ESPECIAL

"Tecnoregulación en Prospectiva"

DE Tecnología & Sentido Común

ESPECIAL
AGOSTO
2024

ESPECIAL

"Tecnoregulación en Prospectiva"

DE Tecnología & Sentido Común

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.

ISSN 2951-8180

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

LIVE STREAMING

Sesión de Formación y Certificación en:

Sistema de Gestión de la Inteligencia Artificial

Director Académico:

Javier Peris

- Duración 5 horas
- Sesión única
- Miércoles de 16:00 a 21:00 horas
- En Directo y en Remoto
- Basado en la norma ISO 42001:2023
- Examen de Certificación Incluido
- Certificación ISO 42001 Leader
- Plazas limitadas

MPPM® MGEIT® eGob®

Miércoles 10 de Abril

+ 34 96 109 44 44
campus@escueladegobierno.es

ESPECIAL AGOSTO 2024

índice

DE CONTENIDOS

https://tecnologiaysentidocomun.com

¡tyc

#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.

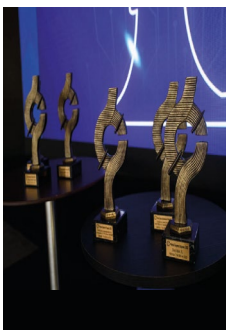
itSMF ESPAÑA

Premio 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

apep

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 Comuni- dad Valenciana COIICV alabó tanto la gran labor de difusión que viene realización 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.

COLEGIO OFICIAL DE INGENIERÍA INFORMÁTICA DE LA COMUNITAT VALENCIANA

Premio 2022 ESET al Periodismo y Divulgación eb Seguridad Informática

VI Premios ESET Periodis- mo y Divulgación: Tecnología y Sentido Común Premiada en la Categoría Blogs por el Articulo 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.

eset

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.

AVIS@ ASOCIACIÓN VALENCIANA DE INFORMÁTICA SANITARIA

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Doble Certificación en:

Gestión Documental y Gestión del Conocimiento

ISO 30301:2021
ISO 30401:2021

Dirección Académica:
Javier Peris

- Dos formatos para tu comodidad
- Opción A: Remoto en Directo
- Opción B: Virtual con Tutoría
- Basado en las Últimas Normas ISO
- Exámenes de Certificación Incluidos
- Certificación ISO 30300 Leader
- Certificación ISO 30401 Leader
- Solicita tu admisión

MPPM® MGEIT® eGob®

Próxima Convocatoria en Directo
Septiembre 2024

Solicita tu admisión en:

+ 34 96 109 44 44
admisiones@escueladegobierno.es

Una regulación de la blockchain como servicio de confianza en la UE

Las tecnologías de registro distribuido (DLT, por sus siglas en inglés), entre las que destacan especialmente las cadenas de bloques (blockchain), vienen siendo objeto de debate jurídico y técnico desde su popularización, principalmente asociada a los activos criptográficos.

Estas tecnologías permiten la creación de una suerte de libro mayor (un almacén de información que mantiene registros finales y definitivos de transacciones) inalterable y gestionado de forma absolutamente descentralizada, que posibilita nuevas aplicaciones, con un potencial transformador muy importante en todos los órdenes. Si bien el concepto de libro mayor fue definido originalmente en la práctica contable y financiera, se puede emplear para el registro de cualesquiera tipos de transacciones, como los movimientos y transferencias de bienes muebles.

Como ejemplo de sistema que ya empieza a madurar en nuestro entorno, podemos referirnos a la Infraestructura Europea de Servicios Blockchain (European Blockchain Services Infrastructure o EBSI, en inglés), una iniciativa conjunta entre la Comisión Europea y la Asociación Europea de Blockchain (EBP) para brindar servicios públicos transfronterizos en toda la UE mediante el uso de la tecnología blockchain.

Para ello, la EBSI se materializará como una red de nodos distribuidos en toda Europa, la infraestructura blockchain, aprovechando un número cada vez mayor de aplicaciones centradas en casos de uso específicos, entre los que destaca singularmente el soporte para la futura Cartera Europea de Identidad Digital.

El pasado 3 de junio, Margrethe Vestager, Vicepresidenta Ejecutiva de la Comisión Europea para Una Europa Adaptada a la Era Digital, y Thierry Breton, Comisario de Mercado Interior, presentaron en Bruselas el esperado texto de la propuesta de modificación del Reglamento eIDAS, para establecer un marco para la Identidad Digital Europea (COM(2021) 281 final) –propuesta de Reglamento eIDAS 2–, y que viene, entre otras cuestiones, a regular los libros mayores electrónicos, incluyendo aquellos basados en Blockchain. Posteriormente, el Consejo de la Unión y el Parlamento Europeo han aprobado sus versiones del Reglamento, a efectos de los diálogos tripartitos que han permitido un acuerdo político el 28 de junio, lo que allana el camino a la aprobación del Reglamento eIDAS 2 antes de final de año.

De forma novedosa, el Reglamento eIDAS 2 ofrece una regulación del libro mayor electrónico. La necesidad de establecer este régimen jurídico conecta con el hecho de que los libros mayores electrónicos aportan a los usuarios prueba y una pista inmutable de auditoría para la secuenciación de transacciones y registros de datos, protegiendo la integridad de los datos, citándose en el Reglamento casos de uso como la compartición de datos desde fuentes descentralizadas, las soluciones de identidad autosoberana o la atribución de

CONTINÚA EN PRÓXIMA PÁGINA


10:00 AM

titularidad en los activos digitales, entre otros; así como en prevenir la fragmentación del Mercado Único Digital, para lo que se debe definir un único marco pan-Europeo que permita el reconocimiento transfronterizo de los servicios de confianza que ofrezcan soporte a la operación de los libros mayores electrónicos, algo que es especialmente relevante cuando el enfoque técnico sea el de una DLT o Blockchain.

En este sentido, se establen los requisitos que debe cumplir todo libro mayor electrónico cualificado, incluyendo su creación por uno o más proveedores de servicios de confianza calificados, la garantía de origen de los registros de datos contenidos en el libro mayor; la garantía del orden cronológico único correcto de los datos en el libro mayor y la precisión de la fecha y hora de la entrada de datos; y el registro de datos de tal manera que cualquier cambio posterior en los datos sea inmediatamente detectable, garantizando su integridad a lo largo del tiempo.

Siguiendo el enfoque de doble nivel propio del Reglamento eIDAS se garantiza, en primer lugar, que todo libro mayor electrónico gozará del principio de no discriminación (por lo que podrá aportarse a un procedimiento administrativo o judicial), pero que, en el caso de que el mismo sea cualificado, los registros de datos contenidos en el mismo gozarán de la presunción de su ordenación secuencial cronológica única y precisa dentro del libro, así como de su integridad. Asimismo, un libro mayor electrónico cualificado será admitido en todos los Estados miembros, facilitando la creación de redes DLT y blockchain de alcance europeo.

En mi opinión, este marco puede suponer la superación de algunas de las problemáticas que están impidiendo el despliegue de las soluciones de SSI y DLT/Blockchain, en especial desde la óptica del uso de blockchain como instrumento acreditativo y de transferencia de responsabilidad legal, que afectan negativamente a enfoques sectoriales como determinados servicios de gestión de criptoactivos.

La regulación del libro mayor electrónico es un imperativo en orden a su adopción fiable, en especial debido a la sustitución de los protocolos de consenso basados en prueba de trabajo (*proof of work*) por otros protocolos que no se basan en pruebas matemáticas intensivas, como sucede con prueba de autoridad (*proof of authority*) o prueba de participación (*proof of stake*), donde es preciso establecer requisitos para poder confiar en el libro mayor electrónico.

No faltarán voces argumentadas que apuesten por mantener esta tecnología sin regulación, pero lo cierto es que el Derecho debe reaccionar ante las disfunciones que hace ya tiempo vienen observándose en este ámbito, y sin duda nos encontramos ante una norma que va a facilitar el uso de estas tecnologías con certidumbre legal.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Doble Certificación en:

Inteligencia Estratégica y Gestión de la Innovación

ISO 56002:2019
ISO 56006:2021

Dirección Académica:
Javier Peris

- Dos formatos para tu comodidad
- Opción A: Remoto en Directo
- Opción B: Virtual con Tutoría
- Basado en las Últimas Normas ISO
- Exámenes de Certificación Incluidos
- Certificación ISO 56002 Leader
- Certificación ISO 56006 Leader
- Solicita tu admisión

MPPM® MGEIT® eGob®

Próxima Convocatoria en Directo
Septiembre

Solicita tu admisión en:

+ 34 96 109 44 44
campus@escueladegobierno.es

Los contratos inteligentes en la propuesta de Ley de Datos

Los contratos inteligentes (*Smart Contracts*) son una de las capacidades de mayor importancia soportadas por las tecnologías de registro o libro mayor electrónico distribuido, como las cadenas de bloques (*Blockchains*). Los contratos inteligentes se definen en ISO 22739:2020 como programas de ordenador almacenados en un sistema de tecnología de libro mayor electrónico distribuido de modo que el resultado de cualquier ejecución del programa se registra en dicho libro mayor, y pueden o no ser considerados contratos en el sentido jurídico del término. De este modo, los contratos inteligentes sustentan la mayoría de las operaciones basadas en cadenas de bloques.

Como parte de la estrategia europea de datos, la Comisión adoptó el 23 de febrero de 2022 la propuesta de Reglamento sobre normas armonizadas sobre el acceso y el uso equitativos de los datos (conocida como Ley de Datos), al objeto de estimular la economía de los datos de la Unión Europea, desbloqueando los datos industriales, optimizando su accesibilidad y uso, y fomentando un mercado europeo de la nube competitivo y fiable.

