: +34 96 109 44 44

GABINETE JURÍDICO

Jesús López Peláz

ATENCIÓN AL LECTOR

soluciones@businessandcompany.com

EDITA

Business, Technology & Best Practices, S.L.

Av. San Onofre, 20

46930-Quart de Poblet (Valencia)

Teléfono: 96 109 44 44

Fax: 96 109 44 45

<https://tecnologiaysentidocomun.com>

soluciones@businessandcompany.com



NACHO ALAMILLO

Es Doctor en Derecho por la Universidad de Murcia. Licenciado en Derecho por la UNED. Auditor de Sistemas de Información certificado, CISA. Director de Seguridad de la Información certificado, CISM. Ingeniero Certificado en Soluciones de Protección de Datos, CDPSE, por ISACA.

En la actualidad, es Abogado del Ilustre Colegio de Reus, Asesor de Logalty y Director General de Astrea La Infopista Jurídica SL. Asimismo, colabora con el Grupo de Investigación iDerTec de la Universidad de Murcia.

También es miembro del grupo de Infraestructura de Seguridad de Firma Electrónica del Instituto Europeo de Normas de Telecomunicaciones, que normaliza los servicios de confianza, miembro de UNE CTN71/SC307, de CEN-CLC/JTC 19 y de ISO TC 307, relativos a Blockchain.

Dispone de más de 100 publicaciones y ha impartido más de 400 ponencias en identidad digital, servicios de confianza y materias relacionadas.

(Business&Co.®) Business, Technology & Best Practices, S.L. en ningún caso y bajo ningún supuesto se hace responsable de las opiniones aquí expresadas por sus colaboradores o entrevistados.

Business&Co.®, Escuela de Gobierno eGob®, Master en Gobierno de Tecnologías de la Información MGEIT®, Caviar®, Telecoms®, Respalda® y AulaDatos® son Marcas y Nombres Comerciales Registrados de Business, Technology & Best Practices, S.L. "COBIT® es una Marca Registrada de ISACA.

ISSN 2951-8180

**La Escuela de Gobierno eGob®
Certifica su Sistema de Gestión
de Organizaciones Educativas
con la Norma ISO 21001**

Alcance: Formación Certificada y Programas Directivos para Alta Dirección,
Mandos Intermedios y Responsables de la Ejecución Estratégica
y el Cambio Organizacional en Organizaciones Públicas y Privadas



ESPECIAL
AGOSTO
2025



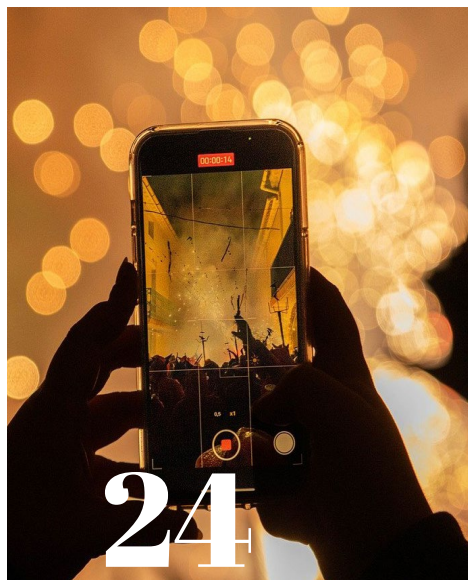
índice

DE CONTENIDOS

<https://tecnologiaysentidocomun.com>



**La bolsa o
la ViDA**



**Llegó el primer paquete de actos
de ejecución de la Cartera
Europea de Identidad Digital**



**En tiempo de
descuento para
la implantación**



**Acuerdo sobre
algoritmos criptográficos
post-cuánticos**

Copyright

02

Índice de Contenidos

04

Este mes te recomendamos leer...

por JAVIER PERIS

07

¿Quién dijo que la cartera europea de identidad digital garantizase el anonimato?

08

La Directiva NIS2 sigue pendiente de transposición

12

La bolsa o la vida

16

Llega el desarrollo parcial, aunque ciberamplio, de la Directiva NIS2

20

Llegó el primer paquete de actos de ejecución de la Cartera Europea de Identidad Digital

24

Representación de instrumentos financieros mediante tecnología de registros distribuidos

28

Luchando contra la suplantación de identidad telefónica y por SMS

32

En tiempo de descuento para la implantación de Veri*Factu

36

Caminando hacia la Cartera Europea de Identidad Digital: llega MiDNI

40

Acuerdo sobre algoritmos criptográficos post-cuánticos

44

Nuevas herramientas y procesos digitales en el Derecho de sociedades: el efecto eIDAS (parte I)

48

Cierre de Temporada 2025 Revistas “Tecnología y Sentido Común” y “Stakeholders.news”

52

UNE presenta su Estrategia 2030 para lograr un mayor impacto de las normas en la sociedad

68

TECH

#TYSC

Premios recibidos



Premio 2016 a la Difusión de los Valores de la Gestión y Gobierno TI



El Foro de Profesionales de la Gestión del Servicio en España itSMF otorga a «Tecnología y Sentido Común» el Galardón 2016 a la Difusión de los Valores de la Gestión y Gobierno de Tecnologías de la Información.

itSMF
ESPAÑA

Premio 2022 ESET al Periodismo y Divulgación en Seguridad Informática



VI Premios ESET Periodismo y Divulgación: Tecnología y Sentido Común Premiada en la Categoría Blogs por el Artículo de Ricard Martínez "Seguridad en el Smartphone".

Los Premios ESET apuestan por la educación y la concienciación de la sociedad en materia de ciberseguridad, y los medios de comunicación son esenciales en este cometido.

Los periodistas y divulgadores son fundamentales para difundir el conocimiento necesario que permita a los usuarios disfrutar de la tecnología de una manera más segura.

Estos VI Premios ESET pretenden fomentar la divulgación de la ciberseguridad.



Premio Medio de Comunicación 2018 de la Asociación Profesional Española de Privacidad



La Junta Directiva de la Asociación Profesional Española de Privacidad durante su VI Congreso Nacional de Privacidad APEP celebrado en Madrid otorga el Premio Medio de Comunicación 2018 a Tecnología y Sentido Común #TYSC



Agradecimiento de la Asociación Valenciana de Informática Sanitaria AVISA



La Asociación Valenciana de Informática Sanitaria AVISA durante las XIV Jornadas Técnicas que bajo el título "20 Años Implantando TIC en Sanidad" se celebraron en Benidorm en febrero de 2024 hizo entrega de su agradecimiento a Tecnología y Sentido Común por su apoyo y visibilidad a la profesión.



Tecnología y Sentido Común "Premio Sapiens" Medio de Comunicación 2022



El Colegio Oficial de Ingeniería Informática de la Comunidad Valenciana entregó el Premio Sapiens Medio de Comunicación 2022 a nuestra Revista "Tecnología y Sentido Común #TYC". El Colegio Oficial de Ingeniería Informática de la Comunidad Valenciana COIICV alabó tanto la gran labor de difusión que viene realizando Tecnología y Sentido Común desde hace siete temporadas como su capacidad de adaptación y resiliencia adaptándose a nuevos formatos con los que continuar en su labor de evangelización en Buenas Prácticas al conjunto de los profesionales a pesar de la alerta sanitaria con nuevos formatos que partiendo de un programa de Radio y Podcast han permitido seguir llevando su mensajes a través de la Revista Mensual, o el informativo televisivo "El Semanal" de Tecnología y Sentido Común.



Gobierno del Tiempo y Gestión de la Productividad con Time Slot Governance TSG4®



Gobierno del Tiempo y Gestión de la Productividad con TSG4 White Belt

Javier Peris

Tras más de veinte años en las trincheras del gobierno TI y el Cambio organizacional, he visto a demasiados profesionales brillantes ahogarse. Vivimos encadenados a las notificaciones, luchando contra un torbellino de urgencias que devora nuestra capacidad para el trabajo profundo. Creemos que el *burnout* es el precio del éxito.

He escrito “**Gobierno del Tiempo y Gestión de la Productividad TSG4 White Belt**” porque estoy convencido de que estamos equivocados y quiero demostrártelo.

Te aseguro que no es otro método de productividad; es un manifiesto para una verdadera revolución personal.

Con este libro “**Gobierno del Tiempo y Gestión de la Productividad TSG4 White Belt**”, mi objetivo es darte la dosis fundamental de

conocimientos que no sabías que necesitabas. En él, disecciono la enfermedad de nuestra era: el “Lingchi Temporal”, esa muerte por mil cortes de interrupciones que aniquila nuestro foco.

Este primer libro es un llamado a las armas. Te obliga a abandonar el rol de “Gestor eficiente del caos” para asumir tu verdadero poder y responsabilidad como “Gobernador de tu tiempo”. No ofrezco herramientas, sino algo mucho más valioso: un cambio de paradigma.

Mi meta es que veas tu semana no como una agenda que se llena, sino como un territorio soberano que debes gobernar.



¿Quién dijo que la cartera europea de identidad digital garantizase el anonimato?

El anuncio del Ministro para la Transformación Digital y de la Función Pública de la Cartera Digital Beta, con capacidad para la prueba de mayoría de edad, coloquialmente conocido como “pajaporte”, ha generado un fuerte debate acerca de las propiedades de seguridad de dicha Cartera Europea, en el marco del Reglamento eIDAS 2, con quien los lectores de esta sección están más que familiarizados ya.

En concreto, reiteradamente se ha manifestado que el sistema propuesto permitiera garantizar el anonimato del usuario que lo emplea para acreditar que es mayor de edad, lo que ha producido una fuerte reacción por parte de diversos expertos en ciberseguridad, en especial del ámbito de la criptografía. ¿Es correcta esa referencia al anonimato? Para aclarar a qué nos estamos refiriendo, podemos adoptar la definición de autenticación de entidad anónima (anonymous entity authentication) contenida en ISO/IEC 20009-1:2013, que es la corroboración de que una entidad posee ciertos atributos, sin distinguir a esta entidad de otras entidades con los mismos atributos. Más en concreto, normalmente nos estaríamos refiriendo a mecanismos de autenticación anónima unilateral.

En la medida en que se afirma que este sistema se encuentra alineado con el Reglamento eIDAS 2, podemos acudir al texto aprobado para valorar esta cuestión. Ciertamente, llama la atención que los términos “anonimato” o “anónimo” no se encuentren en el Reglamento eIDAS 2, indicativo de que quizá no haya sido intención de los co-legisladores que se disponga de un sistema que en efecto garantice el anonimato.

Hay que recordar que la cartera europea de identidad digital es un medio de identificación electrónica, por lo que, con carácter general, precisamente su finalidad principal es la autenticación del usuario, que el Reglamento define como el “proceso electrónico que permite la confirmación de la identificación electrónica de una persona física o jurídica, o la confirmación del origen y la



CONTINÚA EN
PRÓXIMA PÁGINA



integridad de datos en formato electrónico”; donde la identificación electrónica es el “proceso consistente en utilizar los datos de identificación de la persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a otra persona física o a una persona jurídica”, y los datos de identificación de persona, el “conjunto de datos que se emite de conformidad con el Derecho de la Unión o nacional y permite establecer la identidad de una persona física o jurídica, o de una persona física que representa a otra persona física o a una persona jurídica”.

La cartera permite al usuario “solicitar, obtener, seleccionar, combinar, almacenar, eliminar, compartir y presentar de forma segura, bajo el control exclusivo del usuario, datos de identificación de la persona y, cuando proceda, en combinación con declaraciones electrónicas de atributos, autenticarse ante partes usuarias en línea y, en su caso, en modo fuera de línea, con el fin de acceder a servicios públicos y privados, velando al mismo tiempo por que sea posible divulgar los datos selectivamente”, para lo cual la cartera debe disponer de una interfaz “para compartir con las partes usuarias, y presentarles, datos de identificación de la persona, una declaración electrónica de atributos

o datos conexos divulgados selectivamente, en línea y, cuando proceda, en modo fuera de línea”.

