MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

DIRECCIÓN GENERAL DE ORDENACIÓN DE LOS SERVICIOS DE DIGITALIZACIÓN Y DE COMUNICACIÓN AUDIOVISUAL

SUBDIRECCIÓN GENERAL
PARA LA SOCIEDAD DIGITAL

NOTA SOBRE LA MIGRACIÓN DEL ALGORITMO RSA

La Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, establece en su artículo 14 que el Ministerio para la Transformación Digital y de la Función Pública *"como órgano de supervisión, controlará el cumplimiento por los prestadores de servicios electrónicos de confianza cualificados y no cualificados que ofrezcan sus servicios al público de las obligaciones establecidas en el Reglamento (UE) 910/2014 y en esta Ley", y "podrá acordar las medidas apropiadas para el cumplimiento del Reglamento (UE) 910/2014 y de esta Ley."*

En este sentido, este órgano de supervisión establece que los prestadores de servicios de confianza, cualificados y no cualificados, que emplean algoritmos RSA para la prestación de servicios de confianza, deben cumplir con lo establecido por el Centro Criptológico Nacional, en el **Anexo 1- Prestadores de Servicios de Confianza** que acompaña a la Guía de Seguridad de las TIC CCN-STIC 807 Criptología de Empleo en el Esquema Nacional de Seguridad teniendo en cuenta los siguientes aspectos:

1. Prestadores de servicios de confianza cualificados

En relación con las adaptaciones que los prestadores de servicios de confianza cualificados deban acometer en virtud del cumplimiento del citado Anexo, este órgano supervisor determina que el **impacto en la migración del algoritmo RSA con longitud de claves inferiores a 3000 bits es significativo, requiriéndose por tanto que**, conforme a lo establecido en el artículo 24.2 a) del Reglamento (UE) nº 910/2014, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior, modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, en lo que respecta al establecimiento del marco europeo de identidad digital, **el prestador debe remitir, al menos**:

Un informe técnico (IT) elaborado por un Organismo de Evaluación de la Conformidad acreditado por una Entidad Nacional de Acreditación, certificando que el cambio se ha realizado adecuadamente, así como la idoneidad de los algoritmos utilizados, incluyendo su conformidad con los estándares de seguridad vigentes.

El informe técnico deberá aportar como mínimo la **evidencia del hito de celebración de la ceremonia de generación de claves criptográficas.**

C/ POETA JOAN MARAGALL, 41
CP 28020 MADRID
E-mail: LFE@digital.gob.es

No obstante, para aquellos prestadores cualificados que tengan **previsto realizar una auditoría anual o bienal con anterioridad al 31 de diciembre de 2026**, **se dará por válido el informe de evaluación de la conformidad** (CAR) **resultante de la misma y su IT asociado**, siempre y cuando en este último vengan recogidos todos los aspectos mencionados en el texto enmarcado, no siendo necesario aportar ningún documento adicional.

2. Prestadores de servicios de confianza no cualificados

Se recuerda que el artículo 15 de la Ley 6/2020 atribuye a este Ministerio la potestad de realizar las actuaciones inspectoras que sean precisas para el ejercicio de su función de supervisión y control.

Adicionalmente, el Reglamento (UE) nº 910/2014 atribuye a este órgano de supervisión la función (artículo 46 *ter* 3.b) de "*adoptar medidas, en caso necesario, en relación con los prestadores no cualificados de servicios de confianza establecidos en el territorio del Estado miembro que lo designa, mediante actividades de supervisión posteriores, cuando se le informe de que dichos prestadores no cualificados de servicios de confianza, o los servicios de confianza prestados por ellos incumplen presuntamente los requisitos establecidos en el presente Reglamento.*"

Octubre 2025

C/ POETA JOAN MARAGALL, 41
CP 28020 MADRID
E-mail: LFE@digital.gob.es