Esencialmente, la Ley de Datos contiene medidas que permitan a los usuarios de dispositivos conectados acceder a los datos generados por estos dispositivos y por los servicios relacionados con ellos; medidas destinadas a proteger contra las cláusulas contractuales abusivas impuestas unilateralmente; mecanismos para que los organismos del sector público accedan a los datos en poder del sector privado y los utilicen en casos de emergencia pública, tales como inundaciones e incendios forestales, o cuando apliquen un mandato legal en caso de que no se pueda disponer fácilmente de los datos necesarios por otros medios; nuevas normas que conceden a los clientes la libertad de cambiar de proveedor de servicios de tratamiento de datos en la nube; y medidas para promover la elaboración de estándares de interoperabilidad para el intercambio y el tratamiento de datos, en consonancia con la estrategia de normalización de la UE.

Como parte de las medidas de promoción de la interoperabilidad, la propuesta de Ley de Datos apoya el establecimiento de normas para los contratos inteligentes, dado su potencial para ofrecer a los titulares y destinatarios de datos garantías de que se respetan las condiciones para compartir datos. Por ejemplo, para poner técnicamente en marcha el acceso a los datos y su utilización en el contexto de los datos cogenerados de la internet de las cosas.

Más en concreto, un titular de datos legalmente obligado a ponerlos a disposición de destinatarios de datos, podrá utilizar contratos inteligentes, entre otras medidas técnicas de protección adecuadas, para impedir el acceso no autorizado a los datos y garantizar el cumplimiento del régimen jurídico (derecho a compartir datos con terceros, obligaciones de terceros que reciben datos a petición del usuario, compensación por la puesta a disposición de los datos; y resolución de litigios), así como de las condiciones contractuales acordadas para la puesta a disposición de los datos. De ahí la relevancia de los contratos inteligentes como herramienta de gestión automatizada entre las partes en los intercambios de datos.

En definitiva, y con el fin de promover la interoperabilidad de los contratos inteligentes en las aplicaciones de intercambio de datos, la propuesta de Ley de Datos establecerá requisitos esenciales relativos a dichos los

CONTINÚA EN PRÓXIMA PÁGINA

contratos inteligentes. Estos requisitos esenciales se encuentran dirigidos a los profesionales que creen contratos inteligentes para terceros o que integren dichos contratos inteligentes en aplicaciones que apoyen la ejecución de acuerdos de intercambio de datos. Asimismo, los operadores de espacios de datos deberán proporcionar los medios que permitan la interoperabilidad de los contratos inteligentes en el marco de sus servicios y actividades.

Dichos requisitos esenciales son los siguientes:

• **Solidez**, debiendo velarse por que el contrato inteligente se haya diseñado de manera que ofrezca un grado de solidez muy elevado con el fin de evitar errores funcionales y contrarrestar los intentos de manipulación por terceros.

• **Resolución y suspensión seguras**, debiendo velarse por que exista un mecanismo que permita poner fin a la ejecución de transacciones, para lo que el contrato inteligente incluirá funciones internas que permitan reinicializar el contrato o darle instrucciones para poner fin a la operación o suspenderla con objeto de evitar futuras ejecuciones (accidentales).

• **Archivo y continuidad de los datos**, por lo que, en caso de que el contrato inteligente deba resolverse o desactivarse, preverá la posibilidad de archivar los datos de las transacciones, así como la lógica y el código del contrato inteligente, con el fin de llevar un registro de las operaciones con datos efectuadas previamente (auditabilidad).

• **Control de acceso**, de modo que el contrato inteligente estará protegido mediante rigurosos mecanismos de control de acceso en el nivel de la gobernanza y en el del contrato inteligente.

A los efectos de garantizar el cumplimiento de estos requisitos, se deberá realizar una evaluación de conformidad, y expedir una declaración UE de conformidad respecto a dicho cumplimiento. Finalmente, se presumirá que un contrato inteligente que se atenga a las normas armonizadas, o las partes pertinentes de estas normas, elaboradas y publicadas en el Diario Oficial de la Unión Europea es conforme con los requisitos esenciales, en la medida en que dichas normas contemplen esos requisitos.

Como se puede ver, nos encontramos ante una propuesta de Reglamento europeo que puede impulsar de forma muy decidida el uso de los contratos inteligentes en uno de los ámbitos de mayor impacto en cualquier estrategia de compartición de datos, y que se complementa con la propuesta de regulación de los libros mayores electrónicos.

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

LIVE STREAMING

Curso de
Doble Certificación

Gobierno del Tiempo y Gestión de la Productividad

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación TSG4® Yellow Belt
- Certificación UNE 71404 Executive
- Módulo 1: MasterGEIT®
- Módulo 1: MasterPPM®

MPPM® MGEIT® eGob®

Del 15 al 23 de marzo

+ 34 96 109 44 44
campus@escueladegobierno.es

El futuro Esquema Europeo de Certificación de Criterios Comunes

El Reglamento sobre la Ciberseguridad de 2019 regula, además del funcionamiento de la Agencia Europea para la Ciberseguridad (ENISA), la certificación de la ciberseguridad de las tecnologías de la información y la comunicación, dada la creciente criticidad de las mismas para la sociedad digital.

El Reglamento reconoce que la certificación de la ciberseguridad de los productos, servicios y procesos de TIC se utiliza solo en medida limitada, existiendo principalmente a nivel de los Estados miembros (como sucede, por ejemplo, con el Esquema Nacional de Seguridad español, aprobado por RD 311/2022, de 3 de mayo, o con el Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centro Criptológico Nacional, previsto en el RD 421/2004) o en el marco de esquemas impulsados por la industria, por lo que un certificado expedido por una autoridad nacional de certificación de la ciberseguridad no necesariamente es reconocido por los demás Estados miembros.

Esto resulta problemático desde la perspectiva del mercado interior de la Unión, especialmente del mercado único digital, porque puede obligar a las empresas a tener que certificar sus productos, servicios y procesos TIC en los distintos Estados miembros en que operen, en particular para participar en procedimientos de contratación nacionales, con el correspondiente aumento de sus costes. Asimismo, los esquemas existentes presentan deficiencias significativas y diferencias en cuanto a cobertura de productos, niveles de garantía, criterios sustantivos y utilización real, lo que crea dificultades a los mecanismos de reconocimiento mutuo dentro de la Unión; algo que ha quedado puesto de manifiesto en las experiencias existentes en orden a la certificación de la seguridad, significativamente el Acuerdo de Reconocimiento Mutuo (ARM) del Grupo de altos funcionarios sobre seguridad de los sistemas de información (SOG-IS), que se utiliza en relación con dispositivos de creación de firma electrónica, como el DNI electrónico, o los tacógrafos digitales, al amparo de normativas sectoriales.

Para resolver esta problemática, el Reglamento establece un marco europeo de certificación de la ciberseguridad que establezca los principales requisitos horizontales para desarrollar esquemas europeos de certificación de la ciberseguridad y permita que los certificados de ciberseguridad europeos y las declaraciones de conformidad de la UE de productos, servicios o procesos de TIC sean reconocidos y usados en todos los Estados miembros.

Los objetivos de este marco europeo de certificación de la ciberseguridad son contribuir a aumentar la confianza en los productos, servicios y procesos de TIC que hayan sido certificados con arreglo a los esquemas europeos de certificación de la ciberseguridad; evitar la multiplicación de los esquemas de certificaciones nacionales de la ciberseguridad contradictorias o redundantes; y reducir los costes para las empresas que operan en el mercado único digital. Asimismo, los esquemas europeos de certificación de la ciberseguridad deben ser no discriminatorios y basarse en normas internacionales o europeas, a menos que dichas normas resulten ineficaces o inadecuadas para alcanzar los objetivos legítimos de la Unión al respecto.

CONTINÚA EN PRÓXIMA PÁGINA


EXIT

Por su parte, el objetivo de los esquemas europeos de certificación de la ciberseguridad debe ser garantizar que los productos, servicios y procesos de TIC certificados con arreglo a un esquema cumplan los requisitos especificados con objeto de proteger la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados, transmitidos o procesados o las funciones conexas de estos productos, servicios y procesos a lo largo de su ciclo de vida, o los servicios ofrecidos por ellos o accesibles a través de ellos.

En definitiva, el Reglamento crea 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 en la Unión, así como de evitar la fragmentación del mercado interior respecto a los esquemas de certificación de la ciberseguridad en la Unión.

Casi cuatro años después de la aprobación del Reglamento sobre la Ciberseguridad, y después de un complejo proceso, la Comisión Europea ha presentado, por fin, el borrador de Esquema de Certificación de la Ciberseguridad basado en Criterios Comunes (EUCC), construido a partir del, y llamado a suceder al, Acuerdo de Reconocimiento Mutuo (ARM) del Grupo de altos funcionarios sobre seguridad de los sistemas de información (SOG-IS), y alineado con la norma ISO 15408 para la evaluación de la seguridad informática.

La propuesta está llamada a cubrir las necesidades de la certificación de los principales productos que exijan requisitos de ciberseguridad con un nivel de aseguramiento medio o alto, incluyendo productos específicos para la seguridad, a los que se debe exigir especial rigor, pero con el foco puesto en cualquier producto a emplear en entornos críticos o esenciales.

Un ejemplo particular de tipología de producto que deberá sujetarse a esta certificación, en el nivel alto, es la Cartera Europea de Identidad Digital prevista en la Propuesta de Reglamento eIDAS 2, que constituye un medio de identificación electrónica que los ciudadanos de la Unión tendrán disponible, si se cumple el calendario, a partir de mediados de 2026.