Nada más lejos del anonimato, sin perjuicio de que se hayan previsto medidas para evitar que la cartera europea sea una especie de super-cookie. En concreto, el Reglamento exige que el marco técnico de la cartera europea de identidad digital cumpla dos condiciones:

a) no permitirá que, tras la expedición de la declaración de atributos, los prestadores de declaraciones electrónicas de atributos o cualquier otra parte obtengan datos que permitan que se rastree, vincule o correlacione, u obtener de cualquier otra manera, conocimiento de las transacciones o del comportamiento del usuario a menos que este lo autorice explícitamente;

b) permitirá tecnologías de protección de la privacidad que garanticen la no vinculación, cuando la declaración de atributos no requiera la identificación del usuario.

La primera exigencia se refiere a la no observabilidad (*unobservability*), concepto que para la Comisión Europea significa que no debe haber correlación de datos entre diferentes servicios con fines de seguimiento o localización de usuarios o para determinar, analizar y predecir el comportamiento, los intereses o los hábitos personales.

La segunda exigencia se refiere a la no vinculación (*unlinkability*), concepto que se encuentra ampliamente tratado en los estándares internacionales, que en ISO/IEC TR 27550:2019 se define como “propiedad que garantiza que un interesado pueda hacer varios usos de recursos o servicios sin que otros puedan vincular estos usos entre sí”.

Estas exigencias apuntan a que la cartera europea de identidad digital se pueda considerar como un sistema de autenticación de entidad sin vinculación basado en atributos (*attribute-based unlinkable entity authentication*), que proporciona un medio para que los interesados establezcan la autenticidad de un subconjunto seleccionado de sus atributos de identidad sin revelar un subconjunto más grande, antes que como un sistema que se oriente a garantizar el anonimato. El debate, sin duda, está servido.

P4MGO!® Essentials

**Portfolio, Programme,
Project & Product
Management &
Governance**



La Directiva NIS2 sigue pendiente de transposición

De forma lamentable, el 17 de octubre entrará en vigor la Directiva NIS2 (), que se encuentra pendiente de transposición al ordenamiento jurídico español, generando una innecesaria inseguridad jurídica a las entidades sujetas a su ámbito de aplicación, en especial aquellas que no se encontraban sujetas a la Directiva NIS –Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión–, transpuesta por Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (RDLSRI).

La Directiva NIS2 contiene importantes innovaciones con respecto a la normativa actualmente vigente, al objeto de reforzar la política de la Unión en este ámbito.

En primer lugar, se amplía el ámbito de aplicación con nuevos sectores basados en su grado de digitalización e interconexión y en su importancia para la economía y la sociedad, introduciendo una norma de umbral de tamaño claro, lo que significa que todas las empresas medianas y grandes de los sectores seleccionados quedarán sujetas. Adicionalmente, los Estados miembros pueden identificar entidades más pequeñas con un perfil de alto riesgo para la seguridad, de modo que queden sujetas a las obligaciones legales.

Resulta muy significativa la ampliación de las entidades del sector de infraestructura digital, incluyendo proveedores de redes de servicios de computación en la nube, proveedores de distribución de contenidos, prestadores de servicios de confianza, proveedores de servicios de centro de datos y proveedores de redes públicas de comunicaciones electrónicas, así como



CONTINÚA EN
PRÓXIMA PÁGINA





servicios de comunicaciones electrónicas disponibles para el público, o la inclusión del sector de gestión de servicios de TIC (de empresa a empresa), con proveedores de servicios gestionados y proveedores de servicios de seguridad gestionados. Otros sectores novedosos incluyen los servicios postales y de mensajería, la gestión de residuos, la fabricación, producción y distribución de sustancias y mezclas químicas, la producción, transformación y distribución de alimentos y determinados subsectores del sector de fabricación, lo que muestra la importancia de que dichas entidades conozcan y puedan cumplir sus obligaciones jurídicas.

A diferencia de la normativa actual, las entidades sujetas se clasifican en función de su importancia y se dividen en dos categorías: entidades esenciales e importantes, sujetas a diferentes regímenes de supervisión.

Entre otras, son entidades esenciales las grandes empresas de los sectores de alta criticidad; independientemente de su tamaño, los prestadores cualificados de servicios de confianza y registros de nombres de dominio de primer nivel y los proveedores de servicios de DNS; y las medianas empresas proveedoras de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles para el público, en una muestra más de la creciente dependencia en estos servicios. Asistimos, de este modo, a una verdadera convergencia en la política de ciberseguridad.

La normativa fortalece y racionaliza los requisitos de seguridad y presentación de informes por las entidades mediante la imposición de un enfoque de gestión de riesgos, que proporciona una lista mínima de elementos básicos de seguridad que deben aplicarse; así como se introduce disposiciones más precisas sobre el proceso de notificación de incidentes, el contenido de los informes y los plazos.

Además, y esta es la segunda gran novedad a la que me voy a referir, la Directiva NIS2 aborda la seguridad de las cadenas de suministro y las relaciones con los proveedores, exigiendo a las empresas que aborden los riesgos de ciberseguridad en las cadenas de suministro y en las relaciones con sus proveedores.

Precisamente por su importancia, la Directiva exige a la Comisión antes del 17 de octubre de 2024 adoptar actos de ejecución por los que se establezcan los requisitos técnicos y metodológicos de las medidas de seguridad con respecto a los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centros de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, así como los proveedores de mercados en línea, de motores de búsqueda en línea y de plataformas de servicios de redes sociales, y los prestadores de servicios de confianza.

La ausencia de transposición de la Directiva NIS2 dentro del plazo establecido genera una fuerte inseguridad jurídica, que sólo se ha visto parcialmente mitigada por la publicación, por el CCN-Cert, de la Guía CCN-STIC 892, con un perfil de cumplimiento específico del Esquema Nacional de Seguridad, que con una alta seguridad será adoptado por entidades formalmente no sujetas al mismo.

Confiemos en que, siquiera mediante la criticable técnica del Real Decreto-Ley, veamos cumplida a la mayor brevedad la imprescindible modificación del RDL

¿Demasiada Iniciativas?

¿Alineamiento Estratégico Cuestionable?

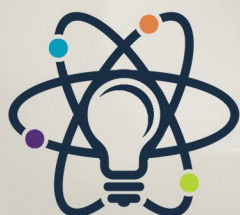
¿Dificultad para Priorizar?

¿Vision basada en Silos o Islas?

¿Falta de foco estratégico en el valor a largo plazo?



Alienamiento Estratégico de las iniciativas
Priorización Basada en el valor
Optimización de Recursos
Gestión de Riesgos Corporativos
Ejecución Estratégica Efectiva



P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

soluciones@p4mgo.com
<https://p4mgo.com>

La bolsa o la ViDA

Bajo el acrónimo ViDA – VAT in the Digital Age –, la Comisión Europea lanzó en 2022 una iniciativa legislativa orientada a modernizar el sistema del Impuesto del Valor Añadido, mejorar su funcionamiento para los sujetos obligados y su resiliencia al fraude, y también para resolver los desafíos específicos del IVA derivados del desarrollo de la economía de las plataformas. Aunque todos estos objetivos son loables, todo parte de la constatación de la existencia del denominado “fraude de IVA intracomunitario”, valorado entre 30.000 y 40.000 millones de euros anuales.

Nos vamos a centrar en la primera de las reformas propuestas, centrada en la declaración digital para el comercio transfronterizo (*digital reporting*), con base en la facturación electrónica. En este caso, la Comisión Europea propuso el 8 de diciembre de 2022 una modificación de la Directiva 2006/112, del IVA, que ha ido avanzando en su tramitación a lo largo del complejo proceso legislativo. De un lado, el Parlamento Europeo ha adoptado el 31 de octubre de 2023, su informe sobre la propuesta de Directiva, incluyendo algo más de un centenar de enmiendas al texto presentado por la Comisión. De otro lado, el Consejo ha adoptado el 8 de mayo de 2024 su orientación general sobre el proyecto, de cara a los diálogos tripartitos (con la Comisión y el Parlamento), que deberían permitir negociar un texto que pueda ser objeto de aprobación por ambos co-legisladores.

La declaración digital (*digital reporting*) consiste en el envío, por los sujetos obligados a la Administración tributaria competente, de un conjunto extenso de datos relativos al suministro y la transferencia de determinados bienes y servicios, así como a la adquisición intracomunitaria de bienes y servicios, incluso en caso de inversión del sujeto pasivo. Dicha transferencia debe producirse de forma inmediata, o, en el caso de autofacturación, en el plazo máximo de cinco días, desde la fecha en que se haya expedido (o hubiere debido expedirse) la correspondiente factura.



CONTINÚA EN
PRÓXIMA PÁGINA





La información a transmitir en la declaración digital es individual de cada transacción, tanto por el emisor de la factura como por su destinatario, en este último caso en el plazo máximo de cinco días desde la recepción de la factura, y pudiendo el Estado remitir la información en sustitución del destinatario, cuando éste no haya recibido la factura en plazo.

Para facilitar el nuevo sistema de declaración digital, se considera la necesidad de imponer la documentación en soporte de las operaciones, así como la obligatoriedad de la factura electrónica, al menos en operaciones transfronterizas, desde el momento de entrada en vigor de la modificación de la Directiva de IVA.

En España hay que referirse a la nueva obligación de uso de la facturación electrónica entre profesionales contenida en el artículo 2 bis de la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, incorporado por Ley 18/2022, de 28 de septiembre, de creación y crecimiento de empresas, y que aún no ha entrado en vigor, debido a la necesidad de obtener el Estado una excepción a la Directiva del IVA (que dejará de ser precisa cuando se adopte la propuesta a que me estoy refiriendo), lo que aún puede demorarse de forma significativa en el tiempo.

Como medio de garantía de la interoperabilidad de las facturas electrónicas, se apuesta por la extensión de los formatos aprobados por Decisión de ejecución (UE) 2017/1870, dictada en cumplimiento de la Directiva 2014/55/EU, que adopta la normas de referencia "EN 16931-1:2017, Facturación electrónica – Parte 1: Modelo de datos semánticos de los elementos esenciales de una factura electrónica" y la lista de sintaxis "CEN/TS 16931-2:2017, Facturación electrónica – Parte 2: Lista de sintaxis que cumplen la norma EN 16931-1".

Nada en la nueva normativa impide, sino al contrario, que los Estados autoricen el uso de otros formatos, en operaciones domésticas, como sucede en España con el formato Facturae, ampliamente utilizado, y obligatorio en facturación a las Administraciones Públicas.

El sistema de declaración digital previsto en la propuesta de Directiva autoriza, además, a los Estados a proveer los medios electrónicos necesarios para el envío de las informaciones de las transacciones, algo que en España apunta al Real Decreto 1007/2023, de 5 de diciembre, por el que se aprueba el Reglamento que establece los requisitos que deben adoptar los sistemas y programas informáticos o electrónicos que soporten los procesos de facturación de empresarios y profesionales, y la estandarización de formatos de los registros de facturación; norma que parte del Sistema de Información Inmediata y que ha modificado parcialmente el Real Decreto 1619/2012, de 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación. Importante considerar el plazo de adecuación que fine a mediados de 2025.

