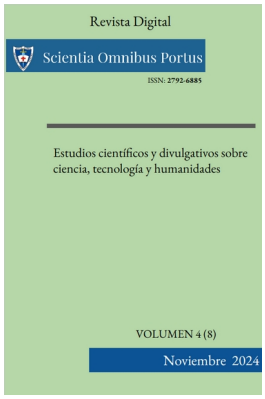
Scientia Omnibus Portus
ISSN: 2792-6885

https://iescelia.org/ojs



Artículo

Impacto de la Directiva NIS2 en los Prestadores de Servicios de Confianza

Tomás Hidalgo Salvador
S.I.A. (An Indra company)
thidalgo@sia.es

Resumen: Este artículo aborda el impacto de la Directiva NIS2 (Directiva 2022/2555), en los prestadores de servicios de confianza (TSP[1]) en el ámbito europeo, con especial enfoque en España. Analiza el rol de estas entidades en la transformación digital y la ciberseguridad, y detalla cómo la NIS2[2] amplía y refuerza los requisitos de seguridad en este sector. También se presentan los antecedentes regulatorios, desde la primera Ley de Firma Electrónica hasta el actual reglamento eIDAS, con su actualización del mes de mayo de 2024. Este marco normativo establece una base robusta para la seguridad y confianza en las transacciones electrónicas, pero con la adecuación de la Directiva NIS2 se busca consolidar una mayor resiliencia frente a los riesgos en el ámbito digital.

Palabras clave: eIDAS, NIS2, ETSI, "Prestador de Servicios de Confianza", TSP, Reglamento, Directiva, Trust

Introducción

Los prestadores de servicios de confianza desempeñan un papel esencial en la transformación digital tanto en España como en Europa. Actúan como garantes de la seguridad y la integridad de las transacciones electrónicas, facilitando servicios como la firma y sello electrónicos, el sellado de tiempo, la autenticación de sitios web, o la declaración electrónica de atributos; este último servicio, incluido en la actualización del Reglamento eIDAS (electronic IDentification, Authentication and trust Service) de mayo de 2024.

En España, el Reglamento Europeo eIDAS (Reglamento 910/2014), tras su entrada en vigor el 1 de julio de 2016, constituía el pilar fundamental para estandarizar y regular estos servicios, otorgando a los prestadores de servicios de confianza un papel clave en la digitalización segura. Estos actores no solo apoyan a las empresas -tanto públicas como privadas- en la adopción de procesos digitales, sino que también garantizan la interoperabilidad entre los Estados miembros, fomentando un mercado único digital más cohesionado.

Sin embargo, en un contexto de crecientes ciberamenazas, la necesidad de un marco más robusto de ciberseguridad llevaba a la Unión Europea a aprobar la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de

1 Del inglés, Trust Service Provider (TSP)
2 Del inglés, Network and Information Systems (NIS)

2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, conocida como NIS2 (Network and Information Security Directive). Esta directiva, que deroga la anterior directiva NIS, establece nuevos requisitos para los prestadores de servicios de confianza al ser tratados como entidades esenciales, ampliando las obligaciones relacionadas con la resiliencia operativa y la protección contra amenazas digitales.

Antecedentes

La regulación de los servicios de confianza en Europa ha seguido una evolución constante, marcada por hitos normativos que han sentado las bases de la confianza en el entorno digital. En este contexto, la Ley 59/2003 de Firma Electrónica en España, basada en la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, fue el primer marco normativo español que reguló la firma electrónica, y marcó un primer paso importante, aunque no exento de limitaciones, en el desarrollo de un marco jurídico para la digitalización. Su objetivo principal era fomentar la confianza en las transacciones electrónicas y facilitar la interoperabilidad entre los Estados miembros.

Como logros conseguidos por esta ley destaca el reconocimiento jurídico de la firma electrónica reconocida que, mediante un certificado digital reconocido y un dispositivo seguro de creación de firma, tenía el mismo valor jurídico que una firma manuscrita. O la interoperabilidad de las firmas electrónicas entre los Estados miembros a través de estándares técnicos que, si bien no lograron una integración completa, supuso un primer paso para eliminar barreras legales en las transacciones digitales transfronterizas.

Las carencias de esta directiva europea como, por ejemplo, la escasa adopción en el sector privado o una regulación centrada casi en exclusiva en la firma electrónica, dejando de lado otros servicios de confianza esenciales como el sello electrónico o el sello de tiempo, fueron las bases para un nuevo enfoque legislativo.

La llegada del Reglamento eIDAS (910/2014) en julio de 2016 marcó un punto de inflexión en la regulación de los servicios de confianza en Europa. Buscaba superar las limitaciones de su predecesora, armonizando las normativas en los Estados miembros y estableciendo un marco único para la interoperabilidad de los servicios de confianza y las transacciones electrónicas.

Uno de los logros más significativos del Reglamento eIDAS fue el reconocimiento y la regulación de los Prestadores de Servicios de Confianza Cualificados (QTSP). Estas entidades se convirtieron en actores clave en el ecosistema digital europeo, proporcionando servicios esenciales como la emisión de certificados cualificados para firmas y sellos electrónicos, el marcado de tiempo cualificado y la autenticación de sitios web. Además, los TSP se convirtieron en garantes de la interoperabilidad y la seguridad, facilitando la aceptación transfronteriza de los servicios de confianza en toda la Unión Europea.