Como se puede constatar, se trata de una ambiciosa iniciativa que ayudará a empresas y administraciones públicas a incrementar sus niveles de seguridad, pero también les permitirá una mejor participación en el mercado único.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Análisis de Negocio y Gestión por Procesos

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación BPA Leader
- Certificación BPM Executive
- Módulo 2: MasterGEIT®
- Módulo 2 MasterPPM®

MPPM® MGEIT® eGob®

Del 5 al 13 de abril

+ 34 96 109 44 44
campus@escueladegobierno.es

Acuerdo político sobre la Cartera Europea de Identidad Digital del eIDAS 2

Ya me he referido en esta sección a la propuesta de modificación del Reglamento eIDAS, para establecer un marco para la Identidad Digital Europea (COM(2021) 281 final) –propuesta de Reglamento eIDAS 2–, que se encuentra en la fase final de tramitación legislativa, una vez que el día 8 de noviembre han finalizado los diálogos tripartitos, alcanzándose un acuerdo político final sobre el texto, que ahora será aprobado por el Consejo de la Unión y por el Parlamento Europeo.

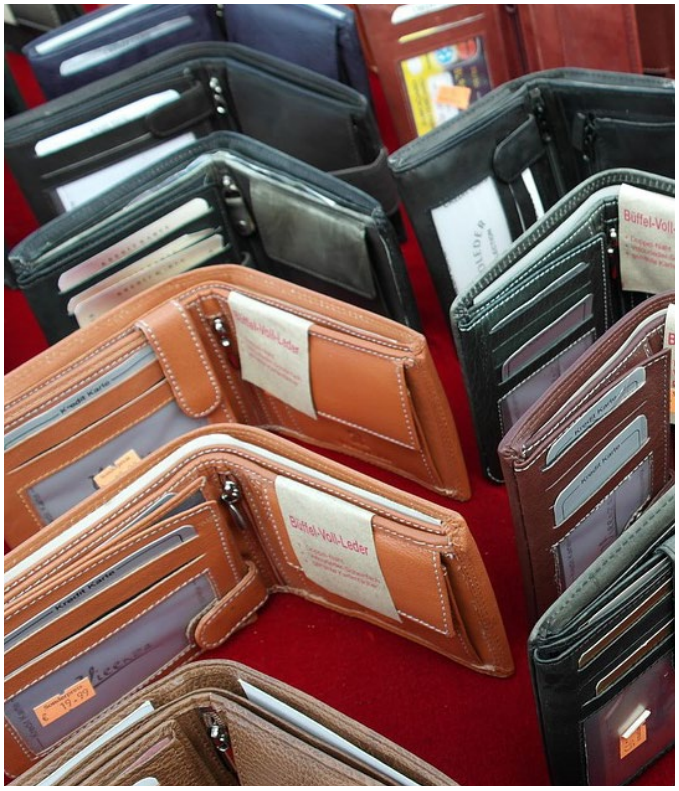
El eje troncal del Reglamento eIDAS 2, como resultado del acuerdo político mencionado, es el establecimiento de un marco de trabajo que, en 2030, conduzca a un amplio despliegue de una identidad digital fiable, voluntaria y controlada por el usuario, reconocida en toda la Unión y que permite a cada usuario controlar sus datos en las interacciones en línea; en línea con los objetivos de la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital, que consagra la visión de la UE sobre la transformación digital, situando a las personas en el centro, empoderando a los ciudadanos e incentivando a las empresas innovadoras.

El Reglamento eIDAS 2 reconoce un verdadero derecho, de los ciudadanos de la Unión, a una identidad digital bajo su control exclusivo, que les permita ejercer sus derechos en el espacio digital, así como a participar en la economía digital.

La aproximación unificada del Reglamento eIDAS 2 viene a resolver carencias del actual Reglamento, como la existencia de sistemas nacionales de identificación electrónica divergentes o la ausencia de estos sistemas en algunos Estados, así como la falta de armonización en el uso de medios de identificación electrónica, o la dificultad en el intercambio de otros documentos con atributos de identidad, como las cualificaciones profesionales, lo que facilita la aplicación del principio de “Sólo una vez”, tan importante para el correcto funcionamiento del mercado interior.

En este contexto, el Reglamento eIDAS 2 regula la cartera europea de identidad digital, que define como un medio de identificación electrónica que permite al usuario almacenar de forma segura, gestionar y validar datos de identidad y declaraciones electrónicas de atributos para ofrecerlos a terceros (partes que confían) y a otros usuarios de carteras europeas de identidad digital, así como crear firmas electrónicas cualificadas o sellos electrónicos cualificados.

CONTINÚA EN PRÓXIMA PÁGINA



Entre los elementos claves de la cartera europea de identidad digital, encontramos los siguientes:

•Los Estados miembros deben proporcionar al menos una cartera europea de identidad digital en el plazo de 24 meses desde la adopción de los actos de ejecución previstos en el propio Reglamento, lo que podría conducirnos a mediados de 2026.
•La cartera europea de identidad digital puede ser proporcionada directamente por el Estado miembro, proporcionada conforme a un mandato del Estado miembro, o proporcionada de forma independiente de un Estado miembro pero reconocida por dicho Estado miembro, lo que permite fórmulas muy interesantes de ordenación de un mercado de identificación electrónica.
•El código fuente los componentes de software de la cartera europea de identidad digital que deban instalarse en los dispositivos de usuarios debe licenciarse como fuente abierta.
•La cartera europea de identidad digital debe permitir su uso en relaciones presenciales y a distancia, tanto con otras carteras como con sistemas de terceros, así como la divulgación selectiva de datos de identidad personal, en su caso en combinación con otros atributos de identidad. Asimismo, la cartera debe permitir a los usuarios verificar la autenticidad y validez de la identidad de los terceros registrados.
•La cartera europea de identidad digital debe permitir la creación de pseudónimos por parte del usuario, y almacenarlos de forma cifrada.
•La cartera europea de identidad debe permitir el acceso por el usuario a un registro de las transacciones realizadas mediante un cuadro de mando que permita visualizar el listado actualizado de los terceros con los que se han intercambiado datos, y cuando proceda, todos los datos intercambiados; solicitar a un tercero la supresión de datos personales; y reportar a la autoridad nacional encargada del control de protección de datos cualquier solicitud sospechosa de datos por un tercero.
•La cartera europea de identidad digital debe ofrecer firmas electrónicas cualificadas y sellos electrónicos cualificados. En el caso de la firma electrónica cualificada, la misma será ofrecida por defecto y sin coste, si bien los Estados miembros pueden establecer medidas proporcionadas para garantizar que se hace un uso no profesional de la misma, lo que permite mantener una sana competencia en relación con el mercado de servicios de confianza.
•Los mecanismos de validación de la cartera europea de identidad digital serán gratuitos, y los Estados miembros deberán proporcionar medios para revocar la validez de la cartera europea de identidad digital.
•Finalmente, y sin ánimo de exhaustividad, los suministradores de las carteras europeas de identidad digital deberán garantizar que los usuarios pueden solicitar fácilmente soporte técnico y notificas problemas técnicos y otras incidencias.

Todos estos elementos permiten realizar una valoración francamente positiva de este nuevo medio de identificación electrónica, aunque, como “el Diablo está en los detalles”, sólo una adecuada implementación técnica garantizará que la promesa de usabilidad, seguridad y privacidad de la cartera europea de identidad digital se cumple.

Para ello, se han puesto en marcha diversas iniciativas, íntimamente relacionadas. En primer lugar, los Estados miembros colaboran en la definición de la arquitectura y las especificaciones técnicas del ecosistema del Reglamento eIDAS 2 (proceso conocido como ARF Toolbox); en segundo lugar, la Comisión Europea desarrolla, con la participación de los Estados miembros, el software de referencia de la cartera europea; finalmente, se han financiado cuatro pilotos de gran escala para probar las capacidades de la cartera, aportando feedback tanto al ARF Toolbox como al software de referencia, siendo uno de ellos el proyecto DC4EU, liderado por España.

Ciertamente, se trata de una iniciativa de muy alto impacto, que avanza a gran velocidad y que, sin duda, hay que tener en el radar en toda iniciativa digital.

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

LIVE STREAMING

Curso de
Doble Certificación

Gestión de Proyectos

OpenPM² (PjM) + ISO 21502

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación OpenPM² (PjM) Executive
- Certificación ISO 21502 Leader
- Módulo 3: MasterGEIT®
- Módulo 3 MasterPPM®

MPPM® MGEIT® eGob®

Del 19 al 27 de abril

+ 34 96 109 44 44
campus@escueladegobierno.es

La era de las declaraciones electrónicas de atributos

Siguiendo con el análisis de la propuesta de modificación del Reglamento eIDAS, para establecer un marco para la Identidad Digital Europea (COM(2021) 281 final) –propuesta de Reglamento eIDAS 2–, a que vengo refiriéndome desde esta tribuna, corresponde analizar sucintamente la enorme novedad que constituye la regulación de las denominadas declaraciones electrónicas de atributos, complemento de la Cartera Europea de Identidad Digital.

La propuesta de Reglamento eIDAS 2 crea nuevos servicios de confianza, que encomienda a un mercado en libre competencia, como viene sucediendo, entre otros, con la certificación de la firma electrónica de las personas físicas o del sello electrónico de las personas jurídicas.