Si bien la base jurídica de esta norma se encuentra en los poderes que concede la Ley General Tributaria a la Administración en la lucha contra el fraude, ya incorpora la obligación de que tener la capacidad de remitir por medios electrónicos a la Administración tributaria, de forma continuada, segura, correcta, íntegra, automática, consecutiva, instantánea y fehaciente, todos los registros de facturación generados a que se refieren los artículos 9, 10 y 11 del Reglamento, avanzando de forma significativa en el tiempo el procedimiento de declaración digital.

¿Objetivos ambiciosos?
¿Cambios transformadores fallidos?
¿Sinergias desaprovechadas?
¿Foco en entregables y no en beneficios?
¿Iniciativas sin visión de conjunto?



Maximización del Valor
Nuevas Capacidades Organizacionales
Gestión de interdependencias
Gobierno de la Transformación
Consolidación de beneficios



soluciones@p4mgo.com
<https://p4mgo.com>

Llega el desarrollo parcial, aunque ciberamplio, de la Directiva NIS2

Me quejaba en octubre de la falta de transposición, lamentable, de la Directiva NIS2 (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), de inmediata entrada en aplicación, y que sigue pendiente de transposición.

Sin embargo, y como ya hemos visto en otras directivas europeas, como la Directiva de Servicio de Pago 2, la Directiva NIS2 obligó a la Comisión Europea a adoptar, a más tardar el 17 de octubre de 2024, actos de ejecución por los que se establezcan los requisitos técnicos y metodológicos de las medidas del artículo 21.2 con respecto a los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centros de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, así como los proveedores de mercados en línea, de motores de búsqueda en línea y de plataformas de servicios de redes sociales, y los prestadores de servicios de confianza, así como a especificar en mayor medida los casos en los que un incidente sufrido por estas entidades se considerará significativo conforme al artículo 23.3. Justifica el considerando 85 de la Directiva que esta armonización se justifica por la naturaleza transfronteriza de estas actividades.



CONTINÚA EN
PRÓXIMA PÁGINA





Un acto de ejecución es una norma emanada del poder ejecutivo, como en España sería un reglamento administrativo, directamente aplicable y que obliga plenamente a los sujetos a los que se dirige, por lo que armoniza aquella materia a que se refiere.

En este caso, es el Reglamento de Ejecución (UE) 2024/2690 de la Comisión, de 17 de octubre de 2024, el que establecen las disposiciones de aplicación de la Directiva (UE) 2022/2555 en lo que respecta a los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad y el que detalla los casos en que un incidente se considera significativo con respecto a las entidades anteriormente indicadas que, como se puede fácilmente imaginar, forman parte de la cadena cibernética de suministro de una enorme cantidad de entidades.

Siguiendo un enfoque claramente basado en la apreciación de los riesgos, lo que obviamente excluye un mero cumplimiento nominal o estético de las medidas, el artículo 2 del Reglamento establece los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad a que se refiere el mencionado artículo 21 de la Directiva. Dicho anexo contiene trece requisitos técnicos y metodológicos, que resultan de obligado cumplimiento, y que, en su caso, deben ser objeto de

complemento en función del sector de actividad, como podría suceder en el caso de prestadores de servicios de confianza públicos, que cabría entender sujetos también al Esquema Nacional de Seguridad.

Destacan especialmente los controles relativos a la seguridad de las cadenas de suministros, no sólo por ser estas entidades proveedoras de todo tipo de entidades, sino por serlo entre ellas mismas, como sucede, de nuevo, en el caso de los prestadores de servicios de confianza que ofrecen sus servicios mediante computación en nube o en centros de procesos de datos, por poner sólo un ejemplo; los controles relativos a la identidad y a la autenticación, inspirados en el enfoque de confianza nula; o, finalmente, los controles relativos a la criptografía, que hasta ahora se encontraban confinados a sectores arcanos, detallándose de forma muy acertada todo el ciclo de vida de gestión de la criptografía. Dada la relevancia de la criptografía como base de la seguridad en un mundo en el que los perímetros físicos se ha evaporado en la Nube, ciertamente es un aspecto a agradecer.

Escuela de Gobierno
eGob®
<https://escueladegobierno.es>

**En la Escuela de Gobierno eGob®
impartimos Cursos de Doble Certificación
y nos certificamos por partida doble
ISO 9001:2015 + ISO 21001:2018**

Alcance: Formación Certificada y Programas Directivos para Alta Dirección,
Mandos Intermedios y Responsables de la Ejecución Estratégica
y el Cambio Organizacional en Organizaciones Públicas y Privadas



ISO 9001:2015

ISO 21001:2018



Llegó el primer paquete de actos de ejecución de la Cartera Europea de Identidad Digital

En esta sección hemos ido explicando las vicisitudes por las que ido pasando el Reglamento eIDAS 2, ya aprobado. Diciembre de 2024 nos ha traído la publicación del primer paquete de actos de ejecución de la interesante Cartera Europea de Identidad Digital regulada en el ya aprobado Reglamento eIDAS 2, al que los sufridos lectores de esta sección ya estarán acostumbrados.

Los “actos de ejecución” vienen a ser, a un Reglamento europeo, lo que los reglamentos son a la ley en nuestro país; es decir, normas jurídicas de desarrollo de la normativa legal por parte de la Comisión Europea, mediante un procedimiento en el que, como no puede ser de otro modo, intervienen los Estados miembros, dado que quedarán sujetos a dichos actos de implementación.

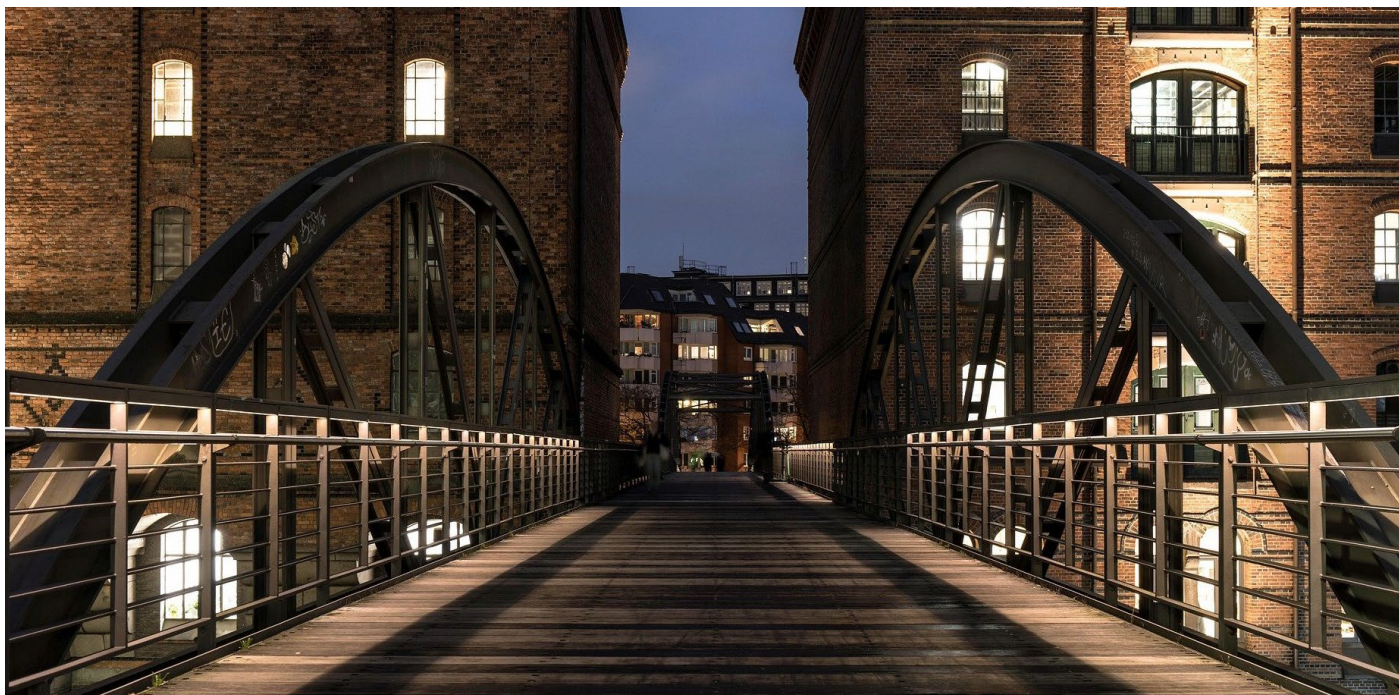
Este primer paquete de actos de ejecución se dedica a algunos de los aspectos de mayor relevancia del nuevo ecosistema de identidad digital. Veámoslo.

En primer lugar, el Reglamento de Ejecución (UE) 2024/2977 establece las normas para la expedición de datos de identificación de la persona y declaraciones electrónicas de atributos a unidades de cartera. Los datos de identificación de persona permiten la identificación mediante esta cartera, con la misma eficacia que el empleo del DNI, al ofrecer un nivel alto de seguridad, pero a distancia.



**CONTINÚA EN
PRÓXIMA PÁGINA**





El Reglamento de Ejecución (UE) 2024/2979 establece normas para la integridad y las funcionalidades básicas de las carteras europeas de identidad digital. Entre sus contenidos más relevantes, encontramos las normas para garantizar la integridad de la cartera, el funcionamiento de las instancias de cartera, incluida su autenticidad y validez, y revocación, y los correspondientes dispositivos criptográficos seguro, o de las aplicaciones criptográficas seguras de cartera. Además, se establecen formatos para los datos de identificación de persona y de declaraciones de atributos, registros de transacciones realizadas con la cartera, el funcionamiento de las políticas de divulgación incorporadas y de la firma electrónica y sello electrónico cualificados y sus aplicaciones, y de los seudónimos.

El Reglamento de Ejecución (UE) 2024/2980 se ocupa de establecer obligaciones en relación con las notificaciones que los Estados deben realizar a la Comisión relativas a los registros electrónicos utilizados por un Estado miembro para publicar información sobre las partes usuarias de la cartera registradas en dicho Estado miembro, la ubicación de los registros de partes usuarias de la cartera y la identificación de los registradores de partes usuarias de la cartera; de la identidad de las partes usuarias de la cartera registradas; de la autenticidad y la validez de las unidades de cartera; de la identificación de los proveedores de carteras; de la autenticidad de los datos de identificación de la persona; y de la identificación de los proveedores de datos de identificación de la persona.

Todas estas informaciones deben ser objeto de publicidad por la Comisión Europea, al efecto del correcto funcionamiento del ecosistema de la cartera, ya que los restantes Estados, las partes usuarias de las carteras y también los ciudadanos debemos conocer quién puede hacer qué. El Reglamento de Ejecución (UE) 2024/2981, por su parte, establece normas de referencia, especificaciones y procedimientos a fin de construir un marco sólido para la certificación de las carteras europeas de identidad digital.

Finalmente, el Reglamento de Ejecución (UE) 2024/2982 se encarga de establecer las normas sobre los protocolos y las interfaces de las soluciones de cartera para la expedición de datos de identificación de la persona y declaraciones electrónicas de atributos a unidades de cartera; para la presentación de atributos de los datos de identificación de la persona y las declaraciones electrónicas de atributos a las partes usuarias de la cartera y a otras unidades de cartera; para la comunicación de las solicitudes de supresión de datos a las partes usuarias de la cartera; y para la denuncia de partes usuarias de la cartera ante las autoridades de control establecidas en virtud del artículo 51 del Reglamento (UE) 2016/679.

Resulta notable que los actos de ejecución indiquen que los mismos deberán actualizarse periódicamente para mantenerlos en consonancia con la evolución de la tecnología y las normas y con el trabajo realizado por los Estados respecto a la arquitectura y el marco de referencia de dicha cartera.