En España, la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, derogó la Ley 59/2003, de firma electrónica, alineándose con el Reglamento eIDAS (UE 910/2014). Esta ley establecía un marco jurídico actualizado para firmas, sellos y otros servicios digitales, garantizando su validez en la Unión Europea y promoviendo la transformación digital con plena seguridad jurídica.

Así mismo, una adopción desigual entre estados miembros de la UE, una falta de usabilidad y accesibilidad, o el uso limitado el sistema de identificación electrónica, sentaron las bases para una actualización del reglamento eIDAS. Por ello, tras un proceso legislativo que incluyó debates y negociaciones durante tres años, el 20 de mayo de 2024 entraba en vigor 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) N.º 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital, conocido como eIDAS2.

Esta actualización del reglamento eIDAS busca ir más allá, integrando un sistema de identidad digital europea y reforzando la usabilidad y seguridad de los servicios de confianza. Con la introducción de la Cartera Europea de Identidad Digital, eIDAS2 pone el foco en que los ciudadanos sean los verdaderos dueños de su identidad digital, otorgándoles control total sobre sus datos personales y permitiéndoles gestionarlos de manera segura y transparente en toda la Unión Europea. Si bien queda fuera del ámbito de este artículo, los Prestadores de Servicios de Confianza Cualificados (QTSP) tendrán un papel fundamental en los servicios de emisión y validación de Declaración Electrónica de Atributos (QEEA[3]).

Prestadores de Servicios de Confianza (TSP)

Un Prestador de Servicios de Confianza, según el reglamento europeo eIDAS, es una entidad pública o privada que ofrece servicios electrónicos esenciales para garantizar la seguridad y la autenticidad en las transacciones digitales dentro del mercado único europeo. Estos servicios incluyen, entre otros, la emisión de certificados electrónicos, la firma y el sello electrónicos, el sellado de tiempo, la autenticación de sitios web y la conservación de firmas electrónicas. Por ejemplo, la Fábrica de Moneda y Timbre (FNMT), que emite de manera gratuita certificados digitales a personas físicas, o la Dirección General de la Policía (DGP), que emite el DNI Electrónico (DNIe) a los ciudadanos españoles, son ejemplos de prestador de servicios de confianza cualificados en España.

3 Del inglés, Qualified Electronic Attribute Attestation (QEEA)

Diferencias entre Servicios de Confianza No Cualificados y Cualificados

En el marco del Reglamento eIDAS y en su actualización eIDAS2, los servicios de confianza se clasifican en no cualificados y cualificados, siendo estos últimos aquellos que cumplen con los requisitos más estrictos establecidos por el reglamento (UE) 910/2014.

Los servicios de confianza no cualificados, aunque cumplen con los requisitos básicos del Reglamento eIDAS, no alcanzan el nivel más alto de seguridad y garantías jurídicas. Estos servicios están sujetos a ciertos controles y medidas, pero carecen del reconocimiento jurídico pleno en toda la Unión Europea. Entre sus características principales destacan:

- **Supervisión básica:** se encuentran supervisados por el organismo competente, pero no están sometidos a auditorías tan rigurosas como los servicios cualificados.
- **Sin reconocimiento transfronterizo pleno:** aunque son operativos, no disfrutan de la aceptación automática en todos los Estados miembros de la Unión Europea.
- **Menor nivel de seguridad:** sus requisitos técnicos y organizativos no son tan estrictos como los exigidos para los servicios cualificados.

Los servicios cualificados representan el nivel más alto de confianza y seguridad en el ecosistema eIDAS. Estos servicios están sujetos a estrictos controles y auditorías periódicas que garantizan su fiabilidad. Sus principales características son:

- **Seguridad jurídica:** gozan de reconocimiento legal pleno en toda la Unión Europea, lo que asegura su validez en transacciones electrónicas.
- **Auditorías periódicas:** deben someterse a evaluaciones cada 24 meses para confirmar su cumplimiento con los requisitos de eIDAS.
- **Etiqueta de confianza UE:** los servicios cualificados se identifican con esta etiqueta, que garantiza su fiabilidad y su conformidad con estándares técnicos y de seguridad rigurosos.
- **Interoperabilidad:** permiten la libre circulación de servicios digitales en la Unión Europea, favoreciendo las transacciones transfronterizas.