Este enfoque responde, a juicio de la Comisión Europea, a la aparición de un nuevo entorno donde el enfoque ha cambiado de la provisión y uso de identidades digitales rígidas a la provisión y dependencia de atributos específicos relacionados con esas identidades, a lo que cabe añadir la necesidad de aplicar tecnologías de protección de la privacidad, como la divulgación selectiva de datos personales, lo que empieza a ser incompatible con la compartición completa de documentos oficiales de identidad, por ejemplo, como se ha visto en recientes resoluciones sancionadoras de la Agencia Española de Protección de Datos.

Entre los nuevos servicios de confianza, encontramos la expedición y de la validación de declaraciones electrónicas de atributos, que el Reglamento define como "una declaración en forma electrónica que permite la autenticación de atributos", definiéndose, asimismo, el concepto de atributo como una "característica, cualidad, derecho o permiso de una persona física o jurídica, o de un objeto". Como ejemplos de atributos, el Reglamento eIDAS 2 cita las cualificaciones académicas, los grados universitarios o las cualificaciones profesionales.

Como se puede ver, se trata de un nuevo tipo de documento electrónico, que vincula uno o varios atributos de identidad a un persona física o jurídica, con la garantía de que dichos atributos han sido verificados y, por tanto, son auténticos. En este sentido, conforme al Reglamento eIDAS 2, una persona física o jurídica podrá contratar los servicios de cualquier prestador de servicios de confianza para que le expida estas declaraciones de atributos y, una vez en su poder, utilizarlas en las transacciones donde se requiera, lo que habilita un nuevo mercado de datos personales bajo el control del interesado, con elevadas garantías de seguridad y de privacidad.

El Reglamento eIDAS 2 prevé dos regímenes jurídicos diferenciados en relación con la expedición de declaraciones electrónicas de atributos, aplicable a las declaraciones expedidas por prestadores de servicios de confianza, en su caso cualificados, u a las declaraciones expedidas por entidades del sector público responsables de fuentes auténticas, o en nombre de las mismas.

La novedad se encuentra, en especial, en la expedición de declaraciones electrónicas de atributos por parte de prestadores de servicios de confianza, dado que supone una técnica de privatización de la actividad jurídica de los actos de constancia, que hasta ahora se encontraba reservada en exclusiva a las autoridades y otras

CONTINÚA EN PRÓXIMA PÁGINA


EU DIGITAL COVID CERTIFICATE
INTERNATIONAL CERTIFICATE OF VACCINATION
DIGITAL GREEN PASS
COVID-19
STATUS: IMMUNE

entidades titulares de registros jurídicos y administrativos. Para ello, el Reglamento eIDAS 2 establece los siguientes efectos jurídicos en relación con las declaraciones electrónicas de atributos:

•**Principio de no discriminación:** No se denegará a una declaración electrónica de atributos el efecto jurídico ni la admisibilidad como prueba en procedimientos judiciales por el mero hecho de que esté en formato electrónico o de que no cumpla los requisitos para las declaraciones electrónicas cualificadas de atributos.
•**Principio de equivalencia funcional:** Una declaración electrónica cualificada de atributos y las declaraciones electrónicas de atributos expedidas por, o en nombre de, un organismo del sector público responsable de una fuente auténtica tendrán el mismo efecto jurídico que las declaraciones legalmente emitidas en papel.

•**Reconocimiento transfronterizo, en sentido doble:** Una declaración electrónica cualificada de atributos expedida en un Estado miembro se reconocerá como una declaración electrónica cualificada de atributos en todos los demás Estados miembros. Asimismo, una declaración de atributos expedida por o en nombre de un organismo del sector público responsable de una fuente auténtica se reconocerá como una declaración de atributos expedida por o en nombre de un organismo del sector público responsable de una fuente auténtica en todos los Estados miembros.

Al objeto de permitir la confianza en las informaciones contenidas en las declaraciones expedidas por prestadores de servicios de confianza, el Reglamento el acceso de los prestadores de servicios de confianza a las fuentes auténticas que contienen los atributos a declarar, las que define como un repositorio o sistema, bajo la responsabilidad de un organismo del sector público o una entidad privada, que contenga y proporcione atributos sobre una persona física o jurídica y que se considere una fuente primaria de dicha información o se reconozca como auténtico de conformidad con el Derecho de la Unión o nacional, incluidas las prácticas administrativas.

El acceso se garantiza, como mínimo, para los siguientes atributos: dirección; edad; género, estado civil, composición familiar, nacionalidad o ciudadanía, cualificaciones educativas, títulos y licencias, cualificaciones, títulos y licencias profesionales, facultades y mandatos para representar a personas físicas o jurídicas, permisos y licencias públicas, y, para personas jurídicas, datos financieros y de la empresa.

Este listado muestra el potencial transformador de esta propuesta, que permite un nuevo mercado descentralizado de datos para su consumo en procesos de negocio, bajo el control del interesado. Sin duda, facilitará el acceso a los datos, cuanto menos, a los datos de las Administraciones Públicas, tan necesario en las transacciones electrónicas.

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

LIVE STREAMING

Curso de
Doble Certificación

Gestión de Programas

OpenPM² (PgM) + ISO 21503

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación OpenPM² (PgM) Executive
- Certificación ISO 21503 Leader
- Módulo 4: MasterGEIT®
- Módulo 4 MasterPPM®

MPPM® MGEIT® eGob®

Del 3 al 11 de mayo

+ 34 96 109 44 44
campus@escueladegobierno.es

Evento de Cierre de Temporada 2024 de las Revistas Tecnología y Sentido Común y Stakeholders.news

El 19 de julio de 2024, las revistas Tecnología y Sentido Común y Stakeholders.News celebraron el Cierre de su novena y tercera temporada respectivamente con un interesante evento en la sede de UNE Asociación Española de Normalización, en Madrid.

En una tradición que se inició el pasado año 2023, las revistas Tecnología y Sentido Común y Stakeholders.News prepararon un cierre de temporada a la altura tanto de la calidad de sus contenidos como del nivel de sus colaboradores. Con la inestimable colaboración de UNE Asociación Española de Normalización, el día 19 de julio de 2024 se reunió en Madrid un granado grupo de profesionales, entre los que estaban algunos de los colaboradores de nuestras revistas.

El evento comenzó con una bienvenida a cargo de Paloma García, Directora de Programas de Normalización y Grupos de Interés de UNE, y de Javier Peris, Director de las revistas Tecnología y Sentido Común y Stakeholders.News, en el que agradecieron a los presentes su asistencia, sobre todo a aquellos afectados por el incidente global en sistemas de información de grandes compañías de todo tipo que se dio en esa fecha.

CONTINÚA EN PRÓXIMA PÁGINA

Evento Protagonista

Tras la bienvenida, se dio paso al ponente principal del evento, Ramsés Gallego, primer español (y tercer europeo) en ser nombrado para el "Hall of Fame" de ISACA internacional, evento que tuvo lugar en este 2024. Renombrado conferenciante, deleitó al público asistente con su charla "De Gestionar a Gobernar …. con 'G' de Ganar", en la que glosó las bondades de dar ese salto hacia el gobierno de las Tecnologías de la Información, sobre todo en los aspectos relacionados con la ciberseguridad. Ciertamente, un lujo contar con él para el evento.

CONTINÚA EN PRÓXIMA PÁGINA

Evento Protagonista

El siguiente acto fue la mesa redonda con cinco de los autores que colaboran con la revista Tecnología y Sentido Común en el que participaron: Alejandro Aliaga líder de la seccion “Radio Security”, Renato Aquilino líder de la sección “Marcos y Normas”, Marlon Molina líder de la seccion “Es Tendencia”, Marcos Navarro líder de la seccion Ai Robot” que a partir de la proxima temporada pasará a llamarse “Ai Futuro” y Manuel Serrat líder de la seccion “Futuro y Seguridad”.

Durante la mesa redonda de Tecnologia y Sentido Común, estos cinco representantes respondieron a las preguntas del presentador y director de la revista, Javier Peris, acerca de los contenidos de la temporada que terminaba, y de qué se podía esperar de sus secciones en cuanto a contenidos y novedades en la décima temporada de la revista.

Alejandro Aliaga centró su intervención en recordad que el objetivo de su sección “Radio Security” es concienciar a los lectores de que existen vectores de ataque no convencionales asociados con las comunicaciones inalámbricas, y que, por la evolución tecnológica, es difícil que éstos se reduzcan.

Por su parte, Renato Aquilino, en su sección “Marcos y Normas” ha centrado sus contenidos en poner de manifiesto el gap existente entre las normas y quienes las escriben, frente a quienes las han de convertir en realidad en las organizaciones, algo que resulta extremadamente complejo en algunos casos.

Por lo que respecta a Marlon Molina, con su sección “Es Tendencia”, ha tratado de contar a los lectores en esta temporada que termina los temas que, mes a mes, han atraído la atención del sector por diferentes motivos.

Marcos Navarro anunció que su sección, a partir de la décima temporada, cambiaba de enfoque y de nombre, para explicar cómo es la vida en 2024, sólo dentro de diez años, gracias a tecnologías como la Inteligencia Artificial y la Robótica.

En cuanto a Manuel Serrat, explicó que con su sección “Futuro y Seguridad” ha tratado de poner el foco en aquellos aspectos de la evolución tecnológica que pueden suponer algún tipo de riesgo, y concienciar a los lectores para evitarlos.

CONTINÚA EN PRÓXIMA PÁGINA

Evento Protagonista

Finalizada esta mesa redonda, se llevó a cabo la segunda Mesa Redonda, que contó con cuatro de los colaboradores de la revista Stakeholders.News: Juan Manuel Domínguez líder de la Seccion "Organizaciones Resilientes", Luis Morán líder de la sección "Personas y Procesos", José Antonio Puentes líder de la seccion "Tendiendo Puentes" y Juan Jesús Urbizu líder de la seccion "Tecno-transformación".