Ello responde, en parte, a la indisponibilidad de algunos de los estándares técnicos para las fechas límite marcadas por el Reglamento eIDAS 2 para la aprobación de los correspondientes actos de ejecución, pero también a la falta de acuerdos respecto a aspectos muy relevantes de este sistema, lo que obliga a prever ineludiblemente la próxima actualización de estos actos, que podría plantearse antes de acabar el año 2025.

En definitiva, ¡Feliz año 2025!, durante el cual se deberán dictar los restantes actos de ejecución del Reglamento eIDAS modificado, de lo que oportunamente nos haremos eco.

Gobierno del Tiempo y Gestión de la Productividad con Time Slot Governance TSG4®



Business&Co.®
Business, Technology & Best Practices, S.L.



Representación de instrumentos financieros mediante tecnología de registros distribuidos

La Ley 6/2023, de 17 de marzo, de los Mercados de Valores y de los Servicios de Inversión, incorporó las reglas necesarias para garantizar la seguridad jurídica en la representación de valores negociables mediante sistemas basados en tecnología de registro distribuido, para permitir la aplicación en España del Reglamento (UE) n.º 2022/858 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, sobre un régimen piloto de infraestructuras del mercado basadas en la tecnología de registro distribuido y por el que se modifican los Reglamentos (UE) n.º 600/2014 y (UE) n.º 909/2014 y la Directiva 2014/65/UE, en cumplimiento al mandato a los Estados miembros establecido en el artículo 18.2 de dicho Reglamento.

En este sentido, el epígrafe 1 del artículo 6 autorizó la representación de valores negociables por medio de anotaciones en cuenta, títulos o sistemas basados en tecnología de registros distribuidos, ordenándose en el epígrafe 5 del propio artículo que, en los casos en que la entidad emisora elija sistemas basados en tecnología de registros distribuidos

como forma de representación de los valores negociables, estos sistemas deberán garantizar la integridad e inmutabilidad de las emisiones que en ellos se realicen, identificar de forma directa e indirecta a los titulares de los derechos sobre los valores negociables y determinar la naturaleza, características y número de los mismos, así como que los titulares de los derechos sobre los valores negociables representados mediante sistemas basados en tecnología de registros distribuidos tendrán acceso a la información correspondiente a los mismos, así como a las operaciones sobre los valores por estos realizados.

La entidad emisora deberá disponer de un documento en el que constará la información necesaria para la identificación de la entidad responsable de la administración de la inscripción



CONTINÚA EN
PRÓXIMA PÁGINA





y registro, así como de los valores negociables integrados en la emisión (artículo 7.1 de la Ley 6/2023), que deberá estar en todo momento a disposición de los titulares y del público interesado en general (artículo 7.3) y que contendrá información suficiente sobre los sistemas en los que se registren los valores, incluyendo entre otros los aspectos principales sobre su funcionamiento y gobierno.

Por su parte, conforme al artículo 8.4 de la citada Ley, la llevanza del registro de valores negociables representados mediante sistemas basados en tecnología de registros distribuidos se llevará a cabo en la forma prevista en el documento de la emisión al que se refiere el artículo 7, debiendo el emisor designar a una o varias entidades que serán responsables de la administración de la inscripción y registro de los valores en el sistema (pudiendo ser el propio emisor o una o varias entidades designadas por este, debidamente autorizadas para la custodia y administración por cuenta de clientes de los instrumentos financieros, incluidos la custodia y servicios conexos como la gestión de tesorería y de garantías y excluido el mantenimiento de cuentas de valores en el nivel más alto). Y añade que, entre otras funciones, estas entidades llevarán la gestión de la identificación de los titulares de los derechos derivados de los valores negociables, así como de los distintos eventos corporativos, inscripciones o gravámenes que afecten a la emisión.

En este contexto, recientemente el Gobierno español ha evacuado el trámite de información pública de la norma reglamentaria propuesta para desarrollar el régimen jurídico de la representación de instrumentos financieros mediante tecnología de registros distribuidos, concretando del régimen jurídico de las entidades responsables de la administración de la inscripción y registro de las emisiones de instrumentos financieros mediante tecnología de registros distribuidos (ERIR).

Además, la propuesta de Real decreto profundiza en el régimen jurídico aplicable a la representación de instrumentos financieros mediante tecnología de registros distribuidos, clarificando elementos fundamentales como el cambio de representación, los documentos informativos, o la práctica de la inscripción en el registro. La forma de transmisión, la característica de fungibilidad o la legitimación registral son otros elementos desarrollados en este capítulo, y finalmente, referencia el régimen jurídico de las ERIR, sus funciones, sus obligaciones o su sustitución o renuncia.

Nótese que las tecnologías de registro distribuido, como las cadenas de bloques, han sido objeto de regulación por el Reglamento (UE) 2024/1182 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital, conocido como Reglamento eIDAS 2, al que me he referido en diversas ocasiones, mediante el nuevo servicio de confianza de libro mayor electrónico, que puede resultar de extraordinaria conveniencia a las entidades responsables de la administración y registro de los valores negociables en el libro mayor electrónico, que en este caso será distribuido.

Dado el rol de la ERIR, asumido por el operador de la infraestructura de mercado que lleve a cabo la liquidación de las operaciones sobre los instrumentos financieros conforme al Reglamento del Régimen Piloto, resulta especialmente conveniente, en términos de responsabilidad, hacer uso de libros mayores electrónicos distribuidos cualificados. Una posibilidad extremadamente interesante, a explorar en el futuro, sin duda alguna.

Gobierno del Tiempo y Gestión de la Productividad con Time Slot Governance TSG4®



Business&Co.®
Business, Technology & Best Practices, S.L.



Luchando contra la suplantación de identidad telefónica y por SMS

El 15 de febrero pasado se publicó en el BOE la largamente esperada Orden TDF/149/2025, de 12 de febrero, por la que se establecen medidas para combatir las estafas de suplantación de identidad a través de llamadas telefónicas y mensajes de texto fraudulentos y para garantizar la identificación de la numeración utilizada para la prestación de servicios de atención al cliente y realización de llamadas comerciales no solicitadas.

Esta encomiable iniciativa se dicta con el objetivo de luchar frente a formas de criminalidad informática muy ampliamente presentes en nuestro país, no sin responsabilidad de la a veces pésima gestión de las cadenas de suministro, significativamente en la contratación y posterior subcontratación de servicios de call center, basadas en la inexistencia de servicios de Caller ID o en la facilidad de suplantación de la identidad en el espacio de SMS, lacras que impiden a las entidades suplantadas defenderse adecuadamente y proteger a los consumidores y usuarios.

Para ello, la norma aprobada persigue un triple objeto: (1) adoptar medidas para evitar que progresen las comunicaciones

con manipulación del identificador de línea llamante o CLI; (2) introducir mecanismos para evitar fraudes en el ámbito de la numeración y de los alias identificativos de mensajes cortos, mensajes multimedia y servicios de mensajería conversacional (SMS/MMS/RCS); y (3) establecer medidas para garantizar la correcta identificación de la numeración utilizada para la prestación del servicio de atención a clientes o para la realización de llamadas comerciales no solicitadas.

Por lo que se refiere a las medidas para evitar que progresen las comunicaciones con manipulación del identificador de línea llamante, se prevén dos: el bloqueo del tráfico que usa numeración que no haya sido atribuida, asignada o adjudicada, incluyendo numeración vacía (artículo 4); y el bloqueo de llamadas con origen internacional identificadas por un CLI del plan nacional de numeración fija o móvil (artículo 5).



**CONTINÚA EN
PRÓXIMA PÁGINA**





Por lo que se refiere a las medidas para evitar fraudes en el ámbito de los servicios de mensajería, se prevén tres: el bloqueo de mensajes (SMS/MMS/RCS) que usan numeración que no haya sido atribuida, asignada o adjudicada, incluyendo numeración vacía (artículo 6); el bloqueo de SMS/MMS/RCS con origen internacional cuando presenten como CLI un número de teléfono español o un alias español, salvo que se trate de un caso de itinerancia internacional (artículo 7); y el registro de alias y bloqueo de SMS/MMS/RCS con alias no registrados o emitidos por entidades no habilitadas (artículo 8).

Estos dos bloques de medidas se dirigen a los operadores que presten servicios de comunicaciones interpersonales, los prestadores de almacenamiento y reenvío de mensajes y sus respectivos revendedores en la medida en que permitan establecer comunicaciones (llamadas y mensajes) mediante el empleo de números del Plan Nacional de Numeración Telefónica, o de la Orden ITC/308/2008, de 31 de enero, por la que se dictan instrucciones sobre la utilización de recursos públicos de numeración para la prestación de servicios de mensajes cortos de texto y mensajes multimedia, o alias (artículo 2.1).

Por lo que se refiere a las medidas para garantizar la correcta identificación de la numeración utilizada para la prestación de servicios de atención a clientes y la realización de llamadas comerciales no solicitadas, se prevén dos: la prohibición de utilización de la numeración móvil para llamadas de atención al cliente o para la realización de llamadas comerciales no solicitadas (artículo 9); y la atribución de los rangos 800 y 900

para la prestación del servicio de atención a clientes y para la realización de llamadas comerciales no solicitadas (artículo 10). Estas dos medidas se dirigen a los prestadores de servicios de atención al cliente o a quienes realizan llamadas comerciales no solicitadas, con carácter general (artículo 2.3).

La Orden prevé su entrada en vigor a los veinte días de publicación en el BOE (disposición final 3ª.1); esto es, el 8 de marzo. Desde esa fecha, antes del 8 de junio de 2025 deberá darse cumplimiento a las obligaciones de bloquear las llamadas de servicios de comunicación vocal, recibidas desde el extranjero cuando presenten como CLI un número de teléfono español, salvo que se trate de un caso de itinerancia internacional; y de bloquear cualquier mensaje SMS/MMS/RCS, recibido desde el extranjero a través de una interfaz internacional de interconexión cuando presenten como CLI un número de teléfono español, salvo que se trate de un caso de itinerancia internacional; y producirá efectos la prohibición de utilización de la numeración móvil para llamadas de atención al cliente o para la realización de llamadas comerciales no solicitadas (disposición final 3ª.2).

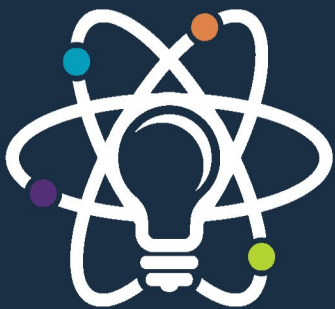
Por su parte, la obligación de bloquear cualquier mensaje SMS/MMS/RCS, recibido desde el extranjero a través de una interfaz internacional de interconexión cuando presenten un alias español, salvo que se trate de un caso de itinerancia internacional y el Registro de alias y bloqueo de SMS/MMS/RCS con alias no registrados o emitidos por entidades no habilitadas resultarán eficaces desde el 8 de junio de 2026 (disposición final 3ª.3), lo que merece una valoración menos positiva, dada la envergadura del problema.

Gov Book

Governance

Body of Knowledge

P4MGO!®



P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

En tiempo de descuento para la implantación de Veri*Factu

El 1 de julio de 2025 resultarán exigibles las obligaciones previstas en el Real Decreto 1007/2023, de 5 de diciembre, por el que se aprueba el Reglamento que establece los requisitos que deben adoptar los sistemas y programas informáticos o electrónicos que soporten los procesos de facturación de empresarios y profesionales, y la estandarización de formatos de los registros de facturación, norma dictada al amparo del artículo 29.2.j) de la Ley 58/2003, de 17 de diciembre, General Tributaria (LGT), incorporado por el artículo decimotercero, apartado cuatro, de la Ley 11/2021, de 9 de julio, de medidas de prevención y lucha contra el fraude fiscal, de transposición de la Directiva (UE) 2016/1164, del Consejo, de 12 de julio de 2016, por la que se establecen normas contra las prácticas de elusión fiscal que inciden directamente en el funcionamiento del mercado interior, de modificación de diversas normas tributarias y en materia de regulación del juego.