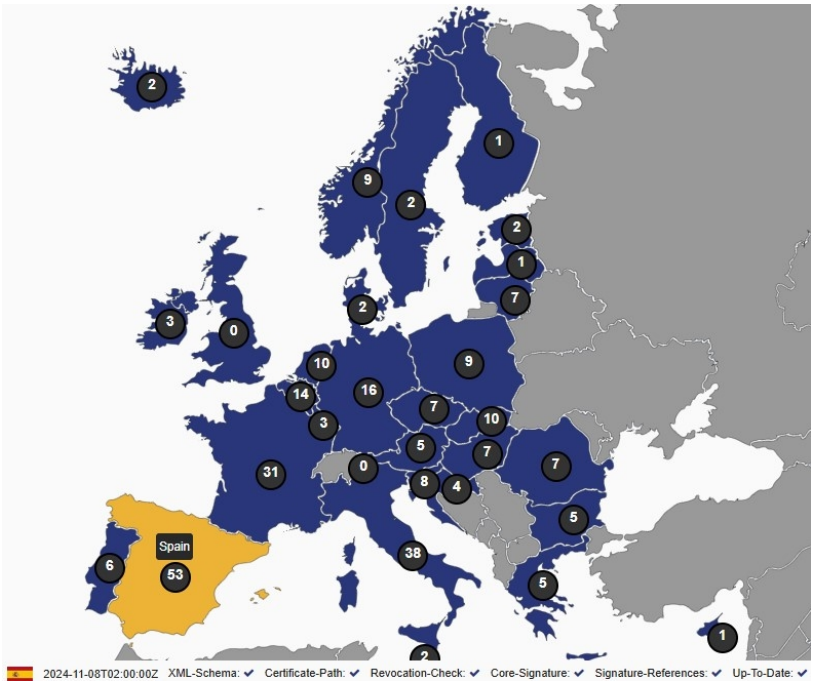


Figura 1. Mapa de QTSP por países. Fuente: https://www.eid.as/tsp-map/

Importancia de ser un TSP Cualificado

La cualificación en el marco del Reglamento eIDAS es un factor determinante para garantizar la confianza y seguridad en el ecosistema digital europeo. Esta condición de "cualificado" otorga a los servicios de confianza un reconocimiento legal pleno en toda la Unión Europea, asegurando a los usuarios que cumplen con los estándares técnicos y de seguridad más exigentes. La seguridad jurídica que ofrece esta cualificación refuerza la fiabilidad de las transacciones electrónicas, así como una mayor confianza en los usuarios -en gran medida, personas jurídicas- que utilizan estos servicios bajo un marco normativo sólido.

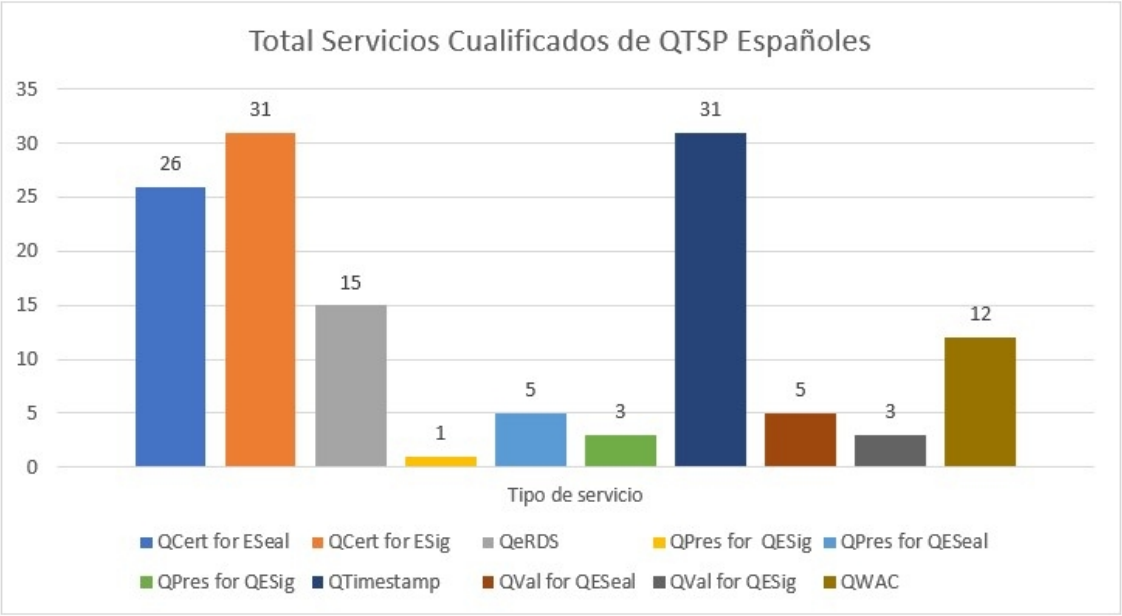


Figura 2. Servicios cualificados ofrecidos por los QTSP españoles

Además, la cualificación facilita la interoperabilidad entre los Estados miembros, permitiendo que los Prestadores de Servicios de Confianza Cualificados (QTSP) operen de forma transparente y sin barreras en el mercado único digital. En la actualidad, España está interconectada -a través del nodo eIDAS- con un total de 23 países para solicitar o proporcionar autenticación transfronteriza. Esto favorece la libre circulación de servicios digitales y fortalece las transacciones transfronterizas, simplificando los procesos para empresas y administraciones públicas. Al mismo tiempo, ser reconocido como QTSP ofrece ventajas competitivas significativas, ya que demuestra el cumplimiento de las normas jurídicas y de seguridad más estrictas, lo que posiciona a estos proveedores como actores de confianza y prestigio en el ámbito europeo.