Dada la temática de la revista, fundamentalmente dirigida a aquellos profesionales de la gestión de proyectos, programas y portfolios y áreas conexas, las preguntas para los participantes en la mesa redonda se centraron en poner de relieve la necesaria aplicación de estándares y buenas prácticas en cada uno de los ámbitos que tratan las diferentes secciones de la revista.

Juan Manuel Domínguez, a través de su sección "Organizaciones Resilientes", expuso aspectos tales como que, en Japón, con aproximadamente 120 millones de habitantes, hay 45.000 empresas centenarias, frente a las poco más de 5.000 que existen en España con 48 millones de habitantes.

Luis Moran comentó algunos de los temas que había tratado durante esta tercera temporada en su sección "Personas y Procesos", y avanzó alguna de las cuestiones que va a tratar en la cuarta temporada de la revista.

José Antonio Puentes (sección "Tendiendo Puentes") compartió con los presentes algunas vivencias personales, relacionadas con las dificultades que la gestión de proyectos enfrenta en determinadas organizaciones.

Por último, Juan Jesús Urbizu, que estas temporadas ha escrito en su sección "Tecno Transformación", apuntó algunas de las cuestiones más relevantes a las que se enfrenta el gestor de proyectos, programas y portfolios en relación con la digitalización de las organizaciones, y más desde la irrupción para el gran público de los sistemas de inteligencia artificial.

CONTINÚA EN PRÓXIMA PÁGINA

Tras las dos mesas redondas, Javier Peris anunció el nombramiento de los tres embajadores de la revista Stakeholders.News en Hispanoamérica más concretamente en Puerto Rico, Uruguay y El Salvador.
En Puerto Rico contaremos cada mes con la participacion de Nesty Delgado en Uruguay contaremos con Daniel Sorokins y en el pais de la eterna sonrisa "El Salvador contaremos con Luis Guardado quienes fueron nombrados y serán a partir de ahora Embajadores de Stakeholders.news.

Los actos de cierre de temporada terminaron con la entrega de los premios Tecnología y Sentido Común y Stakeholders. News, en esta ocasión en su edición de 2024.

El "Premio Tecnología y Sentido Común 2024" recayó en el Consejo General de Colegios Profesionales de Ingeniería Informática (CCII), por su aportación al progreso de la sociedad de la información, el impulso al desarrollo ético de los avances tecnológicos y la defensa y promoción de la ingeniería en informática. El premio fue recogido por José García Fanjul, secretario del CCII y vicedecano del Colegio Oficial de Ingenieros en Informática del Principado de Asturias.

Por otro lado, el "Premio Stakeholders.News 2024" fue otorgado a la Agencia para la Administración Digital de la Comunidad de Madrid, por haberse convertido en referente en la innovación y digitalización de la administración pública y por su compromiso con el cumplimiento y la excelencia del servicio al ciudadano. Este premio fue recogido por Zaida Sampedro Préstamo, subdirectora general de Transformación y Gestión del Cambio de la Agencia para la Administración Digital de la Comunidad de Madrid.

Al terminar el acto, todos los presentes pudieron disfrutar de un magnífico networking alrededor de un espectacular catering que se sirvió en las mismas instalaciones de UNE, con lo que se dio por cerrada la temporada de ambas revistas. ¡Nos vemos en septiembre!

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.

UNE Normalización Española

Progreso compartido

une.org

¿Es el eIDAS 2 una amenaza para la confianza en la web pública?

Los lectores de esta sección ya estarán familiarizados con la propuesta de modificación del Reglamento eIDAS, para establecer un marco para la Identidad Digital Europea (COM(2021) 281 final) –propuesta de Reglamento eIDAS 2–, que entre otras cuestiones viene a adecuar las reglas del mercado de servicios de confianza.

En esta ocasión nos vamos a centrar en la reforma de los certificados de autenticación de sitio web, en su caso cualificados, que ha generado una amarga polémica cuya resolución final aún se encuentra, en cierto modo, pendiente.

Y es que la propuesta de Reglamento eIDAS 2 modifica el régimen jurídico de estos certificados, que se vienen a corresponder con los certificados de servidor seguro empleados para proteger los accesos a las páginas web públicas mediante el protocolo TLS (https://midominio.es), garantizando el cifrado de las comunicaciones electrónicas y, en menor grado, la identidad de sus titulares.

La expedición de los certificados de servidor seguro se realiza por las denominadas autoridades de certificación, oficialmente en régimen de libre competencia, pero con sujeción a la autorregulación de los principales proveedores de software para el acceso a páginas web, incluyendo Google, Mozilla o Microsoft, que mantienen programas de Autoridad de Certificación Raíz. De este modo, para que una compañía pueda emitir un certificado de servidor seguro TLS, debe obligarse a cumplir las exigencias de estos programas, que remiten a la adopción de los requisitos administrativos, organizativos y de seguridad previstos por un foro de la industria (sin personalidad jurídica independiente) conocido como el CA/Browser Forum. Este foro ha definido, esencialmente, cuatro tipologías de certificados de servidor seguro:

- **Certificado Domain Validated (DV)**, que se expide a una persona física u organización que acredita el derecho a utilizar un nombre de dominio, y que sólo contiene un nombre de dominio.
- **Certificado Individual Validation (IV),** que se expide a una persona física que acredita el derecho a utilizar un nombre de dominio y que además contiene el nombre y apellidos del solicitante, verificados mediante documentos públicos o privados.
- **Certificado Organizational Validation (OV)**, que se expide a una organización que acredita el derecho a utilizar un nombre de dominio y que además contiene la denominación social y la dirección de la organización, verificadas mediante consultas a bases de datos o métodos de fiabilidad análoga.

CONTINÚA EN PRÓXIMA PÁGINA

•**Certificado Extended Validation (EV)**, que se expide a una organización que acredita el derecho a utilizar un nombre de dominio y que además contiene un gran cantidad de información identificativa de la organización, verificada mediante procedimientos estrictos.

Por su parte, el Reglamento eIDAS reguló, posiblemente como consecuencia de ciberataques graves como los sufridos por Comodo en 2011 o DigiNotar en 2012, el servicio de confianza de expedición de certificados de autenticación de sitio web, que definió como "una declaración que permite autenticar un sitio web y vincula el sitio web con la persona física o jurídica a quien se ha expedido el certificado", configurando la prestación y utilización de dichos certificados de forma totalmente voluntarias, al tiempo que regula los certificados cualificados de autenticación de sitio web a efectos de generar una mayor confianza por parte de los usuarios.

A este efecto, el Anexo IV detalla los contenidos que deben tener dichos certificados, bastante alineados con las exigencias del CA/Browser Forum, y que han sido objeto de desarrollo técnico por los estándares del ETSI, construidos a partir de las políticas de certificados IV, OV y EV, en función del caso, si bien resulta posible expedir certificados cualificados de autenticación de sitio web sin tener que sujetarse en absoluto a las exigencias del CA/Browser Forum, que no serán admitidos por los fabricantes en el entorno del acceso a la web pública, pudiendo sin embargo ser útiles en escenarios como los intercambios entre proveedores de servicios de pago conforme a la Directiva PSD2.

La propuesta de Reglamento eIDAS 2 cambia este modelo, basado en la voluntariedad, al exigir que los certificados cualificados de autenticación de sitio web deberán ser obligatoriamente reconocidos por los navegadores, que deberán mostrar de forma amigable los datos de identidad y otros atributos contenidos en los certificados, y sin poder sujetar a estos certificados a condiciones adicionales ni obligar a incluir en los mismos otros contenidos.

Esta propuesta ha generado una importante campaña de oposición, liderada por los navegadores, pero a la que también se han sumado algunas organizaciones de la sociedad civil y un nutrido grupo de expertos en ciberseguridad, basada en la posibilidad de que los Estados puedan, nada más y nada menos, que espiar a los ciudadanos mediante la inclusión, en la lista de prestadores cualificados, de algunos que supuestamente generarían certificados al objeto de suplantar la identidad de páginas web.

La propuesta de Reglamento eIDAS 2 ha incorporado medidas para que los navegadores puedan, en el caso de tener dudas fundadas acerca de posibles incidencias de seguridad, suspender cautelarmente el reconocimiento de un certificado o de un conjunto de certificados (lo que podría significar el total de certificados expedidos por un prestador concreto, en su caso), hasta que el supervisor decida sobre el mantenimiento de la cualificación, pero parece que no ha sido suficiente para apaciguar estas críticas.

Quizás nos encontramos ante una sobrerreacción motivada por la pérdida de poder que sufrirán los navegadores, un oligopolio acostumbrado a imponer sus exigencias, pero hasta la aprobación del proyecto por ambos co-legisladores, prevista para marzo de 2024, la lucha continuará. Y es difícil prever cuál será el resultado de este pulso.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Service Management FitSM + ISO 20000

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación FitSM Executive
- Certificación ISO 20000 Leader
- Módulo 5 MasterGEIT®
- Módulo 5 MasterPPM®

MPPM® MGEIT® eGob®

Del 17 al 25 de mayo

+ 34 96 109 44 44
campus@escueladegobierno.es

El Parlamento Europeo apueba el Reglamento de pagos instantáneos en euros

El 7 de febrero pasado, el Parlamento Europeo aprobó la Propuesta que modifica el Reglamento (UE) Nº 260/2012, de 14 de marzo de 2012, por el que se establecen requisitos técnicos y empresariales para las transferencias y los adeudos domiciliados en euros, y el Reglamento (UE) 2021/1230 de 14 de julio de 2021 relativo a los pagos transfronterizos en la Unión, en relación con las transferencias instantáneas en euros, popularmente conocidas como "pagos instantáneos" en la zona única de pagos en euros (SEPA).