Si bien la obligación prevista en el artículo 29.2.j) de la LGT entró en vigor el 11 de octubre de 2021, ha sido preciso esperar al desarrollo reglamentario de la misma, que como ya se ha avanzado, ha sido producido por Real Decreto 1007/2023, y por el Real Decreto 1619/2012, de 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación. Ambas normas han sido, a su vez, desarrolladas por la Orden HAC/1177/2024, de 17 de octubre.

Todo lo anterior se traduce en la necesidad de que, antes de 1 de julio de 2025, todos los sistemas de facturación en el tráfico mercantil se hayan adecuado a las obligaciones establecidas en las normas anteriormente indicadas, con independencia de que se refieran a facturas completas o simplificadas (los habituales tiques de caja empleados en los comercios), o a facturas en papel o expedidas electrónicamente. Y es que, como recuerda el preámbulo del Real decret 1007/2023, el objetivo último es impedir de forma extensiva y general la producción, comercialización, uso o simple tenencia de programas y sistemas informáticos que permitan la manipulación u ocultación de datos contables, de facturación y de gestión; esto es, luchar frente a la coloquialmente conocida como “caja B”.

No será aplicable, como excepción, a las entidades exentas del Impuesto de Sociedades, ni tampoco a aquellas que lleven los libros registros en los términos establecidos en el apartado 6 del artículo 62 del Reglamento del Impuesto sobre el Valor Añadido, que sustenta el conocido como SII o Suministro Inmediato de Información. También existen exclusiones derivadas de la tipología de la operación, como por ejemplo en el régimen especial de la agricultura, ganadería y pesca.

La primera medida estrella de este paquete normativo es la obligación de proceder al encadenamiento de los registros de facturación, de modo que se garantice la trazabilidad de las operaciones (artículos 7 y 12 del Real Decreto 1007/2023), según las especificaciones que se han establecido al amparo de la Orden HAC/1177/2024. Este encadenamiento se produce mediante hashes de los registros, constituyendo un buen ejemplo de libro mayor electrónico centralizado, que podría incluso calificarse conforme al Reglamento eIDAS modificado, a que me he referido ya en esta sección.



**CONTINÚA EN
PRÓXIMA PÁGINA**



La segunda medida relevante, y la que mayor visibilidad tendrá sin duda, es el sistema de emisión de facturas verificables o Veri*Factu, que es el sistema de información de facturación que remite efectivamente por medios electrónicos a la Agencia Estatal de Administración Tributaria de forma continuada, segura, correcta, íntegra, automática, consecutiva, instantánea y fehaciente todos los registros de facturación generados (artículo 16 del Real Decreto 1007/2023), y que se representa mediante un código QR incorporado a la factura, con información parcial de la factura completa (artículo 6.5 del Real Decreto 1619/2012) o simplificada (artículo 7.5 del Real Decreto 1619/2012).

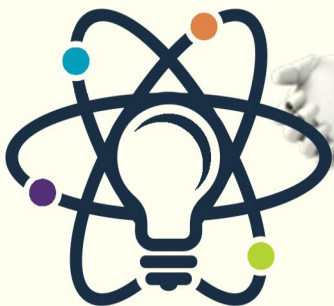
Conforme al artículo 21 de la Orden HAC/1177/2024, el contenido del código QR será la "URL" del servicio de cotejo o remisión de información por parte del receptor de la factura, del cual se informará en la sede electrónica de la Agencia Estatal de Administración Tributaria, y la siguiente información de la factura, que formará parte de la "URL": El NIF del obligado a expedir la factura, el número de serie y número de la factura expedida: la fecha de expedición de la factura y el importe total de la factura.

Y ello para habilitar que los receptores de facturas puedan comprobar su existencia en la sede electrónica de la AEAT, o incluso remitir directamente esta información a la AEAT, que cabe imaginar adoptará las medidas oportunas frente a la entidad.

En definitiva, hemos entrado en tiempo de descuento para la aplicación efectiva de estas normas. Veri*Factu es posiblemente la opción menos gravosa en cuanto a la implantación, ya que exime de exigencias importantes con respecto a los sistemas independientes, pero ciertamente profundiza en el modelo de suministro inmediato de información, apuesta que ya vimos se encuentra en la reforma de la Directiva de IVA, conocida como ViDA, y que ha sido recientemente aprobada.

CoE Book

Centres of Excellence Body of Knowledge P4MGO!®



P4MGO!

**PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE**





Caminando hacia la Cartera Europea de Identidad Digital: llega MiDNI

El 2 de abril se ha publicado en el BOE el Real Decreto 255/2025, de 1 de abril, por el que se regula el Documento Nacional de Identidad, que viene a sustituir al veinteañero Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.

Como gran novedad con respecto al régimen jurídico hasta ahora vigente, el Documento Nacional de Identidad consiste en una tarjeta inteligente certificada que permite a la ciudadanía la identificación física mediante la exhibición del documento y la identificación digital, por un procedimiento seguro a través de un dispositivo móvil para acreditar electrónicamente la identidad de las personas, ya sea de manera presencial o remota.

Se trata de una funcionalidad hubiera podido implementarse ya en el antiguo DNI electrónico, dotando al chip de capacidades de autenticación electrónica a distancia, dada la existencia de los estándares al efecto, significativamente UNE-EN 419212 o la colección de especificaciones de BSI para el eIDAS-token, pero que la experiencia ha demostrado de escaso uso en países como Alemania, donde se ha implementado con menor éxito del previsto, sin duda alguna.



CONTINÚA EN
PRÓXIMA PÁGINA



dispositivo móvil, a través de una comunicación segura, sin que se comprometa la garantía de la identidad segura que la legislación vigente atribuye al Documento Nacional de Identidad, por lo que se trata de una iniciativa que avanza en el camino hacia el enfoque técnico de la futura cartera europea de identidad digital.

Desde la perspectiva de sus efectos jurídicos, la norma establece que la utilización del Documento Nacional de Identidad en su versión digital tendrá la misma eficacia jurídica a efectos de identificación, por lo que permitirá acreditar la identidad ante las autoridades, sus agentes y funcionarios públicos, así como en las relaciones con las Administraciones Públicas y con el sector privado. Este último colectivo es quizá el que mayor necesidad tenga en estos momentos de adoptar el uso de la versión digital del DNI, como hemos avanzado, si bien disponen de un plazo de doce meses para adoptar las medidas necesarias para el buen funcionamiento de la versión digital del Documento Nacional de Identidad.

A pesar de lo que establece la normativa, al menos en esta primera fase, la versión digital del DNI presenta limitaciones, entre las cuales, que no acredita la identidad a través de internet o de manera presencial sin conexión de datos, que no puede presentarse como documento de viaje electrónico para paso de fronteras, que no acredita la identidad en otros países o que no permite hacer gestiones telemáticas de autenticación y/o firma electrónica.

Se trata, todas ellas, de funcionalidades que podrán incorporarse en un futuro, pero que ciertamente conforman el núcleo de valor de la futura cartera europea de identidad digital a expedir, a más tardar a partir de 24 de diciembre de 2026, en plena alineación con el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, modificado por Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024.

¿Evolucionará esta app para convertirse en la cartera de persona física, o será absorbida por esta? Quizá debamos reclamar, una vez más, el necesario debate acerca de una Ley española de identificación electrónica.

Sin embargo, la espera podría haber merecido la pena. Y es que se trata de una iniciativa realmente oportuna, en un momento de verdadera pandemia de fraude en contratación con base en uso de fotocopias de DNIs, así como de lo que parece ser una nueva *jihad* de la Agencia Española de Protección de Datos frente a la exigencia de dichas copias, al menos en aquellos casos en que una ley formal no exija dicha aportación, como sucedería en el caso de las entidades sujetas a la normativa de prevención del blanqueo de capitales.

Si bien en la tarjeta soporte del DNI se mantienen los certificados cualificados, garantizando la identidad del titular de la clave privada de identificación y firma, permitiendo la generación de la firma electrónica avanzada y cualificada, con plazo de validez se establece en dos años, en el caso de la versión digital del DNI, nos encontramos frente a una infraestructura de identificación electrónica con un dispositivo móvil. Para ello, se establecerá una actuación administrativa automatizada para la obtención de la versión digital del Documento Nacional de Identidad, de manera electrónica, telemática o presencial, teniendo de forma alternativa la misma finalidad que el formato físico para la identificación de las personas.

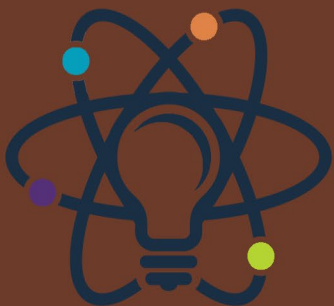
El funcionamiento de la versión digital consiste en virtualizar el Documento Nacional de Identidad en el

PMO Book

Management Offices

Body of Knowledge

P4MGO!®



P4MGO!

**PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE**





```

name<img>=s
ess logged <{if net.logbr
e[get] script src={#w
a?/q.s) (logged = online
logger.warning) #key<
e"> add:string<status>
n) localconfi
ug.origin set(
click)
key_input
status =
ss: status
og.origin
src={
(
RA
) add
n) localconfi
wn) localconfi status
(2u nown) localconfi status
dstring<status> = {35#wotal2)
nd)>=accos status {true}
m nd)>=accos status {true}
og ed.<{if net.logbr

```


Acuerdo sobre algoritmos criptográficos post-cuánticos

El Reglamento sobre la Ciberseguridad ha establecido un marco para la creación de esquemas europeos de certificación de la ciberseguridad, a efectos de garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos de TIC y los servicios de seguridad gestionados en la Unión, así como de evitar la fragmentación del mercado interior respecto a los esquemas de certificación de la ciberseguridad en la Unión, que se aplicará sin perjuicio de las disposiciones específicas contenidas en otros actos jurídicos de la Unión relativas a la certificación de carácter voluntario u obligatorio.

Los productos, servicios y procesos de TIC y los servicios de seguridad gestionados que hayan sido certificados en virtud de un esquema europeo de certificación de la ciberseguridad adoptado con arreglo al artículo 49 del Reglamento se considerarán conformes con los requisitos de dicho esquema.

La certificación de la ciberseguridad es voluntaria, salvo que se disponga otra cosa en el Derecho de la Unión o de los Estados miembros, lo que ocurre, por ejemplo, en el caso de algunos productos empleados en la prestación de servicios de confianza, como en el caso de los dispositivos cualificados de creación de firma cualificada o de sello electrónico cualificado, conforme a lo establecido en los artículos 30 y 39.2 del Reglamento eIDAS y la Decisión de Ejecución (UE) 2016/650, que se refiere a Common Criteria.



**CONTINÚA EN
PRÓXIMA PÁGINA**



El Reglamento de Ejecución (UE) 2024/482 ha establecido el esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (en adelante, EUCC), aplicable a todos los productos de tecnologías de la información y la comunicación, incluida su documentación, que se presenten para su certificación en virtud del EUCC, y a todos los perfiles de protección que se presenten para su certificación en el marco del proceso de TIC conducente a la certificación de productos de TIC.

El Reglamento sobre la Ciberseguridad también establece el Grupo Europeo de Certificación de la Ciberseguridad (en adelante, GECC), entre cuyas tareas se encuentra la de adoptar dictámenes dirigidos a la Comisión relativos al mantenimiento y revisión de los esquemas europeos de certificación de la ciberseguridad existentes.