Proceso de Cualificación de un Prestador de Servicios de Confianza bajo eIDAS

La cualificación de un Prestador de Servicios de Confianza (TSP) en el marco del Reglamento eIDAS consiste en un proceso riguroso para asegurar que los servicios ofrecidos cumplan con los estándares de seguridad y calidad en la Unión Europea. Este procedimiento incluye varias etapas clave, diseñadas para evaluar la conformidad técnica y organizativa del prestador.

El primer paso es la evaluación de la conformidad, realizada por un organismo acreditado de evaluación de conformidad. Este proceso, regido por estándares específicos como la norma ETSI[4] EN 319 403, examina si el prestador cumple con los requisitos técnicos y legales establecidos en el Reglamento eIDAS. Entre otros aspectos, se evalúan las políticas de seguridad, los procedimientos operativos, la infraestructura técnica y la capacidad del prestador para gestionar los servicios de confianza. En España, este rol de supervisión recae en la Entidad Nacional de Acreditación (ENAC), que garantiza que los organismos de evaluación, empresas privadas que ofrecen servicios de acreditación, realicen su trabajo bajo los más altos estándares de calidad y profesionalidad.

Una vez completada la evaluación, los resultados son revisados por el organismo supervisor nacional, que en el caso de España es competencia de la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital. Esta determina si el prestador cumple las condiciones necesarias para obtener el estatus de cualificado.

Tras conseguir la cualificación, se incluye al TSP en la Lista de Confianza Europea (EU Trusted List), otorgándole un reconocimiento oficial en toda la Unión Europea. Además, el prestador queda sujeto a una supervisión continua, que incluye auditorías obligatorias cada 24 meses para asegurar que siga cumpliendo con los requisitos establecidos.

Directiva NIS2

La Directiva NIS2 (Directiva 2022/2555), en vigor desde el 16 de enero de 2023, establece un marco normativo renovado para mejorar la ciberseguridad en la Unión Europea, con un enfoque en sectores esenciales, incluidas infraestructuras críticas, sanitarias, bancarias y digitales, entre otras. Su objetivo principal es garantizar un nivel uniforme y elevado de ciberresiliencia entre los Estados miembros. Para ello, se centra en tres pilares fundamentales:

1. **Fortalecer la resiliencia en sectores críticos:** la directiva NIS2 amplía su alcance a un mayor número de sectores clave, asegurando la protección de servicios esenciales frente a ciberamenazas.

4 Del inglés, European Telecommunications Standards Institute (ETSI)

2. **Reducir disparidades entre Estados miembros:** se busca armonizar las capacidades de ciberseguridad en toda la Unión Europea, eliminando las desigualdades entre mercados con diferentes niveles de preparación.
3. **Fomentar una respuesta coordinada:** promueve la colaboración transfronteriza mediante la notificación de incidentes y la adopción de normas comunes, asegurando una gestión eficaz de ciberamenazas.

NIS2 (Directiva 2022/2555)	
Sectores y entidades esenciales	**Sectores y entidades importantes**
Energía	Proveedores digitales
Transporte	Servicios postales y de mensajería
Banca	Gestión de residuos
Infraestructura del mercado financiero	Alimentación
Sanidad	Productos químicos
Servicios de agua	Investigación
Infraestructura digital	Fabricación
Gestores de servicios TIC	
Aguas residuales	
Servicios gubernamentales	
Aeroespacial	

Tabla 1. Sectores/Entidades esenciales e importantes definidos en la directiva NIS2.

El artículo 21 de la directiva NIS2 establece una serie de controles de ciberseguridad obligatorios que las entidades deben implementar para gestionar los riesgos asociados a sus sistemas de red e información. Estos controles incluyen:

1. **Análisis de riesgos y políticas de seguridad**: cada entidad debe realizar evaluaciones periódicas y adoptar políticas adecuadas para mitigar riesgos.
2. **Gestión de incidentes**: deben contar con procedimientos para prevenir, detectar y responder eficazmente a incidentes de ciberseguridad.
3. **Continuidad del negocio**: se exige desarrollar planes que garanticen la operatividad durante interrupciones y su pronta recuperación.
4. **Cifrado y autenticación**: uso de tecnologías que aseguren la integridad y confidencialidad de la información.
5. **Concienciación y formación**: capacitación del personal en buenas prácticas de seguridad.

La totalidad de requisitos mínimos y medidas para la gestión de riesgos de ciberseguridad del artículo 21 de la directiva NIS2 se pueden consultar en [3].

Proceso de trasposición de la Directiva NIS2

La Directiva NIS2, cuyo plazo de transposición venció el 17 de octubre de 2024, ha tenido una implementación desigual en los Estados miembros de la Unión Europea. Tan solo cuatro países, Bélgica, Hungría, Croacia y Letonia, lograron transponerla completamente dentro del plazo estipulado, cumpliendo con los requisitos exigidos. Otros Estados miembros, como Austria, Italia, y Polonia, avanzaron de manera significativa con la presentación de proyectos legislativos, pero no completaron el proceso en su totalidad. En el extremo opuesto, países como España, Portugal y Bulgaria apenas han iniciado el desarrollo de los borradores legislativos necesarios para su implementación.