El nuevo Reglamento tiene como objetivo garantizar que los clientes minoristas y las empresas, especialmente las pymes, no tengan que esperar por su dinero, así como mejorar la seguridad de las transferencias, por lo que los bancos y otros proveedores de servicios de pago (PSP) deberán garantizar que las transferencias de crédito sean asequibles y se procesen de inmediato. La normativa entrará en vigor, para proveedores establecidos en Estados con euro, en 9 meses para recepción de transferencias inmediatas, y 18 meses para envío de transferencias inmediatas.

La transferencia instantánea se define, en el nuevo Reglamento, como una transferencia que se ejecuta de forma inmediata, las 24 horas del día y en cualquier día natural (nuevo artículo 2bis). El nuevo artículo 5bis.1 del Reglamento (UE) nº 260/2012 obliga a los PSP que ofrezcan el servicio de envío y recepción de transferencias a ofrecer también, a todos sus clientes el servicio de transferencia instantánea, debiendo además asegurar que todas las cuentas de pago que admitan recepción de transferencias admitan también recepción de transferencias instantáneas 24 horas, todos los días del año.

Sin duda, la primera medida estrella del nuevo Reglamento se contiene en el nuevo artículo 5bis.4.c), en cuya virtud el PSP del beneficiario deberá, en un plazo de diez segundos desde el momento de la recepción de la orden de pago para una transferencia instantánea por parte del PSP del ordenante, abonar el importe de la transacción de pago disponible en la cuenta de pago del beneficiario en la moneda en la que está denominada la cuenta del beneficiario y confirmar la finalización de la transacción de pago al PSP del ordenante.

Obviamente, resulta extraordinariamente importante determinar cúando se ha producido dicha recepción de la orden de transferencia, lo que supone establecer reglas específicas y diferentes de las comunes a otros servicios de pago. Por ello, y con carácter general, el nuevo artículo 5bis.3 concreta que el momento de recepción de una orden de pago para una transferencia instantánea será el momento en que haya sido recibida por el PSP del ordenante, independientemente de la hora o dia del calendario. Asimismo, si el ordenante y su PSP acuerdan que la ejecución de la orden

CONTINÚA EN PRÓXIMA PÁGINA

de pago para una transferencia instantánea tendrá lugar en un momento específico en un día específico o en el momento en que el ordenante haya puesto fondos a disposición de su PSP, el momento de recepción de la orden de pago para una transferencia inmediata se considerará la hora acordada, independientemente de la hora o día natural.

De este modo, y en ambos casos, se elimina el efecto de la recepción de orden en día inhábil o en día hábil en horario cercano a día inhábil, pero con tres excepciones: ordenación no electrónica (en papel) de transferencia inmediata, orden individual integrada en un paquete y transferencias con origen en cuentas no denominadas en euros.

Además, el PSP del beneficiario se asegurará de que la fecha del valor del crédito para la cuenta de pago del beneficiario sea la misma fecha que la fecha en la que el PSP del beneficiario acredita la cuenta de pago del beneficiario con el importe de la transacción de pago (artículo 5bis.4.d)), lo que evitará problemas, por ejemplo, en pagos de facturas sujetas al régimen especial de IVA de caja.

Finalmente, el PSP del ordenante deberá informar de forma gratuita al ordenante y, en su caso, al proveedor de servicios de iniciación de pagos, si el importe de la operación de pago se ha puesto a disposición en la cuenta de pago del beneficiario, inmediatamente después de recibir la confirmación de finalización, o cuando el PSP del ordenante no reciba dicha confirmación de finalización en un plazo de diez segundos desde el momento de la recepción de la orden de pago para una transferencia instantánea (artículo 5bis.4.e)). En todo caso, si no se recibe dicha confirmación en este plazo de diez segundos, el PSP del ordenante retrocederá la operación (artículo 5bis.5).

La segunda medida estrella del Reglamento, y ésta tiene mayor impacto en nuestro país, es que cualquier cargo cobrado por un PSP a los ordenantes y beneficiarios con respecto al envío y recepción de transferencias instantáneas no será superior a los cargos cobrados por ese PSP con respecto al envío y recepción de otras transferencias de crédito del tipo correspondiente, lo que finaliza con la práctica de ofrecer transferencias ordinarias sin coste y transferencias instantáneas con coste.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Seguridad de la Información

CSX + ISO 27001

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación CSX Executive
- Certificación ISO 27001 Leader
- Módulo 6: MasterGEIT®

MGEIT® eGob®

Del 7 al 15 de junio

+ 34 96 109 44 44
campus@escueladegobierno.es

El Parlamento obliga a la Comisión a rendirse ante los navegadores

Comentaba en mi artículo de febrero la polémica generada por la reforma del régimen jurídico de los certificados de autenticación de sitio web, en su caso cualificados. Se recordará que estos certificados se vienen a corresponder con los certificados de servidor seguro empleados para proteger los accesos a las páginas web públicas mediante el protocolo TLS (https://midominio.es), garantizando el cifrado de las comunicaciones electrónicas y, en menor grado, la identidad de sus titulares.

La propuesta de Reglamento eIDAS 2 parte de la exigencia de que los certificados cualificados de autenticación de sitio web sean obligatoriamente reconocidos por los navegadores (a los que, por cierto, el Reglamento eIDAS 2 se refiere como "prestadores de servicios de navegación web"), que deberán garantizar que los datos de identificación de la persona declarados en el certificado y los atributos declarados adicionales se muestren al usuario de un modo fácil de consultar. Asimismo, garantizarán la compatibilidad e interoperabilidad con los certificados cualificados de autenticación de sitios web, y no podrán obligar a incluir en estos certificados otros contenidos.

Como también se recordará, explicaba desde esta privilegiada tribuna la intensa campaña de información (y, no en menor medida, de desinformación) que se ha generado alrededor de la propuesta del Reglamento eIDAS 2, y que parece haber calado suficientemente en el ánimo del Parlamento Europeo, hasta el punto de haberse admitido una enmienda final como condición para la aprobación del Reglamento eIDAS 2 en el Plenario del 29 de febrero.

Dicha enmienda, la número 7, consiste en la incorporación de la siguiente Declaración de la Comisión relativa al artículo 45, que procede reproducir en forma íntegra:

"La Comisión acoge con satisfacción el acuerdo alcanzado, que, en su opinión, aclara que los navegadores están obligados a garantizar apoyo e interoperabilidad para los certificados cualificados de autenticación de sitios web con el único fin de mostrar los datos de identidad del propietario del sitio web de un modo fácil de entender. La Comisión entiende que esta obligación no prejuzga los métodos utilizados para mostrar dichos datos de identidad.

CONTINÚA EN PRÓXIMA PÁGINA


EVERLAST
TECATE
IRON BOY
hermosa
NIKE

La Comisión acoge con satisfacción el acuerdo alcanzado, que, en su opinión, aclara que el requisito de que los navegadores web reconozcan los certificados cualificados de autenticación de sitios web no restringe las propias políticas de seguridad de los navegadores y que el artículo 45, en los términos propuestos, deja en manos de los navegadores la tarea de preservar y aplicar sus propios procedimientos y criterios con el fin de mantener y preservar la privacidad de las comunicaciones en línea utilizando el cifrado y otros métodos probados. La Comisión entiende que el proyecto de artículo 45 no impone obligaciones o restricciones a la manera en que los navegadores establecen conexiones cifradas con sitios web o autentican las claves criptográficas utilizadas al establecer dichas conexiones.

La Comisión recuerda que, de conformidad con el apartado 28 del Acuerdo interinstitucional entre el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea sobre la mejora de la legislación, de 13 de abril de 2016, la Comisión recurrirá a grupos de expertos, consultará a partes interesadas específicas y llevará a cabo consultas públicas, según proceda".

La conclusión a la que ineludiblemente cabe llegar es la rendición de la Comisión frente a la industria de los navegadores, un verdadero oligopolio vinculado al control criptográfico de un DNS, por lo que los certificados de autenticación de sitio web seguirán debiendo cumplir normas adicionales, quizá excepto en cuanto a su contenido, como condición para ser "admitidos".

Esta situación sólo puede solventarse mediante dos escenarios, que vienen debatiéndose los últimos años en foros como el ETSI TC ESI, donde se "cocinan" los estándares globales de servicios de confianza. El primer escenario, ya actualmente implantado, es el de continuidad; esto es, expedir un certificado de autenticación de sitio web que cumpla, de forma simultánea, tanto las exigencias legales del Reglamento eIDAS 2, como las exigencias del CAB/Forum y de los programas de Root CA de los navegadores. Ahí parece que la única mejora será el progresivo abandono de políticas como Extended Validation (EV) en favor de Domain Validation (DV), posiblemente mediante procedimientos de expedición altamente automatizados (basados en ACME) y la adopción de las reglas del Reglamento eIDAS a efectos de la verificación de la identidad del titular. DV vendría a garantizar el control del nombre de dominio, y eIDAS 2, la identidad civil del titular de dicho dominio.

El segundo escenario consistiría en recuperar una idea que hace unos años circula en ETSI, que es "convertir" el certificado de autenticación de sitio web en una suerte de certificado de atributo, que funcionaría de forma vinculada con el certificado DV a que me acabo de referir. El Reglamento eIDAS jamás exigió que el certificado de autenticación de servidor web incorporase clave pública alguna, por lo que no existiría inconveniente en acudir a este nuevo enfoque, lo que, de nuevo, en realidad queda en gran medida en manos de los navegadores.