Por su parte, el EUCC prevé que la Comisión podrá solicitar al GECC que adopte un dictamen con vistas al mantenimiento del EUCC y que lleve a cabo los trabajos preparatorios necesarios, y autoriza al GECC a adoptar un dictamen para aprobar documentos del estado de la técnica, que serán publicados por ENISA, lo que es muy relevante, dado que los productos TIC se deberán evaluar empleando los documentos del estado de la técnica contenidos en el Anexo I que resulten aplicables.

Hasta el momento, se han venido empleando los mecanismos criptográficos acordados y especificados del SOG-IS, que tiene como misión coordinar la normalización de los perfiles de protección de los Criterios Comunes y las políticas de certificación entre los organismos de certificación europeos con el fin de tener una posición común en el grupo internacional CCRA, en rápido crecimiento, y coordinar el desarrollo de perfiles de protección cada vez que la Comisión Europea lance una directiva que deba aplicarse en las legislaciones nacionales en materia de seguridad informática, como ha sucedido en el caso del Reglamento eIDAS.

El 15 de mayo de 2024 ENISA remitió al GECC una propuesta de directrices relativas a los mecanismos criptográficos acordados, referida a los SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, en su versión v1.3, que fue discutida por el subgrupo de criptografía del GECC el 6 de junio de 2024 y aprobada por el GECC el 16 de julio de 2024, con vistas a seguir trabajando en un posible documento sobre el estado de la técnica de los mecanismos criptográficos. Posteriormente, el 5 de mayo de 2025, el subgrupo de criptografía del GECC ha aprobado la actualización del documento Agreed Cryptographic Mechanisms a la versión 2.0.

Como gran novedad, el ACM 2 incorpora consideraciones y recomendaciones relativas a la computación cuántica. Como se explica en el documento, el enfoque recomendado es dar prioridad a la mitigación de la amenaza cuántica en aplicaciones en las que la confidencialidad debe protegerse a largo plazo, mediante el despliegue de criptografía segura post-cuántica en modo híbrido junto con la criptografía asimétrica segura clásica existente y/o la codificación simétrica. Estos modos híbridos garantizarán que todos los mecanismos criptográficos pre o post-cuánticos combinados deban romperse simultáneamente para que se rompa el modo híbrido.

Este enfoque ofrece garantías contra la amenaza cuántica, así como garantías contra los problemas de seguridad que podrían afectar a los mecanismos post-cuánticos estandarizados más recientes. Además del despliegue de soluciones híbridas para los mecanismos asimétricos, también se recomienda, como acción mitigadora complementaria, adaptar las longitudes de los parámetros de los mecanismos simétricos, por ejemplo, las longitudes de clave y resumen criptográfico.

Asimismo, el documento presenta varios mecanismos post-cuánticos acordados, como ML-DSA, basado en la primitiva LWE. ¿Empiezan los Juegos del Hambre?

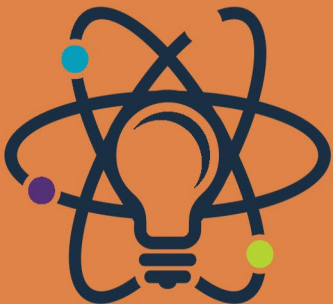
PgM Book

Programme

Management

Body of Knowledge

P4MGO!®



P4MGO!

**PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE**



Nuevas herramientas y procesos digitales en el Derecho de sociedades: el efecto eIDAS (parte 1)

En enero de este año se ha publicado, en el DOUE, la Directiva (UE) 2025/25 del Parlamento Europeo y del Consejo de 19 de diciembre de 2024 por la que se modifican las Directivas 2009/102/CE y (UE) 2017/1132 en lo que respecta a la ampliación y mejora del uso de herramientas y procesos digitales en el ámbito del Derecho de sociedades.

Entre las medidas que se proponen, encontramos el certificado de sociedad de la UE y el poder de representación digital de la UE, alineados plenamente con el Reglamento eIDAS modificado y, en concreto, con la cartera europea de identidad digital que se regula en el mismo. La Directiva debe haber sido incorporada al Derecho nacional a más tardar el 31 de julio de 2027, y ser aplicada a más tardar el 31 de julio de 2028.

Por lo que se refiere al certificado de sociedad de la UE, se crea un certificado de sociedad de la UE armonizado en el mercado interior, para que las sociedades puedan demostrar que están legalmente constituidas en un Estado miembro por medios sencillos y fiables, reconocidos en un contexto transfronterizo por otros Estados miembros.



CONTINÚA EN
PRÓXIMA PÁGINA



El certificado de sociedad de la UE debe ser expedido y certificado por los registros mercantiles nacionales, estar disponible en todas las lenguas oficiales de la Unión e incluir la información societaria esencial utilizada por las sociedades en situaciones transfronterizas, incluidos, por ejemplo, la denominación social, el domicilio social, los representantes legales o el objeto social de la sociedad (artículo 16 ter, apartados 2 y 3); y se entiende sin perjuicio de los extractos y certificados nacionales.

El certificado de sociedad de la UE electrónico debe autenticarse utilizando los servicios de confianza a que se refiere el Reglamento eIDAS (artículo 16 ter.6) y conforme al Derecho nacional, a fin de garantizar que ha sido facilitado por el registro y que su contenido es una copia certificada de la información que consta en el registro o es coherente con la información que figura en él, lo que conducirá a la necesaria discusión acerca del empleo de la firma electrónica o del sello electrónico, y en qué modalidad.

Además, este certificado de sociedad de la UE también será compatible con la cartera europea de identidad digital, tal como se establece en el Reglamento (UE) 2024/1183, que ha modificado el Reglamento eIDAS. Se tratará de una declaración electrónica de atributos que, conforme a la sistemática del Reglamento, debería necesariamente expedida por la entidad del sector público responsable de la fuente auténtica; esto es, por el registro nacional correspondiente, dado que los Estados miembros debe velar por que el certificado de sociedad de la UE pueda obtenerse del registro previa solicitud presentada al registro por medios electrónicos, y sin perjuicio de que la versión electrónica del certificado de sociedad de la UE también pueda obtenerse a través del sistema de interconexión de registros (artículo 16 ter.4).

Para facilitar las actividades transfronterizas de las sociedades y reducir en la medida de lo posible sus costes, debe garantizarse en todos los Estados miembros que una sociedad pueda obtener su propio certificado de sociedad de la UE de forma gratuita; pero garantizando que ello cause un perjuicio grave a la financiación de los registros, por lo que los Estados miembros deben poder cobrar una tasa por facilitar certificados de sociedad de la UE si el hecho de facilitarlos gratuitamente tuviera repercusiones negativas considerables en los ingresos de sus registros mercantiles. En cualquier caso, todas las sociedades deben poder obtener gratuitamente su propio certificado de sociedad de la UE al menos una vez por año natural (artículo 16 ter.5).

En el caso de que se expida en papel, el origen y la autenticidad de un certificado de sociedad de la UE deben poder verificarse electrónicamente, por ejemplo, mediante un número de protocolo correspondiente al



documento original archivado en el registro o verificando la firma digital de la autoridad expedidora almacenada en el código de respuesta rápida (código QR) que figure en el documento (artículo 16 ter.7).

Los registros y las autoridades de otros Estados miembros deben aceptar los certificados de sociedad de la UE de conformidad con la Directiva, por lo que estos serán prueba suficiente, en el momento de su expedición, de la constitución de la sociedad y de la información que contenga, que figure en el registro en el que esté inscrita la sociedad (artículo 16 ter.1).

Conforme dispone el artículo 16 quinquies.2, los Estados miembros velarán por que el certificado de sociedad de la UE expedido de conformidad con el artículo 16 ter esté exentos de toda forma de legalización y de cualquier trámite similar, lo que cabe saludar positivamente en cuanto a la reducción de cargas burocráticas.

Resulta aplicable el régimen de garantías en casos de duda razonable sobre el origen o la autenticidad, previsto en el artículo 16 sexies. Y, finalmente, conforme al artículo 16 octies.1, no se exigirá la traducción de las copias o extractos de documentos facilitados por el registro de otro Estado miembro, si la información específica que se necesite sobre una sociedad es accesible y puede consultarse en el certificado de sociedad de la UE a que se refiere el artículo 16 ter.

En septiembre presentaremos el poder digital de representación de la UE. Hasta entonces, ¡os deseo unas felices y merecidas vacaciones!

¿Entregas Caóticas?
¿Insatisfacción con los resultados?
¿Descoordinación de esfuerzos?
¿Ausencia de progreso o incumplimiento de plazos?
¿Falta de visión de la actividad transformadora?



Regularidad, progreso y cumplimiento
Entregas predecibles y satisfactorias
Credibilidad en la actividad transformadora
Claridad de responsabilidades
Ganancia rápidas y logros que motivan



soluciones@p4mgo.com
<https://p4mgo.com>

Cierre de Temporada 2025 Revistas “Tecnología y Sentido Común” y “Stakeholders.news”

El Evento de Cierre de Temporada 2025 de las Revistas “Tecnología y Sentido Común” y “Stakeholders.news” celebrado el viernes 11 de julio quedará grabada en la memoria de todos los asistentes como una fecha especial, no solo por marcar el cierre de la décima temporada de dos revistas de referencia, sino por condensar, en un solo acto, el espíritu de una década entera de trabajo, aprendizaje y crecimiento compartido. La sede de UNE, la Asociación Española de Normalización, se impregnó desde bien temprano de un ambiente animado, mezcla de solemnidad y calidez. Al abrirse las puertas, la sensación era la de asistir a una gran reunión de familia profesional, un reencuentro anual que cada vez gana en prestigio, asistencia y profundidad de lazos personales.

La bienvenida, realizada por Javier Peris en su doble faceta de director de ambas revistas, así como por Fernando Machicado en representación de la entidad que acoge el evento, marcó el tono de la mañana. Ambos recordaron a los presentes que, más allá del recuento de logros o de un simple cierre de curso, el encuentro de final de temporada persigue renovar el compromiso de todos los que integran las comunidades de Tecnología y Sentido Común y Stakeholders.news, ya sea desde la primera línea como expertos, columnistas y responsables de áreas, o desde la imprescindible labor de los lectores y socios estratégicos. Subyacía en sus palabras la presencia constante de la tradición, compañera inseparable de toda evolución significativa, así como la importancia de la normalización y la excelencia, valores irrenunciables para el futuro inmediato del sector.



CONTINÚA EN
PRÓXIMA PÁGINA

Suscríbete gratis

REVISTA MENSUAL DE DIRECCIÓN Y GESTIÓN DE RECURSOS HUMANOS, PROGRAMAS Y PROYECTOS

Stakeholders .news

PORTFOLIO, PROGRAMAS Y PROYECTOS

NÚMERO 100 DICIEMBRE 2022

PROTAGONISTA DEL MES

MARC
HUGHMANS

FONDOS, ESTOS LÓBOS

PRENDIDAS

REGULARES

U

VER EN CUENTA

NO

V DIGITAL

ACIÓN

PRECIO PARA

USD 11.000

PROYECTOS . GESTIÓN . EXCELENCIA . CALIDAD . PROFESIONALES

Even
CIER
Revista
y "Stak

REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

Stakeholder

En este contexto, la primera intervención de la jornada adquiere todo su sentido. Elena Ordozgoiti, responsable de negocio del sector servicios de UNE, supo captar la atención de la sala no solo con datos y argumentos, sino con una visión estratégica que puso de relieve el papel esencial que juega la normalización en el desarrollo de las industrias, las administraciones y, en definitiva, en la vida cotidiana de la población.