Ante este escenario previsible de falta de uniformidad en la armonización de las normativas de ciberseguridad a nivel europeo, la comisión europea publicaba el mismo 17 de octubre de 2024 las primeras normas de implementación bajo la Directiva NIS2; es decir, "aterrizaba" el contenido de la ley en diversos requerimientos técnicos y metodológicos enfocados a fortalecer la ciberseguridad de las entidades relevantes en la UE.

En este sentido, ENISA[5] (Agencia de Ciberseguridad de la Unión Europea) ha desarrollado una guía técnica (Implementation guidance on NIS 2 security measures) para apoyar a los Estados miembros de la UE y a las entidades en la implementación de los requisitos técnicos y metodológicos establecidos por el Reglamento de Ejecución (UE) 2024/2690 de la Directiva NIS2. El objetivo principal de esta guía consiste en proporcionar explicaciones adicionales sobre los conceptos legales, ejemplos de evidencias que demuestren el cumplimiento de los requisitos y tablas que relacionan las exigencias normativas con estándares europeos, internacionales y marcos nacionales. Por ejemplo, se mapean los controles del Reglamento de Ejecución (UE) 2024/2690 con las medidas de protección definidas en el anexo II del Esquema Nacional de Seguridad (ENS).

5 Del inglés, European Union Agency for Cybersecurity

Por otro lado, si bien la directiva establece la obligatoriedad de auditorías periódicas, específicas o ad hoc tras incidentes significativos, al no existir una trasposición, esta falta de regulación nacional impide definir con claridad las fechas, frecuencias y requisitos concretos, dificultando la planificación por parte de las entidades esenciales e importantes. En el caso de los Prestadores de Servicios de Confianza (TSP), serán a través de las auditorías de cumplimiento eIDAS, por su mapeo con la norma ETSI EN 319 401, la manera de verificar la implantación real de las medidas de ciberseguridad exigidas por la normativa europea.

Relación entre eIDAS2 y NIS2: Prestadores de Servicios de Confianza como Entidades Esenciales

Con la llegada de eIDAS2, la actualización del Reglamento eIDAS introduce un marco normativo más ambicioso y alineado con las necesidades actuales del ecosistema digital europeo. Uno de los cambios más significativos es la relación directa que establece entre la seguridad de los Prestadores de Servicios de Confianza (TSP) y la nueva Directiva NIS2 (Directiva 2022/2555), que regula la ciberseguridad en Europa.

El artículo 19 del Reglamento eIDAS2 establece que los Prestadores de Servicios de Confianza cualificados estarán sujetos a medidas de seguridad más estrictas, con el fin de garantizar la confianza, integridad y disponibilidad de los servicios. Dicho artículo hace una referencia explícita a la Directiva NIS2, destacando que los TSP deben cumplir con los requisitos de seguridad aplicables a las entidades esenciales, categoría en la que han sido incluidos por la NIS2.

La Directiva NIS2 amplía el alcance de la regulación de ciberseguridad, clasificando a los TSP como entidades esenciales que ofrecen servicios de naturaleza crítica, al englobarlos dentro del sector "Infraestructura digital" [ver tabla.1]. Entre estos servicios se incluyen la emisión de certificados cualificados, el marcado de tiempo y la autenticación de sitios web, cuya seguridad y disponibilidad son fundamentales para el funcionamiento del mercado único digital. Como entidades esenciales, los TSP deben implementar, entre otras, las siguientes medidas de seguridad bajo la NIS2:

1. **Gestión de riesgos**: adoptar políticas avanzadas de gestión de riesgos de ciberseguridad que incluyan planes para prevenir, detectar y responder a incidentes.
2. **Notificación obligatoria de incidentes**: informar de cualquier incidente de seguridad significativo a las autoridades competentes dentro de plazos definidos, facilitando la respuesta coordinada a ciberamenazas.
3. **Resiliencia operativa**: garantizar la continuidad de los servicios esenciales ante ataques o fallos tecnológicos.
4. **Colaboración internacional**: participar en redes de cooperación transfronteriza para la gestión de ciberamenazas.

Para los TSP, este marco implica nuevas obligaciones operativas y técnicas, pero también aumenta su fiabilidad y prestigio como garantes de confianza en la digitalización europea. Esta sinergia entre eIDAS2 y NIS2 asegura la continuidad y resiliencia de los servicios esenciales en un contexto de crecientes amenazas.

Normas Técnicas ETSI: pilar de la conformidad y seguridad

Las normas técnicas ETSI constituyen un conjunto de estándares desarrollados por el Instituto Europeo de Normas de Telecomunicaciones (ETSI), una organización independiente reconocida internacionalmente por su labor en la elaboración de directrices técnicas en telecomunicaciones, tecnologías de la información y servicios digitales. Estas normas establecen requisitos claros y uniformes que aseguran la interoperabilidad, calidad y seguridad de sistemas y servicios en el mercado europeo.

El objetivo principal de las normas ETSI es proporcionar un marco técnico que facilite la conformidad con las regulaciones europeas y promueva la confianza en los servicios tecnológicos. Para asegurar el cumplimiento de estándares de calidad y seguridad requeridos, las normas ETSI se utilizan como referencia para la evaluación de conformidad o para la supervisión continua de servicios, entre otros. Desarrolladas por expertos de la industria, administraciones públicas y organismos reguladores, estas normas garantizan que las especificaciones respondan a las necesidades técnicas y operativas del mercado. Por ejemplo, hay normas ETSI que definen los requisitos técnicos para las Telecomunicaciones 4G/5G (ETSI EN 301 908), o para los requisitos de seguridad para dispositivos de Internet de las Cosas (IoT) (ETSI EN 303 645).

