NOTA INFORMATIVA

Uso de Cl@ve por terceros: refuerzo del criterio restrictivo de la Administración Pública y su impacto en modelos de intermediación digital

La Agencia Estatal de la Administración Tributaria ("AEAT") a través de su comunicación publicada en abril bajo el título "Uso personal de Cl@ve y prevención de prácticas de intermediación no autorizadas" refuerza su criterio respecto el carácter personal e intransferible del sistema Cl@ve y cuestionando expresamente los modelos en los que terceros intervienen en el uso de credenciales del ciudadano para acceder a servicios de la Administración Pública.

Aspectos clave

- La AEAT reafirma que Cl@ve es un mecanismo estrictamente personal, cuyo uso debe realizarse directamente por el titular, sin intervención de terceros en el proceso de autenticación.

- Se desaconsejan expresamente los modelos de intermediación técnica en los que un tercero gestiona o utiliza las credenciales del usuario, o accede a la Administración en su nombre para obtener información (AEAT, Seguridad Social, etc.). Se consideran prácticas indebidas:
    - el uso de credenciales por terceros, incluso con consentimiento,
    - la captura o reutilización de credenciales u OTP,
    - la automatización del proceso de autenticación mediante sistemas interpuestos.

- Este posicionamiento tiene un claro impacto en determinados modelos digitales actualmente utilizados (especialmente en sectores como banca, fintech o agregadores de información), al cuestionar su encaje con los criterios de la Administración.

La presente Nota Informativa tiene por objeto exponer las consideraciones formuladas por la Agencia Estatal de Administración Tributaria ("**AEAT**") en relación con el carácter **personal e intransferible** de los sistemas Cl@ve y **la necesidad de prevenir prácticas de intermediación o utilización por terceros** publicadas el pasado mes de abril bajo el título **"Uso personal de Cl@ve y prevención de prácticas de intermediación no autorizadas"**[1].

I. ANTECEDENTES

Antes de abordar el contenido concreto de las afirmaciones realizadas por la AEAT resulta conveniente contextualizar su publicación dentro del marco regulatorio actualmente existente.

Cl@ve es un sistema de identificación, autenticación y firma electrónica habilitado por la Administración General del Estado para facilitar la relación electrónica de los ciudadanos con las Administraciones Públicas. De acuerdo con la propia definición facilitada por la Cl@ve:

> *Se trata de una plataforma común para la identificación, autenticación y firma electrónica, un sistema interoperable y horizontal que evita a las Administraciones Públicas tener que implementar y gestionar sus propios sistemas de identificación y firma, y a los ciudadanos tener que utilizar métodos de identificación diferentes para relacionarse electrónicamente con la Administración.*

Conviene aclarar que este tipo de sistemas son fruto de la entrada en vigor de la distinta normativa aplicable[2] que tiene por finalidad la transformación digital y regular los mecanismos de identificación y autenticación electrónica de los ciudadanos en sus relaciones con las Administraciones Públicas.

[1] Agencia Tributaria: Uso personal de Cl@ve y prevención de prácticas de intermediación no autorizadas

[2] entre otras, Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (en adelante, el "**Reglamento eIDAS**"), la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, la "**LPACAP**"), la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianz, así como el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y el funcionamiento del sector público por medios electrónicos.

En este contexto, los artículos 9 y 10 de la LPACAP contemplan distintos **sistemas de identificación y firma electrónica admitidos para que los ciudadanos puedan relacionarse con las Administraciones Públicas**, entre los que se incluye Cl@ve. Por su parte, el Reglamento eIDAS reconoce expresamente la **figura de los prestadores de servicios de confianza**, entendidos como aquellas personas físicas o jurídicas que prestan uno o varios servicios de confianza, ya sean cualificados o no cualificados.

