

Nota informativa

La plataforma para la resolución de litigios en línea refuerza su seguridad con nuevas medidas de autenticación multifactorial

Los usuarios, además de utilizar su teléfono móvil, podrán usar también una llave de seguridad USB para autenticarse y acceder a todos los servicios informáticos de la Comisión Europea

Madrid, 07 de octubre de 2022. La Comisión Europea incorpora nuevas medidas de ciberseguridad en los servicios informáticos que ofrece actualmente, entre los que se encuentra la [plataforma para la Resolución de Litigios en Línea \(RLL\)](#). De esta forma, todos los usuarios tendrán que realizar una autenticación multifactorial para poder seguir accediendo a dichos servicios. Con este nuevo sistema se persigue crear un entorno digital más seguro y afianzar la confianza de los ciudadanos. Para ello, los usuarios podrán escoger distintas opciones para llevar a cabo la autenticación, de forma que podrán hacerlo a través de su teléfono móvil convencional mediante un SMS; a través de su teléfono móvil inteligente, utilizando para ello la APP “EU Login” disponible en Google Play y App store; o bien a través de una llave de seguridad USB.

Acerca autenticación multifactorial

La autenticación multifactorial (MFA, Multi-factor authentication) constituye una medida de seguridad que añade una nueva capa de protección adicional a las contraseñas utilizadas habitualmente para acceder a determinados servicios o entornos digitales. Se trata de un método de autenticación electrónica en el que se requieren dos o más factores (p. ej. una contraseña y una huella dactilar) para acceder a una página web o aplicación.

Acerca de las llaves de seguridad USB

¿Qué es una llave de seguridad USB?

La llave de seguridad USB es un dispositivo que se utiliza para realizar la verificación en dos pasos sin necesidad de utilizar el teléfono móvil o correo electrónico. Utiliza el estándar de verificación en dos pasos U2F (Universal 2nd Factor) y funciona de forma sencilla. Tan solo hay que conectar la llave de seguridad USB a un ordenador y la llave se encarga de realizar la autenticación multifactorial.

Se trata de un dispositivo que comercializan distintos fabricantes con diferentes marcas. Yubikey, FIDO2, U2F (Universal Second Factor), son solo algunos ejemplos de las llaves que podemos encontrar en el mercado.

¿Cómo hacer la autenticación multifactorial con una llave de seguridad USB?

Adquirir la llave

Cualquier persona podrá adquirirla en una tienda de tecnología o en comercios online. Hay múltiples opciones de compra. Por ejemplo, por 29 € puede conseguirse una llave de seguridad USB Yubico a través de este [enlace](#).

Recomendaciones para adquirirla

Cualquier llave compatible con FIDO2 es una buena opción ¿Utiliza el protocolo de identificación WebAuthN? Entonces, dispone de un protocolo considerado como muy seguro. Hay que tener también en cuenta que algunos modelos integran lectores de huellas dactilares para agregar más seguridad al proceso. En estos casos, puede que se añada –además– un elemento adicional de complejidad ya que, por ejemplo, para poder acceder a Windows sería necesario utilizar también la llave. Antes de comprarla, debe comprobarse el tipo de puerto USB (USB-A o USB-C) que utiliza el ordenador donde se va a utilizar con el fin de asegurarnos de que la llave y el equipo sean compatibles. Asimismo, se recomienda no utilizar el mismo dispositivo para identificarse y acceder a todos los servicios online que requieren de doble factor de autenticación.

Seleccionar el método de autenticación en la página web EU Login

Para poder utilizar una llave de seguridad USB como método de autenticación multifactorial en los servicios online de la Comisión Europea, el usuario deberá tener -previamente- una cuenta en la plataforma [EU Login](#). Una vez registrado, deberá realizar estos sencillos pasos:

- Acceder, desde un ordenador, a su cuenta online [EU Login](#) e identificarse con sus claves de usuario.
- Seleccionar “Gestionar mis Claves de Seguridad y Plataformas de Confianza”.
- Insertar la llave de seguridad USB.
- Seleccionar “Añadir una llave de seguridad” e identificarla con un nombre.

>> [Tutorial “Cómo autenticarse en EU Login”](#). (Páginas 5, 26 y 27).

Una vez añadida, para realizar la autenticación multifactorial, se selecciona la llave como forma de autenticación, se inserta en el puerto USB y se hace clic en el botón correspondiente. Cabe advertir que los usuarios deben custodiar esta llave de forma adecuada para evitar el mal uso que puedan hacer terceras personas.

>> Para explicar el proceso, CEC-Alemania ha publicado un [video tutorial](#).

Acerca de la plataforma RLL

La Plataforma RLL (Resolución de Litigios en Línea) es una herramienta on line desarrollada por la Comisión Europea para la resolución litigios en línea que tiene como fin ayudar a consumidores y comerciantes a solucionar conflictos relativos a compras de productos y servicios contratados online. Esta plataforma puede ser utilizada por todos los ciudadanos que residan en la Unión Europea, Noruega, Islandia o Liechtenstein para tratar de encontrar la mejor solución posible a sus problemas de consumo, para negociar una solución directamente con la empresa o para acordar que un organismo de resolución de litigios se encargue de su caso. Se trata de una plataforma sin vínculos con ninguna empresa que puede ser utilizada en todas las lenguas oficiales de la UE, así como en islandés y noruego.

El contenido de esta nota informativa recoge únicamente las opiniones del autor que es el único responsable del mismo. No refleja las opiniones de la Comisión Europea y/o la Agencia Ejecutiva de Consumidores, Salud, Agricultura y Alimentación (CHAFEA), y/o su sucesor el Consejo Europeo de Innovación y la Agencia Ejecutiva de PYMES (EISMEA) o cualquier otra institución de la Unión Europea. La Comisión Europea y la Agencia no asumen ninguna responsabilidad por el uso que pueda hacerse de la información que contiene.

El contenido de esta nota informativa, disponible en el dominio europa.eu, puede contener "enlaces externos" a sitios web en otros dominios diferentes a europa.eu que son responsabilidad exclusiva de su autor. Los servicios de la Comisión Europea no tienen ningún control ni asumen ninguna responsabilidad sobre estos "enlaces externos". Cuando los visitantes de los sitios web de la Comisión deciden entrar en tales "enlaces externos" que dirigen a sitios web con dominios distintos de europa.eu, lo hacen bajo su propia responsabilidad, abandonando el dominio oficial de la Comisión Europea. En particular, estos visitantes estarían sujetos a las políticas de cookies, privacidad y legalidad (incluyendo la protección de datos y los requisitos de accesibilidad) del sitio web externo.