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

LIVE STREAMING

Curso de
Doble Certificación

Continuidad de Negocio

BCI + ISO 22301

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación BCI Executive
- Certificación ISO 22301 Leader
- Módulo 7: MasterGEIT®

MGEIT® eGob®

Del 5 al 13 de julio

+ 34 96 109 44 44
campus@escueladegobierno.es

El nuevo servicio de confianza de archivo electrónico

El 11 de abril ha visto, finalmente, la firma del Reglamento eIDAS 2 por parte de los co-legisladores de la Unión, por lo que el mismo se encuentra ya únicamente pendiente de su publicación en el Diario Oficial de la Unión Europea.

Me he referido ya a diversas de las novedades de la reforma de la normativa de servicios de confianza de la Unión, incluyendo los libros mayores electrónicos (como *Blockchain*), la Cartera Europea de Identidad Digital, las declaraciones electrónicas de atributos o los certificados de autenticación de sitio web.

Este mes hablaremos de otra de las novedades importantes en el Reglamento, como es el nuevo servicio de confianza de archivo electrónico, que se define como el servicio que garantiza la recepción, el almacenamiento, la recuperación y la eliminación de datos electrónicos y documentos electrónicos para asegurar su durabilidad y legibilidad, así como para preservar su integridad, confidencialidad y prueba de origen durante todo el período de conservación (artículo 3.48 eIDAS modificado).

Se trata de una definición que amplía el anteriormente existente servicio de conservación de firma o sello electrónico; a saber, el uso de procedimientos y tecnologías capaces de ampliar la fiabilidad de los datos de la firma electrónica cualificada más allá del período de validez tecnológico (arts. 34 y 40 del Reglamento eIDAS) y que claramente conecta con algunas legislaciones nacionales, como la caja fuerte digital *(le coffre-fort numérique)* regulada en la francesa Ley n° 2016-1088 de 8 de agosto de 2016, o el archivo electrónico *(service d'archivage électronique)* de la belga Ley de 21 de julio de 2016, que admite cualificación, entre otras.

Resulta de extraordinaria importancia que el servicio se refiera a los datos y documentos electrónicos creados en forma digital, así como a los documentos en papel escaneados y digitalizados (Considerando 66 del Reglamento eIDAS 2), ya que ello permitirá, por primera vez en España, una verdadera digitalización sustitutiva de los documentos en papel en el sector privado, con reconocimiento pleno.

Como en otros servicios de confianza, existe una modalidad cualificada que debe cumplir los siguientes requisitos: a) ser prestado por prestadores cualificados de servicios de confianza; b) utilizar procedimientos y tecnologías capaces de asegurar la durabilidad y legibilidad de los datos y documentos electrónicos más allá del período de validez tecnológica y, al menos, durante el período de conservación legal o contractual, manteniendo al mismo tiempo su integridad y la exactitud de su origen; c) garantizar que dichos datos y documentos electrónicos se conserven de tal manera que queden protegidos contra su pérdida o alteración, excepto en el caso de los cambios relativos a su soporte o formato electrónico; d) permitir que las partes usuarias autorizadas reciban de forma automatizada un informe que confirme que los datos o documentos electrónicos recuperados de un archivo electrónico cualificado gozan de la presunción de integridad desde el inicio del período de conservación hasta el momento de su recuperación.

Sin embargo, la verdadera novedad es el establecimiento de efectos jurídicos.

En primer lugar, se garantiza el principio de no discriminación, en cuya virtud no se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a los datos electrónicos ni a los documentos electrónicos conservados mediante un servicio de archivo electrónico por el mero hecho de que estén en formato electrónico o no estén conservados mediante un servicio cualificado de archivo electrónico.

Por su parte, los datos electrónicos y documentos electrónicos conservados mediante un servicio cualificado de archivo electrónico gozarán de la presunción de su integridad y origen durante el período de conservación por el prestador cualificado de servicios de confianza, además de su reconocimiento transfronterizo en todos los demás Estados miembros.

CONTINÚA EN PRÓXIMA PÁGINA

Esta regulación, junto a las normas técnicas que deben referenciarse hacia mediados de 2025, a más tardar, permitirá completar las estrategias de entidades del sector privado que habían apostado por la digitalización del pasivo documental, y que se encontraban con el riesgo legal de eliminación del soporte papel por culpa de la legislación procesal española, que trata estas copias digitalizadas como copias reprográficas a cotejar con los originales para recibir valor probatorio pleno, debiendo, en caso de no estar disponibles, ser valoradas a la sana crítica.

Finalmente, y dada la conexión con las actividades de los archivos nacionales y las instituciones de la memoria, en su calidad de organizaciones dedicadas a la conservación del patrimonio documental en interés público, que suelen estar reguladas por el Derecho nacional y no prestan necesariamente servicios de confianza en el sentido del presente Reglamento, el Reglamento deberá entenderse sin perjuicio de su funcionamiento (Considerando 67 eIDAS 2), previsión plenamente razonable dado el marcado carácter mercatil, y tecnológico, de los servicios de confianza.

Se trata de una importantísima adición a la caja de herramientas de prueba electrónica del Reglamento eIDAS que ayudará a la eliminación de una de las barreras relevantes al negocio electrónico, como es el papel, sin tener que modificar las leyes procesales de cada uno de los 27 Estados miembros de nuestra muy diversa Unión Europea.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de
Doble Certificación

Gobierno de I&T

COBIT + ISO 38500

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación COBIT Executive
- Certificación ISO 38500 Leader
- Módulo 8: MasterGEIT®

MGEIT® eGob®

Del 6 al 14 de septiembre

+ 34 96 109 44 44
campus@escueladegobierno.es

El nuevo servicio de confianza de firma y sello en Nube

El 30 de abril se ha publicado en el Diario Oficial de la Unión Europea el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) nº 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital (Reglamento eIDAS 2), al vengo refiriéndome mayoritariamente en esta sección, habiendo entrado en vigor el pasado 20 de mayo.

Este mes hablaremos de otra de las novedades importantes en el Reglamento, que es el nuevo servicio de confianza de gestión de dispositivos de creación de firma electrónica a distancia o dispositivos de creación de sello electrónico a distancia (artículo 3.16.f) del Reglamento eIDAS modificado), frecuentemente conocido como firma o sello "en Nube".

Este servicio técnico se encuentra ampliamente extendido en la Unión Europea, dado que la redacción inicial del Reglamento eIDAS ya había autorizado que un prestador cualificado pudiera gestionar los datos de creación de firma electrónica cualificada o de sello electrónico cualificado por cuenta del firmante (persona física) o del creador de sellos (persona jurídica), estableciendo determinados requisitos para ello. Dado el modelo de catálogo cerrado de servicios de confianza, que no mencionaba esta actividad, la misma sólo podía realizarse por un prestador que ofreciera uno de los servicios de confianza que podían obtener la cualificación, normalmente la expedición de certificados cualificados de firma electrónica cualificada o de sello electrónico cualificado, o la expedición de sellos cualificados de tiempo electrónicos. La primera posibilidad resultaba bastante razonable, dado que ambas actividades se refieren a la gestión de claves del certificado y atendiendo al modelo de responsabilidad estricta contenido en el Reglamento eIDAS, no siendo quizá tan razonable acudir a la segunda opción, en especial porque las exigencias de seguridad de dicha expedición de sellos cualificados de tiempo electrónicos se encuentras bastante más alejados.

CONTINÚA EN PRÓXIMA PÁGINA

La principal novedad consiste en la regulación de esta actividad, como servicio de confianza específico e independiente de los restantes servicios de confianza; esto es, se trata de una actividad que ahora se puede ejercer de forma autónoma, sin necesidad de ofrecer otro servicio, por lo que abre el mercado, al tiempo que sujeta a los prestadores al régimen de supervisión del Reglamento eIDAS.

Siguiendo el modelo de doble nivel de intervención en la regulación de los servicios de confianza propio del Reglamento eIDAS, también en este caso nos encontramos ante un servicio que puede prestarse sin cualificación o con ella, en función de que el mismo cumpls los requisitos establecidos por el propio Reglamento para el servicio cualificado para la gestión de dispositivos cualificados de creación de firma electrónica a distancia (nuevo artículo 29 bis del Reglamento eIDAS modificado) y para el servicio cualificado para la gestión de dispositivos cualificados de creación de sello electrónico a distancia (nuevo artículo 39 bis del Reglamento eIDAS modificado).

Si bien en la modalidad cualificada la innovación legal es menor, en cambio en el caso de la prestación del servicio sin cualificación encontramos importantísimas novedades jurídicas, que van a producir un elevado impacto.

Y es que muchas entidades en España (y posiblemente en otros Estados) han adoptado el enfoque de la gestión centralizada de los certificados de firma electrónica avanzada de sus apoderados, empleados e, incluso, clientes, en especial en sus relaciones con las Administraciones Públicas, conforme a la normativa reguladora del procedimiento administrativo común. Y lo han hecho como han considerado apropiado, con base en sus propios requerimientos y contratos, de forma completamente autoregulada.

Desde el 20 de mayo de 2024, estas entidades han quedado sujetas al Reglamento eIDAS modificado, excepto cuando el servicio sea utilizado exclusivamente dentro de sistemas cerrados resultantes del Derecho nacional o de acuerdos entre un conjunto definido de participantes. Por tanto, cuando el servicio se ofrezca al público, en el mercado, dicha entidad siempre se encontrará sujeta al Reglamento.