En el caso de los Prestadores de Servicios de Confianza (TSP), estas normas proporcionan un marco esencial para garantizar la seguridad jurídica y técnica de los servicios definidos por el reglamento eIDAS. Por ejemplo, las especificaciones técnicas de un certificado digital para realizar firmas, o los requerimientos para una video identificación remota de un usuario para emitir un certificado digital. Algunas de las normas más relevantes que aplican a los TSP se detallan a continuación:

- **ETSI EN 319 401**: define los requisitos generales de política y seguridad aplicables a los TSP.
- **ETSI EN 319 403**: regula los criterios para la evaluación de conformidad de los TSP, siendo esencial para los procesos de auditoría.
- **ETSI EN 319 411-1 y 319 411-2**: establecen los requisitos específicos para los TSP que emiten certificados cualificados y no cualificados, incluyendo aspectos de gestión operativa y técnica.
- **ETSI EN 319 421**: cubre los requisitos para servicios de sellado de tiempo cualificado.

- **ETSI EN 319 412**: detalla los perfiles de certificados electrónicos para personas físicas, jurídicas y sitios web.

ETSI EN 319 401: La reina indiscutible de las normas para los TSP

La norma ETSI EN 319 401 establece los requisitos generales de política y seguridad aplicables a los Prestadores de Servicios de Confianza (TSP), y proporciona un marco técnico y organizativo para garantizar que sus servicios sean seguros, confiables e interoperables. Esta norma sirve como referencia fundamental para la implementación de servicios regulados bajo el Reglamento eIDAS, asegurando el cumplimiento de los estándares europeos.

Los requisitos definidos en la ETSI EN 319 401 cubren aspectos clave de la gestión de los TSP, incluyendo:

- **Gestión de riesgos**: exige la identificación, evaluación y mitigación de riesgos relacionados con la operación de los servicios de confianza.
- **Políticas y procedimientos organizativos**: detalla la necesidad de documentar políticas de seguridad claras, que definan las responsabilidades y procedimientos para la prestación de los diferentes servicios ofertados.
- **Resiliencia operativa**: incluye requisitos para garantizar la continuidad del negocio y la recuperación ante incidentes que puedan afectar la operación de los servicios.
- **Protección de datos y activos**: establece controles para asegurar la confidencialidad, integridad y disponibilidad de los datos procesados por los TSP.
- **Auditoría y supervisión**: obliga a la implementación de mecanismos de control interno y externo para verificar el cumplimiento continuo de la norma.

Así mismo, la norma se actualiza periódicamente para incorporar avances tecnológicos y requisitos regulatorios, como los introducidos por la Directiva NIS2. Además de asegurar la conformidad con el Reglamento eIDAS, esta norma ETSI también fomenta la confianza y la seguridad de los actores en el ecosistema digital europeo.

Estructura de la norma ETSI TS 319 401		
5. Risk Assessment	5. Risk Assessment [5]	
6. Policies and practices	6.1 Trust Service Practice statement [11]	
	6.2 Terms and Conditions [6]	
	6.3 Information security policy [7]	
7. TSP management and operation	7.1 Internal organization [7]	7.1.1. Organization reliability [6]
		7.1.2 Segregation of duties [1]
	7.2 Human resources [19]	
	7.3 Asset Management [12]	7.3.1 General requirements [2]
		7.3.2 Assets inventory and classification [7]
		7.3.3 Storage media handling [3]
	7.4 Access Control [13]	
	7.5 Cryptographic controls [1]	
	7.6 Physical and environmental security [5]	
	7.7 Operation security [10]	
	7.8 Network security [21]	
	7.9 Vulnerabilities and Incident management [27]	7.9.1 Monitoring and logging [5]
		7.9.2 Incident response [12]
		7.9.3 Reporting [4]
		7.9.4 Event assessment and classification [2]
		7.9.5 Post-incident reviews [4]
	7.10 Collection of evidence [8]	
	7.11 Business continuity management [13]	7.11.1 General [2]
		7.11.2 Backup [4]
		7.11.3 Crisis management [7]
	7.12 TSP termination and termination plans [11]	
	7.13 Compliance [5]	
	7.14 Supply chain [31]	7.14.1 Supply chain policy [4]
		7.14.2 Supply chain procedures and processes [15]
		7.14.3 Responsibility, third parties agreements and SLA [12]
(*) Entre corchetes, el nº de controles		

Tabla 2. Estructura ETSI TS 319 401

Norma ETSI TR 119 404: primera adaptación de ETSI EN 319 401 a NIS2

En febrero de 2023, tras la entrada en vigor de la Directiva NIS2 el 16 de enero de 2023, se publicaba la norma ETSI TR 119 404 (NIS2 and its impact on eIDAS standards) como respuesta a los nuevos requerimientos de la Directiva NIS2 y su impacto en los estándares aplicables a los Prestadores de Servicios de Confianza (TSP) bajo el Reglamento eIDAS. En ella se identificaban las áreas donde los controles establecidos en el estándar ETSI EN 319 401 necesitaban ser ampliados o adaptados para alinearse completamente con las exigencias de la NIS2. Si bien ya abarcaba en gran medida los principios de gestión de

riesgos y ciberseguridad establecidos por la NIS2, ciertos aspectos como, por ejemplo, la seguridad en la cadena de suministro y la gestión avanzada de vulnerabilidades, requerían mayor detalle y desarrollo.