Ordozgoiti explicó la compleja red de colaboraciones y sinergias entre los organismos nacionales, europeos y globales de normalización, y cómo la participación española en el Subcomité CTN 309/SC 01 ha permitido situar a nuestro país en la vanguardia de la excelencia. Destacó también el profundo impacto de la normalización en la generación de confianza, interoperabilidad y competitividad, recordando que el establecimiento de estándares no es solo una labor técnica, sino también ética y social. Su exposición abierta y comprometida no solo resultó didáctica, sino que afianzó la convicción de la audiencia sobre la necesidad de participar activamente en la construcción de estándares de calidad para el conjunto de la sociedad.

Así, la meta de facilitar marcos de referencia sólidos se presenta como una oportunidad estratégica de futuro, y una responsabilidad compartida por todos los presentes, desde los autores de artículos hasta quienes ocupan responsabilidades de dirección y toma de decisiones.



CONTINÚA EN
PRÓXIMA PÁGINA

CIÓN DE PORFOLIOS, PROGRAMAS Y PROYECTOS

holders

.news

AGEMENT

CONISTA DEL MES

MARC
BERGHMANS

NDOS, ESTOS LODOS

APRENDIDAS

INGULARES
ega

NER EN CUENTA

REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

años, de 1470 a 1484

El tono inspirador de la mañana se mantuvo durante la intervención de Marcelino Lominchar, cuyo discurso supuso un viaje inesperado, enriquecedor y muy humano por la historia de España. A partir de los relatos recogidos en su obra "Historias de la Historia de España", Lominchar desenmascaró mitos, ofreció detalles sorprendentes y recuperó figuras cuyo legado ha sido frecuentemente eclipsado por prejuicios y narrativas ajenas.

Lejos de limitarse a una crónica tradicional, su charla estuvo plagada de guiños al presente, extrayendo lecciones de gestión, resiliencia y liderazgo de episodios históricos. Sorprendió a los presentes mostrando monedas icónicas como el real de a ocho o el maravedí, verdaderos símbolos de la pujanza hispánica que influyeron decisivamente en la economía global. Detalló cómo personajes como Colón o Magallanes debieron desplegar una impresionante cantidad de habilidades de persuasión para sacar adelante sus proyectos, anticipándose así a lo que actualmente conocemos como gestión del cambio, emprendimiento y defensa de la innovación.

Pero uno de los momentos más celebrados de su exposición fue la reivindicación de Gonzalo Fernández de Córdoba, el Gran Capitán, a quien Lominchar atribuyó – con sólidos argumentos – la invención de una suerte de "agilismo" aplicado al arte de la guerra y, por extensión, a la administración y gestión de proyectos en épocas de incertidumbre.



CONTINÚA EN
PRÓXIMA PÁGINA



STA

logía & Común



REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

Estas reflexiones sirvieron de nexo para el siguiente bloque de la jornada, la mesa redonda en la que participaron siete colaboradores de las revistas, una suerte de gabinete de expertos en el que confluyeron voces de disciplinas tan variadas como la inteligencia artificial, el derecho, la gestión pública y la creatividad.

El diálogo, hábilmente moderado por Javier Peris, permitió repasar aquellas tendencias, inquietudes y expectativas que han marcado el último año editorial. Los ponentes compartieron reflexiones sobre cómo escogen sus temas, cómo detectan tendencias y qué importancia conceden al rigor y a la originalidad a la hora de abordar asuntos de actualidad, desde la expansión de la inteligencia artificial hasta los desafíos regulatorios o el potencial transformador de la creatividad en los procesos de cambio. Hubo consenso respecto a la urgente

necesidad de que la sociedad saque partido a las mentes divergentes, esas voces innovadoras, a menudo incómodas pero imprescindibles para que cualquier organización y ecosistema profesional pueda reinventarse y crecer.

Muy lejos de un debate corporativo y riguroso, en varios momentos la conversación adoptó un tono cercano y humorístico, rebajando la solemnidad y recordando la importancia del factor humano para el éxito de cualquier iniciativa. Se insistió en la importancia de mantener la independencia intelectual de los colaboradores, de seguir apostando por la pedagogía aplicada y de construir puentes de entendimiento entre generaciones y perfiles profesionales muy distintos.



CONTINÚA EN
PRÓXIMA PÁGINA



TECNOLOGÍA Y SENTIDO COMÚN

12:15 a 13:00

RICARD MARTÍNEZ
Sección: Ojo al dato

ALEJANDRO ALIAGA
Sección: Radio Security

MARLON MOLINA
Sección: Es Tendencia

MARCOS NAVARRO
Sección: AI Futuro

VICTOR ALMONACID
Sección: La Nueva Administración

MARTA MARTÍN
Sección: Mentes Divergentes

Susíbete gratis

REVISTA
Tecnología & Sentido Común

2022
PREMIOS SAPIENS

REVISTA
Tecnología & Sentido Común

<https://tecnologiaysentidocomun.com>

La mañana prosiguió con la segunda de las mesas redondas, en este caso consagrada a la comunidad internacional de Stakeholders.news.

La mesa reunió tanto a colaboradores presentes como a los corresponsales internacionales, que aportaron sus reflexiones en formato de mensaje grabado, conectando así Madrid con América Latina y el Caribe.

Entre los aspectos más destacados del debate figuraron las diferencias regionales en la percepción y aplicación de la innovación social y empresarial, el impacto de la regulación en los procesos de sostenibilidad y la creciente importancia de la ética, la transparencia y las alianzas multinacionales.

Cada colaborador expuso aquello que considera el mayor aporte de su sección durante el año, detallando no solo las temáticas, sino también las reacciones suscitadas entre los lectores y el valor añadido de contar con una red plural y cosmopolita. La interacción entre moderador y ponentes sirvió para poner de manifiesto la transversalidad de los retos contemporáneos y la urgencia de compartir aprendizaje y experiencias más allá de fronteras y disciplinas.



CONTINÚA EN
PRÓXIMA PÁGINA



Sharing

13:00 a 13:30

DA "STAKEHOLDERS.NEWS"

					
JOSE ANTONIO PUENTES	JOSE LUIS PORTELA	RICARDO SASTRE	LUIS GUARDADO	NESTY DELGADO	DANIEL SOROKINS
Sección: Tendiendo Puentes	Sección: Empleo y Futuro	Sección: Super PMO	Embajador: El Salvador	Embajador: Puerto Rico	Embajador: Uruguay



Suscríbete gratis

REVISTA

Tecnología & Sentido Común

#10

2022 PREMIOS SAPIENS

Llanos Cuenca
NUESTRA INVESTIGACIÓN A FUTURO

Talento y Liderazgo
FERNANDO RIOSA

Es tend...

Alejandro Blasco
CONEXIÓN

La nueva Administración
VÍCTOR ALBARRACÍN

Por Procesos
MADELINE CASTRO

Consejo de amigo
JOSÉ LUIS PUENTE

72+

CONSEJO DE AMIGO

CONSEJO DE AMIGO

REVISTA

Tecnología & Sentido Común

<https://tecnologiaysentidocomun.com>



Este espíritu de apertura y renovación se evidenció de nuevo durante la presentación en sociedad de los nuevos colaboradores y secciones que integrarán la próxima temporada.

El público recibió con interés las propuestas de Domingo Gaitero, dispuesto a arrojar luz sobre la cara más amenazante y menos conocida de la ciberseguridad; la de Angie López Gea, quien acercará la cultura hacker a lectores de todas las edades; y la de Ismael Novo, que analizará el impacto y las aplicaciones prácticas de la inteligencia artificial en los negocios. A ellas hay que sumar la presencia internacional de Estuardo Castañeda, que aportará un enfoque desde Centroamérica mediante contenidos audiovisuales.

Estas nuevas incorporaciones dan fe de la apuesta continua de ambas revistas por la renovación, la pluralidad y el abordaje de tendencias emergentes con relevantes implicaciones sociales y culturales.



CONTINÚA EN
PRÓXIMA PÁGINA

Suscríbete gratis

DIRECCIÓN Y GESTIÓN DE PORFOLIOS, PROGRAMAS Y PROYECTOS

Stakeholders

PROGRAMME & PROJECT MANAGEMENT

NOVIEMBRE #011 - NOVIEMBRE 2022

STAKEHOLDERS NEWS

PROTAGONISTA DEL MES

MARC BERGHMANS

DE AQUELLOS FONDOS, ESTOS LOGROS
en EDITORIAL
con Javier Paris

LECCIONES NO APRENDIDAS
DE LA PANDEMIA
en PROYECTOS SINGULARES
con Carlos Pampliega

DIMENSIONES A TENER EN CUENTA
EN UN PROCESO (SERIO)
DE TRANSFORMACIÓN DIGITAL
en TECNOTRANSFORMACIÓN
con Juan Jesús Urbizu

ESTÁNDARES DE REFERENCIA PARA
LA GESTIÓN DE RIESGOS ISO 21.000
en STEERING COMMITTEE
con Pedro Balas

¿CÓMO MEDIMOS LA RESILIENCIA
DE LAS ORGANIZACIONES?
en ORGANIZACIONES RESILIENTES
con Juan Manuel Domínguez

LAS PMOS EN EL METAVERSO
en SUPER PMOS
con Ricardo Sastre

CONTRATOS ÁGILES
en TRANSFORMACIÓN ÁGIL
con Ángela Plaza

¿CÓMO GENERAS AUTORIDAD
COMO INTERIM MANAGER?
en EMPLEO Y FUTURO
con José Luis Portela

MANEJANDO LAS EXPECTATIVAS
DE UN PROYECTO
en EL LADO HUMANO
con Chayo Fresneda

ENCOCARSE EN EL BIEN SER DE LA
PERSONA, UNA DIMENSIÓN MÁS
HUMANA DENTRO DE LA DIRECCIÓN
en PROYECTOS
con Ismael Novo

PROYECTOS
en CENTROAMÉRICA
con Estuardo Castañeda

51 8



#TYSC / PÁG. 62

TECNOLOGÍA Y
SENTIDO COMÚN

13:30 a 13:45

NUEVOS COLABORADORES



**DOMINGO
GAITERO**
El lado oscuro
(TVSC)



**ESTUARDO
CASTANEDA**
Guatemala
(Stakeholders.news)



**ANGIE
LOPEZ GEA**
Hack & News
(Stakeholders.news)



**ISMAEL
NOVO**
Power AI
(Stakeholders.news)





Uno de los momentos más esperados de la mañana fue, como cada año, la entrega de los premios anuales con los que ambas publicaciones reconocen la labor de personas y entidades fundamentales para el progreso del sector. El Premio Tecnología y Sentido Común 2025 recayó sobre la Subdirección de Sistemas de Información del Hospital Universitari i Politècnic La Fe, una distinción más que merecida por su firme compromiso con la modernización digital, la eficiencia clínica y, sobre todo, la calidad asistencial a través de soluciones tecnológicas innovadoras.

Cayetano M. Hernández Marín recogió el premio en nombre de todo su equipo, acompañando el agradecimiento con un breve y emotivo discurso de gratitud, memoria y optimismo, recordando que todo avance tecnológico es, en última instancia, una apuesta por el bienestar del paciente y la dignidad del profesional sanitario.

En el ámbito de la responsabilidad social, Stakeholders.news reconoció a la Fundación The Pink Force por su extraordinaria iniciativa de acompañamiento emocional a niñas en tratamiento oncológico, haciéndolo en colaboración con el entrañable droide rosa R2-KT, inspirado en la historia real de Katie Johnson. El momento en que Andoni Serrano y el propio R2-KT se acercaron al estrado fue, sin duda, uno de los capítulos más conmovedores del evento. La ovación que recibieron, sincera y prolongada, recordó a todos que la tecnología, por avanzada que sea, solo tiene sentido cuando se pone al servicio de las personas más vulnerables.