Aclarado lo anterior, **resulta de interés recordar que esta no es la primera vez que las Autoridades Públicas se pronuncian sobre esta cuestión**. De hecho, **ya en 2022, el Ministerio de Asuntos Económicos y Transformación Digital** publicó la "Nota aclaratoria sobre la utilización de certificados electrónicos por personas diferentes del titular o firmante"[3], en la que afirmó de forma expresa que:

> *En conclusión, se recuerda que los certificados electrónicos son de uso personal e intransferible, y la posibilidad de que el titular o firmante de un certificado electrónico expedido a su nombre transfiera su posesión y revele sus claves de acceso a cualquier tercero no es conforme con la legislación vigente en materia de servicios electrónicos de confianza*. (el subrayado es nuestro)

Este criterio resulta plenamente coherente con lo previsto tanto en las Preguntas frecuentes (FAQs) sobre Cl@ve Pin[4] como en la documentación informativa publicada por la propia AEAT y por la Administración General del Estado, donde se insiste reiteradamente sobre su carácter personal e intransferible.
Ahora bien, si este principio ya venía siendo sostenido por la Administración desde hace años, cabe plantearse una cuestión fundamental: **¿qué aporta realmente de nuevo el reciente comunicado de la AEAT**?

II. CONTENIDO DE LAS RECOMENDACIONES

La comunicacion de la **AEAT debe interpretarse como una advertencia expresa frente a determinados modelos de negocio basados en la intermediación en el acceso a datos públicos, particularmente aquellos que se apoyan en el consentimiento del**

[3] Nota delegación de firma
[4] Cl@ve | Cl@ve PIN - Preguntas frecuentes (Faqs)

usuario/cliente para operar con sus credenciales, reproducen esquemas de "delegacion práctica" de la autenticación o permiten a terceros acceder directamente a información personal en sedes electrónicas.

Pues bien, actualmente, en el contexto de la digitalización de los servicios públicos y de los modelos de intercambio de información "Open Data" se han desarrollado soluciones de intermediación, a través de las cuales, el prestador se posiciona como un intermediario técnico entre el ciudadano y la Administración, asumiendo de facto la realización del proceso de autenticación en nombre de aquel.

Aunque en su gran mayoría estos modelos suelen basarse en el consentimiento del usuario y buscan simplificar su experiencia, la AEAT es contundente al respecto.

La comunicación de la AEAT, aunque no introduce por sí misma unas prohibiciones con rango de ley, sí considera como uso indebido determinadas prácticas que deben interpretarse como recomendaciones o criterio administrativo.

A continuación, resumimos las prácticas referenciadas:

- Cl@ve es un mecanismo de identificación, autenticación y firma electrónica de uso personal, directo e intransferible;

- no está permitido que terceros utilicen los mecanismos de autenticación de Cl@ve del ciudadano para acceder en su nombre a los servicios electrónicos de las Administraciones Públicas;

- es un uso indebido el acceso a servicios mediante las credenciales del ciudadano aunque haya prestado su consentimiento;

- es un uso indebido utilizar sistemas técnicos de intermediación que capturen, reutilicen o automaticen procesos de autenticación o mostrar o gestionar códigos QR o similares a través de sistemas interpuestos;

- es un uso indebido al almacenar, tratar o reutilizar contraseñas, códigos de un solo uso (OTP) y otros elementos destinados a autenticar al ciudadano.

En suma, la AEAT considera un uso indebido de Cl@ve cualquier tipo de uso del sistema que conlleve una intermediación en virtud de la cual un tercero acceda a las Administraciones Públcias empleando las credenciales del ciudadano .

En definitiva, aunque el criterio de la AEAT no introduce una prohibición legal expresa, sí supone un endurecimiento claro en la interpretación administrativa del uso de sistemas de identificación electrónica. Desde una perspectiva práctica no invalida automáticamente los modelos existentes, pero incrementa significativamente su exposición a riesgos de compliance, supervisión y continuidad a medio plazo

Además, la propia AEAT advierte expresamente que podrá implementar las medidas técnicas y organizativas que considere necesarias para proteger a los ciudadanos y garantizar la integridad de los mecanismos de identificación y autenticación, lo que refuerza la idea de una orientación claramente restrictiva y anticipa posibles limitaciones futuras, mediante desarrollos normativos o técnicos, respecto de los modelos de intermediación basados en el uso de credenciales de terceros.

Finalmente, debe tenerse en cuenta que, en estos esquemas, las actuaciones realizadas mediante Cl@ve se atribuyen plenamente a su titular, incluso cuando interviene un tercero,lo que refuerza el riesgo asociado a su uso compartido o delegado.

Área de Privacidad de ECIJA
info@ecija.com
Telf: + 34 91.781.61.60