ASEPEC

LOS PRESTADORES CUALIFICADOS DE SERVICIOS DE CONFIANZA: ALIADOS ESTRATÉGICOS EN EL CUMPLIMIENTO DEL REGLAMENTO DORA

El Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, conocido como Reglamento DORA, tiene como objetivo establecer un elevado nivel común de resiliencia operativa digital en el sector financiero europeo, abordando los riesgos relacionados con las tecnologías de la información y la comunicación (TIC). La creciente digitalización de este sector, aunque beneficiosa, también aumenta la vulnerabilidad a las ciber-amenazas, lo que hace esencial una gestión eficaz de estos riesgos.

DORA establece un conjunto armonizado de requisitos y obligaciones a las entidades financieras, con enfoque en la gestión de riesgos tanto internos como externos. Las entidades financieras deben gestionar los riesgos derivados de su propia actividad y de sus relaciones con terceros, especialmente con proveedores de servicios TIC.

En este escenario, los Prestadores Cualificados de Servicios de Confianza (PCSC) pueden tener un rol relevante en ayudar a las Fintech a cumplir los requisitos establecidos por DORA, y liberarlas de la necesidad de supervisión adicional a estos proveedores.

Entre las principales ventajas que ofrecen se enumeran las siguientes:

1. Certificaciones de cumplimiento de estrictos estándares de seguridad y calidad

Los PCSC respaldan sus operaciones en certificaciones de conformidad emitidas por organismos independientes de evaluación acreditados, que verifican el cumplimiento de estrictos estándares de seguridad y calidad, conforme al Reglamento 2014/910, modificado por el Reglamento (UE) 2024/1183, en lo que respecta al establecimiento del marco europeo de identidad digital (en adelante Reglamento eIDAS), así como otros requisitos tecnico-jurídicos y de organización complementarios, establecidos en estándares técnicos internacionales, definidos por organismos internacionales de normalización como ETSI y CEN.

2. Supervisión continua por organismos nacionales competentes

El ciclo de vida de las operaciones de los PCSC y hasta el cese de los servicios es supervisado por Organismos Nacionales competentes definidos por cada Estado Miembro de la UE que intervienen también en el proceso administrativo de acreditación como PCSC. La superación de manera favorable de este proceso les habilita para integrarse en las Lista Europea de prestadores cualificados de servicios de confianza (TSL) y para utilizar la etiqueta de confianza de la Unión Europea para los servicios de confianza conforme al Reglamento de Ejecución (UE) 2015/806.

3. Reducción de procesos de homologación de proveedores

La posesión de estas certificaciones de conformidad emitidas por auditores externos independientes, la supervisión continua de organismos nacionales competentes y la etiqueta de confianza de la Unión Europea, refuerzan la seguridad y fiabilidad de los servicios cualificados de confianza, reduciendo la necesidad de largos cuestionarios y verificaciones en procesos de homologación de proveedores.

4. Cumplimiento del requisito de auditorías independientes

La acreditación como PCSC debe mantenerse en el tiempo y requiere superar auditorías de recertificación cada dos años, con auditorías de mantenimiento del servicio realizadas anualmente. En la práctica, los Prestadores Cualificados de Servicios de Confianza son auditados todos los años y la supervisión del organismo nacional competente sobre su actividad es constante. En este caso al contar con un Prestador Cualificado de Servicios de Confianza (PCSC) como proveedor, las entidades financieras no necesitarían realizar auditorías ni cuestionarios adicionales sobre ellos para cumplir con los requisitos de auditoría independiente y evaluación de seguridad periódica establecidos en DORA.

5. Gestión y notificación de incidentes

Los PCSC disponen de procesos consolidados para la gestión y notificación de incidentes que permiten apoyar y colaborar con las Fintech en el cumplimiento de las obligaciones de DORA en este ámbito.

6. Alta disponibilidad y resiliencia operativa

Los requisitos de alta disponibilidad que deben cumplir los prestadores de servicios de confianza apoyan el cumplimiento de los requisitos de DORA para la resiliencia operativa de las Fintech. Si bien este requisito debe ser abordado de manera integral para todas las operaciones de las Fintech, en aquellos componentes del servicio en los que intervenga un PCSC auditado se facilita su cumplimiento y se reduce la necesidad de verificaciones y auditorías adicionales.

7. Servicios alineados con normativa europea de ciberseguridad Directiva (UE) 2022/2555 (Directiva NIS2)

La Directiva NIS2 tiene un impacto directo en los PCSC al ser considerados como infraestructuras críticas. Las obligaciones y controles de ciberseguridad de NIS2 se han incorporado a la norma técnica aplicable a todos los PCSC, el estándar ETSI EN 319 401 v.3.1.1 (2024-06). Este cumplimiento refuerza su análisis y gestión de riesgos, así como la detección y respuesta ante incidentes, y garantiza la continuidad del servicio, se fortalecen las medidas de controles de acceso, seguridad física y lógica, y la gestión de la configuración y backups de respaldo.

Asimismo, se establecen obligaciones de propagar los requisitos de seguridad del PCSC a lo largo de su cadena de suministro y dependencias. Dado que los PCSC ya incorporan estas exigencias normativas europeas, las entidades financieras no necesitan realizar auditorías adicionales ni someterlos a supervisiones propias para validar el cumplimiento de sus requisitos de ciberseguridad.

En conclusión, los Prestadores Cualificados de Servicios de Confianza Cualificados desempeñan un papel fundamental en el sector financiero al garantizar el cumplimiento de las normativas de ciberseguridad y resiliencia operativa establecidas por el Reglamento DORA y la Directiva NIS2. Gracias a sus rigurosos procesos de certificación y supervisión continua, **las entidades financieras pueden confiar en que sus proveedores de servicios de confianza ya cumplen con los estándares exigidos**, lo que les permite concentrarse en sus operaciones sin la carga de auditorías y verificaciones adicionales. Esto no solo mejora la eficiencia operativa, sino que también fortalece la seguridad y la gestión de riesgos en un entorno digital cada vez más complejo.

ASEPEC

C/Serrano 69, Madrid. ECIJA HQ
info@asepec.es