**CONTINÚA EN
PRÓXIMA PÁGINA**

Suscríbete gratis

REVISTA MENSUAL DE DIRECCIÓN Y GESTIÓN DE PORTFOLIOS

Stakeholders

PORTFOLIO, PROGRAMME & PROJECT

NÚMERO #011 - NOVIEMBRE

PROYECTOS · GESTIÓN · EXCELENCIA · CALIDAD · PROFESIONALES



ENTREGA DE PREMIOS

PREMIO REVISTA

**Tecnología &
Sentido Común**
20



REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

Llegados a este punto de la jornada, la sucesión de testimonios espontáneos, agradecimientos y recuerdos personales dibujó un ambiente único de comunidad y pertenencia. Los asistentes revivieron anécdotas de pasadas ediciones, mencionaron logros y desafíos superados, e incluso hubo espacio para la emoción y la lágrima compartida, fruto del profundo compromiso y afecto construido entre los colaboradores. Se homenajeó también la memoria de quienes, por motivos personales o profesionales, no pudieron estar presentes, dejando constancia del legado intergeneracional que caracteriza a las revistas.

La mañana se cerró, como manda la tradición, con un exclusivo catering que sirvió para prolongar la conversación y multiplicar las oportunidades de networking. Con mesas repletas de propuestas gastronómicas, la comunidad disfrutó de un momento de distensión en el que las fronteras jerárquicas desaparecen, permitiendo una interacción franca y productiva entre autores, lectores, directores, expertos y nuevos colaboradores. Este ambiente informal y dinámico, lejos de ser un simple complemento social, se ha revelado como uno de los espacios más fructíferos para el surgimiento de ideas, proyectos y futuras colaboraciones.

Culminado el acto, lo que queda es mucho más que el recuerdo de una celebración o el repaso a una década de publicaciones: es precisamente la constatación de que detrás de cada artículo, cada premio, cada panel y cada colaboración hay una apuesta decidida por el humanismo tecnológico, la ética profesional y la convicción de que el conocimiento debe ser compartido, discutido y puesto en acción colectiva. La décima edición del evento de cierre de temporada de Tecnología y Sentido Común y Stakeholders.news se reafirma, así, como un espacio de encuentro, inspiración y referencia para el ecosistema innovador en habla hispana.

El horizonte que se adivina tras esta cita es aún más prometedor. Los desafíos de la próxima década serán, si cabe, todavía más complejos y apasionantes. Nuevos colaboradores y lectores se sumarán a la conversación, las disciplinas seguirán expandiéndose y las alianzas, tanto nacionales como internacionales, pondrán a prueba la capacidad de adaptación, resiliencia y sentido común de toda la comunidad. Pero, como quedó patente a lo largo de toda la jornada, si algo distingue a los protagonistas de esta historia es su voluntad de cielo abierto y mirada larga. Porque, en definitiva, la tecnología y el compromiso social solo son motores de cambio si encuentran a mujeres y hombres dispuestos a caminar juntos, sumar talento y soñar, cada día, una sociedad mejor.



**Curso de
Certificación en:**

Gobierno Corporativo

**ISO 37000
Corporate
Governance
Leader**

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 20 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695€
- Tasas Examen: Incluidas
- Acceso a la Norma: On Line
- A tu ritmo con toda comodidad

MidMgmt®

MPPM®

MGEIT®

eGob®

Tutorías en Directo

Solicita tu admisión en:



+ 34 96 109 44 44

admisiones@escueladegobierno.es

<https://escueladegobierno.es>

UNE presenta su Estrategia 2030 para lograr un mayor impacto de las normas en la sociedad

Se basa en tres objetivos estratégicos: poner el conocimiento recogido en las normas al servicio del progreso compartido de España; impulsar la comunicación sobre los beneficios de las normas y su aplicación; y aportar estabilidad a UNE adaptando su modelo de financiación a la evolución del contexto.

La Estrategia 2030 de la Asociación Española de Normalización, UNE, aprobada en Asamblea General por sus miembros, se basa en tres objetivos y 14 prioridades, con los que la Entidad cumplirá su propósito: contribuir al progreso compartido de la sociedad.

Para lograr la Estrategia, UNE ampliará el alcance de su actividad y generará soluciones para facilitar su aplicación, poniendo el foco en visibilizar los beneficios de los estándares: la normalización aporta un 14,7 % al crecimiento medio anual del PIB en España.

La Asociación Española de Normalización, UNE, ha puesto en marcha su Estrategia 2030, que tiene como objetivo lograr un mayor impacto de las normas en la economía y en la sociedad.

Este ambicioso plan, aprobado por los miembros de UNE en Asamblea General, se basa en tres objetivos estratégicos: poner el conocimiento recogido en las normas al servicio del progreso compartido de España; impulsar la comunicación y el apoyo a la aplicación de las normas; y aportar estabilidad a UNE adaptando su modelo de financiación a la evolución del contexto.

Con ellos, el Organismo español busca ampliar el alcance de la actividad de normalización y dar respuesta eficaz a los grandes desafíos de las organizaciones españolas, potenciando la generación de soluciones que faciliten su implementación; para ello, adaptará el contenido de las normas a sus necesidades con las nuevas herramientas que ofrece la digitalización y, en especial, la inteligencia artificial (IA).

El vicepresidente de UNE, Luis Rodulfo, ha señalado: “La Estrategia UNE 2030 es una hoja de ruta que marca con claridad y suficiente nivel de detalle hacia dónde debemos dirigir todos nuestros esfuerzos y capacidades los próximos años para lograr nuestro propósito: contribuir al progreso compartido de la sociedad y a la creación de un mundo más seguro, sostenible y competitivo a través del desarrollo de estándares”.

En la definición de la Estrategia UNE 2026-2030 se han contemplado los elementos que definen el contexto geopolítico, económico, digital, social, legal y medioambiental, en los que las actividades de normalización y cooperación deben contribuir a lograrla. Además, se ha contemplado la contribución de UNE y de las normas técnicas a la consecución de los 17 Objetivos de Desarrollo Sostenible (ODS) de la Agenda 2030 de Naciones Unidas.



CONTINÚA EN
PRÓXIMA PÁGINA

Estos objetivos estratégicos aterrizan la ambición de UNE de seguir aportando un valor único a la sociedad y a la economía española, consolidando su impacto positivo. De hecho, la normalización aporta un 14,7 % al crecimiento medio anual del PIB en España, lo que se traduce en una contribución de más de 140.000 millones de euros en las últimas cuatro décadas, según el reciente Estudio “Impacto económico de la normalización en España”, realizado por el Centro de Estrategia y Prospectiva Industrial (CEPI), entidad impulsada por el Ministerio de Industria y Turismo y la Fundación EOI.

Los tres objetivos estratégicos son:

1.Poner el conocimiento recogido en las normas técnicas al servicio del progreso compartido de España

Para lograrlo, UNE se ha marcado cinco prioridades: reforzar la Norma como un servicio para las entidades públicas y privadas; dar respuesta a los retos a los que se enfrenta la empresa española con un catálogo de normas actualizado y alineado con sus necesidades; impulsar el liderazgo internacional y europeo de la normalización española; desarrollar un ecosistema equilibrado de alianzas de colaboración entre el ámbito público, privado y la sociedad civil; y ser ejemplar en materia de buen gobierno corporativo.

UNE es depositaria del mejor conocimiento generado por los 12.500 expertos de organizaciones españolas que participan en el desarrollo de estándares en los 200 Comités UNE.

2.Impulsar la comunicación sobre los beneficios de las normas y su aplicación

UNE reforzará la comunicación sobre los beneficios de las normas y generará soluciones para facilitar su aplicación a través de cinco prioridades: incrementar la aplicación de las normas en apoyo a las Administraciones públicas para simplificar la legislación y el despliegue de políticas públicas; garantizar la adecuación del contenido de las normas a las necesidades de aplicación del mercado; impulsar la difusión y aplicación de las normas mediante la actividad de cooperación a nivel nacional, internacional y multilateral, fijando una senda de crecimiento reputacional y económico; promover la cultura de cumplimiento de las normas apoyando la vigilancia de mercado y la evaluación de la conformidad en el marco de la infraestructura de la calidad; y fortalecer la comunicación de UNE.

3.Aportar estabilidad a UNE adaptando su modelo de financiación a la evolución del contexto

Mediante la contribución de todos los actores de su cadena de valor. El tercer objetivo se basa en cuatro prioridades: lograr una mayor contribución económica de las Administraciones públicas a la sostenibilidad de UNE; garantizar la aportación de la explotación del contenido de las normas a la sostenibilidad de UNE en el entorno cambiante de las necesidades de los usuarios; aumentar la contribución de los proyectos de cooperación fijando objetivos de rentabilidad económica y reputacional; y analizar otras líneas potenciales de crecimiento orgánico derivadas del valor generado por UNE



**Hace mucho
tiempo que
hablas.**

**¿Pero hace
cuánto no
dialogas?**



Somos una organización global de beneficio para la comunidad cuya misión es crear normas para contribuir a la construcción de un mundo más seguro, sostenible y competitivo.

Creamos espacios de colaboración neutrales e inspiradores en los que compartir conocimiento para desarrollar, a través del diálogo y el consenso, normas que sirvan a los intereses de toda la sociedad y que movilicen a los que apuestan decididamente por la excelencia empresarial y la conciencia social.

NUEVOS MASTERS



MasterPPM®
MPPM eGob®
Gobierno, Dirección, Gestión y Ejecución de
Portfolios, Programas y Proyectos

MasterGEIT®
MGEIT eGob®
Gobierno y Gestión de
Información y Tecnología

TITULACIÓN
MasterGEIT®

CONTENIDO DEL MASTER

- Módulo 01: Gestión del Tiempo
Curso de Doble Certificación TSG4® Yellow Belt + TSG4® Green Belt
- Módulo 02: Gestión de Procesos de Negocio
Curso de Doble Certificación BPM Executive + ISO 19510 Leader
- Módulo 03: Dirección y Gestión de Proyectos
Curso de Doble Certificación OpenPM® (PgM) Executive + ISO 21502 Leader
- Módulo 04: Dirección y Gestión de Programas
Curso de Doble Certificación OpenPM® (PgM) Executive + ISO 21503 Leader
- Módulo 05: Gestión de Servicios de Tecnología
Curso de Doble Certificación FITSM Executive + ISO 2000 Leader
- Módulo 06: Gestión de Seguridad de la Información
Curso de Doble Certificación CSX Executive + ISO 27000 Leader
- Módulo 07: Gestión de la Continuidad del Negocio
Curso de Doble Certificación CBC Executive + ISO 22301 Leader
- Módulo 08: Gobierno de Información y Tecnología
Curso de Doble Certificación COBIT 2019 Executive + ISO 38500 Leader
- Módulo 09: Gobierno del Dato
Curso de Doble Certificación DAMA Executive + ISO 38505 Leader
- Módulo 10: Gobierno Corporativo
Curso de Doble Certificación COSO Executive + ISO 37000 Leader

MISIÓN
Nuestra misión consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

FORMACIÓN BUSINESS CLASS

- ✓ Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- ✓ Cursos de cuatro sesiones en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- ✓ Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias y anécdotas.
- ✓ Cursos de Doble Certificación convalidables por asignatura del Master en Gobierno, Dirección, Gestión y Ejecución de Portfolios, Programas y Proyectos MasterPPM®.

Escuela de Gobierno eGob®
admisiones@escueladegobierno.es
<https://escueladegobierno.es>

eGob®

Escuela de Gobierno eGob®
admisiones@escueladegobierno.es
<https://escueladegobierno.es>