La publicación de este informe marcó un paso crítico en la preparación de los TSP para cumplir con las nuevas exigencias regulatorias y asegurar que puedan ofrecer servicios seguros y confiables mientras se adaptan a un entorno normativo en constante evolución. Su adopción temprana permitió a los supervisores y prestadores identificar gaps antes de la implementación definitiva de la NIS2 y su integración en el eIDAS2.

Actualización del ETSI EN 319 401: cumplimiento con los Requisitos de la NIS2

En junio de 2024, la versión v3.1.1 de la norma ETSI EN 319 401 (General Policy Requirements for Trust Service Providers) alineaba sus controles estándares técnicos con los requerimientos de la Directiva NIS2. La actual versión incorpora controles específicos diseñados para reforzar ciberseguridad de los Prestadores de Servicios de Confianza (TSP), tratados como entidades esenciales bajo la NIS2.

El Artículo 21 de la NIS2 especifica una serie de controles que incluyen la gestión de riesgos de ciberseguridad, la continuidad del negocio, y la respuesta y notificación ante incidentes, entre otros. La norma ETSI EN 319 401 ha mapeado estos controles a sus cláusulas principales, garantizando que los TSP puedan demostrar conformidad tanto con el eIDAS2 como con la NIS2. Esto mapeo realizado incluye:

- **Gestión de riesgos**: requisitos detallados en la norma para identificar, evaluar y mitigar riesgos relacionados con los servicios de confianza.
- **Seguridad en la cadena de suministro**: controles sobre proveedores y terceros, incluyendo acuerdos de nivel de servicio (SLA) y auditorías periódicas para asegurar la seguridad en todos los niveles de la operación.
- **Continuidad del negocio**: planificación de recuperación ante desastres, copias de seguridad y gestión de crisis como parte de las políticas de resiliencia operativa.
- **Notificación y manejo de incidentes**: procesos claros para la notificación a las autoridades competentes y la gestión interna de incidentes.

La actualización de la ETSI EN 319 401 refuerza significativamente la ciberseguridad de los Prestadores de Servicios de Confianza (TSP), introduciendo un total de 70 nuevos requisitos (NR) distribuidos en puntos clave.

ETSI TS 319 401	
Change Type	Controls
Unchanged	123
NR (New Requirement)	70
PC (Partially Changed)	10
NCT (New Content)	7

Tabla 3. Tipo de cambio en los controles de ETSI 319 401 v.3.1.1

Uno de los más impactados es el "7.14 Supply Chain", con 26 nuevos controles orientados a gestionar los riesgos asociados a la cadena de suministro, considerada como un componente crítico de la infraestructura digital. Esta actualización pone un énfasis especial en la necesidad de establecer políticas, procedimientos y procesos robustos para garantizar la seguridad en cada eslabón de la cadena. Los nuevos controles incluyen la formalización de auditorías regulares a proveedores, la inclusión de cláusulas específicas de seguridad en los contratos y la monitorización continua de los servicios externos. Estas medidas reflejan un compromiso con las directrices de la Directiva NIS2, que subraya la importancia de una gestión proactiva y estructurada de la cadena de suministro como elemento esencial para proteger los servicios esenciales frente a vulnerabilidades externas y amenazas emergentes.

Area	Control	Description
7.11.2 Backup	**REQ-7.11.2-01**	The TSP shall maintain backup copies of information and sufficient resources, including facilities, network and information systems as well as personnel in accordance with risk assessment and business continuity plan.
7.11.2 Backup	**REQ-7.11.2-02**	The TSP shall define backup plans taking into account at least the following: **a)** recovery times; **b)** assurance of the backup copies completeness and accuracy (including configuration data and information stored in cloud service environment); **c)** storage of backup copies at a safe location or locations which are outside the network of the system backed up and are at sufficient distance to escape any damage from a disaster at the main site; **d)** physical/environmental and logical controls for backup copies in accordance with their information classification level; and **e)** processes for restoring information from backup copies (including approval processes).
7.11.2 Backup	**REQ-7.11.2-03**	The TSP shall perform integrity check on the backup copies.
7.11.2 Backup	**REQ-7.11.2-04**	The TSP shall test at planed intervals the recovery of backup copies and redundancies and shall take corrective actions in case of findings. The results of these tests shall be documented.

Tabla 4. Ejemplo de nuevos controles incluidos en la ETSI TS 319 401

Otro punto modificado en profundidad es el "7.9 Vulnerabilities and Incident Management", con 15 nuevos requisitos enfocados en la detección, análisis y respuesta a vulnerabilidades e incidentes. Estos cambios refuerzan la resiliencia de los TSP al establecer protocolos avanzados para la gestión de incidentes, desde la clasificación inicial hasta la notificación rápida a las autoridades competentes.