Y ello implica que el prestador debrá cumplir con las obligaciones que impone el Reglamento en relación con los servicios no cualificados, como por ejemplo las obligaciones de seguridad procedimental y técnica previstas en el nuevo artículo 19 bis, y quedará plenamente sujeto a las potestades del órgano de supervisión, lo que incluye la potestad sancionadora, que permite la imposición de multas administrativas de hasta 5.000.000 euros a los prestadores, con o sin cualificación (nueva redacción del artículo 16, que desplaza el artículo 19 de la Ley 6/2020).

Finalmente, estas entidades deberán comunicar su actividad como prestador no cualificado al órgano de supervisión, conforme a lo establecido en el artículo 12 de la Ley 6/2020, antes del 20 de agosto, para su conocimiento y publicidad en la correspondiente sede electrónica.

Se trata de importantes novedades que, sin duda, contribuirán a la profesionalización de esta actividad del sector de prestación de servicios de confianza, pero que pueden conducir a que diversos prestadores decidan abandonar la actividad para no asumir los costes de cumplimiento.

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

LIVE STREAMING

Curso de
Doble Certificación

Gobierno Corporativo COSO + ISO 37000

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación COSO Executive
- Certificación ISO 37000 Executive
- Módulo 10: MasterGEIT®
- Módulo 1:0 MasterPPM®

MPPM® MGEIT® eGob®

Del 22 al 30 de noviembre

+ 34 96 109 44 44
campus@escueladegobierno.es

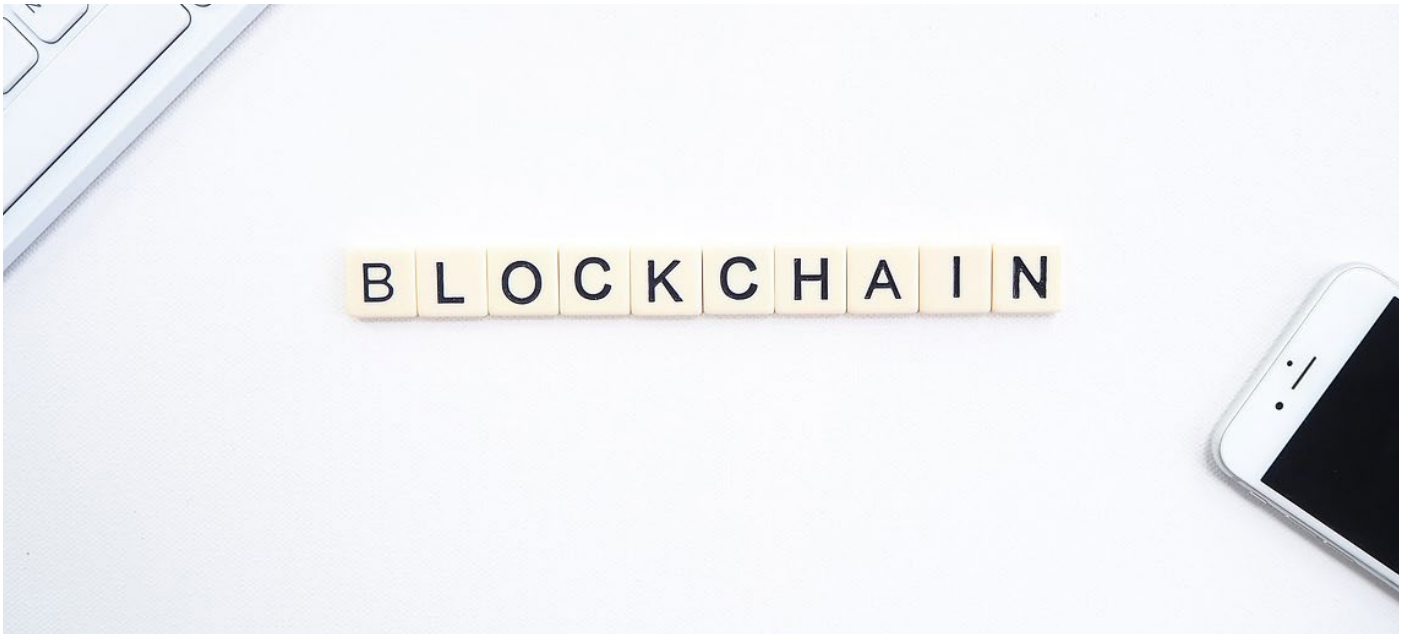
La Comisión Europea crea el consorcio para el blockchain europeo

El recientemente aprobado Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) nº 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital (Reglamento eIDAS 2), regula el nuevo servicio de confianza que denomina "libro mayor electrónico", que supone el primer reconocimiento jurídico general de las tecnologías de registro distribuido, como las cadenas de bloques (blockchains), innovación a la que ya me he referido en esta sección.

Esta novedad legislativa nació para dar cobertura jurídica al proyecto de cadena de bloques liderado por la Comisión Europea, veintiún Estados miembros de la Unión Europea y Noruega, a partir de la firma de la European Blockchain Partnership el 10 de abril de 2018, al que posteriormente se unirían otros ocho Estados, conocido como European Blockchain Services Infrastructure (EBSI).

Desde su inicio, el proyecto EBSI se ha centrado tanto en el despliegue de la infraestructura como en el desarrollo de casos de uso de la misma. EBSI ha desplegado una red piloto con más de 40 nodos repartidos por toda Europa para proyectos piloto, en particular en lo que respecta al intercambio y la verificación de credenciales relativas a ciudadanos u organizaciones en diversos sectores o áreas como la educación, el aprendizaje permanente y la seguridad social, de forma alineada con el marco europeo de identidad digital regulado en el propio Reglamento eIDAS 2, y que sustenta el Piloto de Gran Escala DC4EU. La Oficina de Propiedad Intelectual de la Unión Europea (EUIPO) también utiliza EBSI para poner a prueba acciones de lucha contra la falsificación, junto con otros casos de uso de trazabilidad.

CONTINÚA EN PRÓXIMA PÁGINA



Como parte del Programa Europa Digital, la Comisión ha financiado también la iniciativa EBSI Nodes Expansion (EBSI-NE), una iniciativa de colaboración entre 24 organizaciones de 14 Estados europeos, todas ellas reconocidas por su experiencia en tecnologías de registro distribuido y por iniciativas anteriores de EBSI. La misión principal de EBSI-NE es fortalecer la red EBSI mediante la adición de 18 nuevos nodos validadores a la red de producción y la prestación de servicios de soporte integrales a todas las partes interesadas relevantes de EBSI; con el objetivo de acelerar la adopción de la tecnología blockchain en toda Europa.

Precisamente en EBSI-NE se están realizando los trabajos preparatorios para la eventual cualificación de la red EBSI como servicio de confianza de libro mayor electrónico, lo que permitirá la aplicación de la presunción legal prevista en el Reglamento eIDAS 2; esto es, que los registros de datos contenidos en un libro mayor electrónico cualificado gozarán de la presunción de unicidad y exactitud de su orden cronológico secuencial y de su integridad.

Una de las dificultades identificadas en su momento para poder iniciar la prestación de servicios con base en EBSI fue la ausencia de un vehículo jurídico que pudiera obligarse contractualmente con los nodos, con los usuarios del servicio y responder frente a terceros. Ello es preciso, además, para disponer de una entidad con personalidad jurídica que pueda actuar como prestador de servicios de confianza, a los efectos del Reglamento eIDAS.

La solución a dicha dificultad ha venido de la mano de la creación, mediante la Decisión de Ejecución (UE) 2024/1432 de la Comisión, de 21 de mayo de 2024, por la que se crea el Consorcio Europeo de Infraestructuras Digitales para la Asociación Europea de Cadenas de Bloques y la Infraestructura Europea de Cadena de Bloques para los Servicios (EUROPEUM-EDIC).

El Consorcio Europeo de Infraestructuras Digitales (EDIC, en inglés) es un nuevo tipo de persona jurídica prevista en la Decisión (UE) 2022/2481 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 por la que se establece el programa estratégico de la Década Digital para 2030, que forma parte de los instrumentos de ejecución de proyectos plurianuales por parte de los Estados miembros.

El EDIC adquiere personalidad jurídica desde la entrada en vigor de la Decisión de la Comisión que los crea y tiene, en cada Estado miembro, la capacidad jurídica más amplia reconocida a las personas jurídicas por la legislación de dicho Estado miembro.

En el EUROPEUM-EDIC, acogido por Bélgica, participan Croacia, Chipre, Grecia, Italia, Luxemburgo, Portugal, Rumania y Eslovenia, mientras que Polonia ha manifestado su interés, y se ocupará de establecer y gestionar EBSI para prestar servicios transfronterizos a escala de la Unión, en particular servicios públicos, deapoyar la cooperación transfronteriza entre autoridades públicas en materia de tecnologías descentralizadas y de facilitar la interoperabilidad de las soluciones basadas en dichas tecnologías descentralizadas.

Cabe felicitarse por el éxito que supone este hito, que por fin ha de permitir disponer en Europa de cadenas de bloques fiables, resilientes y con valor jurídico pleno.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Doble Certificación en:

Gestión de Beneficios y Gestión de Portafolios

P4MGO!® BfM Leader
P4MGO!® PfM Leader

Dirección Académica:
Javier Peris

- Dos formatos para tu comodidad
- Opción A: Remoto en Directo
- Opción B: Virtual con Tutoría
- Metodología P4MGO!®
- Exámenes de Certificación Incluidos
- Certificación P4MGO!® BfM Leader
- Certificación P4MGO!® PfM Leader
- Solicita tu admisión

MPPM® MGEIT® eGob®

Próxima Convocatoria en Directo
Octubre 2024

Solicita tu admisión en:

+ 34 96 109 44 44
admisiones@escueladegobierno.es

P4MGO!

NUEVOS MASTERS

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