Además, los puntos "7.3 Asset Management" y "7.11 Business Continuity Management", con 7 nuevos controles cada uno, introducen medidas más estrictas para garantizar la identificación y protección de activos críticos, así como la continuidad operativa ante fallos o ciberataques.

Conclusiones

La integración de la Directiva NIS2 con el marco regulatorio de eIDAS y las normas ETSI marca un hito significativo en la consolidación de un ecosistema digital europeo más seguro y resiliente. Como entidades esenciales bajo la NIS2, los Prestadores de Servicios de Confianza Cualificados (QTSP) refuerzan sus requisitos de seguridad mediante controles específicos. Dichos controles aseguran la continuidad operativa, la gestión de riesgos y la protección frente a ciberamenazas. Cabe destacar que, ante futuras auditorías de cumplimiento eIDAS realizadas por entidades acreditas por ENAC, los QTSP deberán demostrar la implementación efectiva de estos nuevos requisitos y controles.

El Reglamento eIDAS2, con su artículo 19, establece un puente directo hacia las exigencias de la NIS2, destacando la importancia de un enfoque integrado en la gestión de ciberseguridad. Este marco actualizado exige que los TSP no solo cumplan con los estándares tradicionales de confianza y calidad, sino que también implementen medidas avanzadas que incluyan, entre otros, la gestión de vulnerabilidades, la monitorización continua de la cadena de suministro o la notificación de incidentes. Este enfoque, alineado con las normas ETSI EN 319 401 incorpora controles específicos basados en los requisitos de la NIS2.

Las normas ETSI, como las series 319 401 y 319 403, desempeñan un papel central en la estandarización técnica, y proporcionan directrices claras que garantizan la interoperabilidad y el cumplimiento regulatorio en toda la Unión Europea. Además, iniciativas como la guía técnica desarrollada por ENISA ofrecen herramientas prácticas para facilitar la implementación de estos requisitos y fortalecer la seguridad en sectores críticos.

Por último, la convergencia de las normas eIDAS, ETSI y NIS2 no sólo refuerza la confianza en los TSP, sino que también posiciona a Europa como líder en la protección de su infraestructura digital y la resiliencia en el entorno digital europeo.

Referencias bibliográficas

[1]. Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, sobre la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (2014). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32014R0910

[2]. Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (2024). https://eur-lex.europa.eu/eli/reg/2024/1183/oj

[3]. Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión. https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A32022L2555

[4]. Ley 59/2003, de 19 de diciembre, de firma electrónica (2003). https://www.boe.es/eli/es/l/2003/12/19/59/con

[5]. Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza (2020). https://www.boe.es/eli/es/l/2020/11/11/6/con

[6]. ETSI. Electronic Signatures and Trust Infrastructures Activities. https://portal.etsi.org/TB-SiteMap/esi/esi-activities

[7]. eIDAS – The Ecosystem. https://www.eid.as/

[8]. Secretaría de Estado de Digitalización e Inteligencia Artificial. (2024, noviembre 12). Servicios electrónicos de confianza. https://avance.digital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/FirmaElectronica.aspx

[9]. European Commision. EU/EEA Trusted List Browser. https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls

[10]. Secretaría de Estado de Digitalización e Inteligencia Artificial. Prestadores de servicios electrónicos de confianza no cualificados. https://sedeaplicaciones.minetur.gob.es/Prestadores/Inicio.aspx?opcion=nc#

[11]. Secretaría de Estado de Digitalización e Inteligencia Artificial. Prestadores de servicios electrónicos de confianza cualificados. https://sedeaplicaciones.minetur.gob.es/Prestadores/Inicio.aspx

[12]. SANS. NIS2 Directive Readiness: Compliance, Challenges, and Recommendations. (2024). https://www.sans.org/white-papers/nis2-directive-readiness-compliance-challenges-recommendations/

[13]. European Commision. New rules to boost cybersecurity of EU's critical entities and networks. (2024, octubre 17). https://digital-strategy.ec.europa.eu/en/news/new-rules-boost-cybersecurity-eus-critical-entities-and-networks

[14]. ENISA. Implementation guidance on NIS 2 security measures - Draft for Consultation. (2024, noviembre 07). https://www.enisa.europa.eu/publications/implementation-guidance-on-nis-2-security-measures

[15]. The NIS2 directive in EU: A country-by-country breakdown. (2024, Octubre 18). https://www.truid.app/blog/the-nis2-directive-in-eu-a-country-by-country-breakdown

[16]. ENAC. Entidad Nacional de Acreditación. (2024). https://www.enac.es/

Biografía

Tomás Hidalgo Salvador es Ingeniero Técnico en Informática por la Universidad de Almería con más de 25 años de experiencia laboral en las áreas de TI, Ciberseguridad y Auditoría de riesgos tecnológicos en entornos bancarios. En la actualidad trabaja como auditor interno de cumplimiento en el área de Digital Identity & Signature de la empresa SIA (An Indra Company), entidad que es Prestadora de Servicios de Confianza Cualificados bajo el reglamento eIDAS.