

NOTA TÉCNICA

DESCRIPCIÓN DE LAS PRUEBAS DE CONCEPTO SOBRE SISTEMAS DE VERIFICACIÓN DE EDAD Y PROTECCIÓN DE PERSONAS MENORES ANTE CONTENIDOS INADECUADOS

ÍNDICE

I.	INTRODUCCIÓN	3
II.	PRUEBAS DE CONCEPTO	5
A.	Descripción general de las pruebas de concepto	6
B.	Prueba de concepto orientada a ordenadores o consolas de videojuegos	8
C.	Prueba de concepto orientada a teléfonos móviles con Android	10
D.	Prueba de concepto orientada a teléfonos móviles con iOS	13
III.	CONCLUSIÓN	17

I. INTRODUCCIÓN

La AEPD ha preparado el [“Decálogo de principios. Verificación de edad y protección de personas menores de edad ante contenidos inadecuados”](#) (el Decálogo) que recoge los principios que debe cumplir un sistema de verificación de edad y protección del menor ante contenidos inadecuados para personas menores de edad. El objetivo de dicho Decálogo es garantizar la protección del interés superior del menor, los principios, derechos y obligaciones establecidos en el RGPD en el marco de dichos sistemas y el de señalar las pautas para garantizar la protección de los derechos fundamentales de todas las personas usuarias de Internet.

La protección del menor ante contenidos inadecuados se ha de enmarcar en la protección del interés superior del menor. El interés superior del menor es más amplio que impedir su acceso a contenidos inadecuados. El interés superior del menor abarca la protección de todos sus derechos fundamentales, y en particular, todos los aspectos que puedan afectar a su seguridad, su salud y su desarrollo, así como su intimidad.

La protección del menor ante contenidos inadecuados no puede ser una excusa para vulnerar derechos fundamentales, en particular de las propias personas menores. Los derechos fundamentales de todas las personas usuarias de Internet se deben proteger independientemente de su edad. Y, de igual forma, los derechos fundamentales, en particular los relativos a la protección de datos, no se pueden usar como una excusa para no desarrollar las medidas adecuadas para proteger a las personas menores de edad.

La protección de las personas menores de edad ante la exposición incontrolada a contenidos o sitios inadecuados para ellas no debe convertirse en la vigilancia de todas las personas usuarias de Internet. En particular, esta protección no legitima la captación continuada y masiva de los datos de las personas menores de edad, para su perfilado y para la permanente exposición de este colectivo vulnerable a la publicidad que enriquece estos sitios.

Ya existen soluciones en el mercado que sirven para verificar la edad de las personas usuarias de Internet y muchas de ellas no abordan la protección global de los derechos y libertades de la ciudadanía. Algunas se basan en compartir credenciales o atributos de identidad con los proveedores de contenidos para que puedan realizar comprobaciones directamente, otras se basan en la incorporación de proveedores de identidad especializados que recogen la información de navegación, otras confían en estimaciones de edad realizadas mediante la aplicación de técnicas de inteligencia artificial a imágenes faciales recogidas en tiempo real, y muchas funcionan con una combinación de las características anteriores. Sin embargo, multitud de estas soluciones implican un tratamiento de datos que incumple con los requisitos básicos del RGPD, incluyen operaciones de alto riesgo para los derechos y libertades de las personas usuarias y, lo que es peor, establecen [limitaciones importantes en la protección del interés superior del menor y de sus derechos fundamentales](#).

Un sistema que va a afectar a todas las personas usuarias de Internet, con particular incidencia en las personas menores de edad, ha de cumplir escrupulosamente con la normativa de protección de datos y supone un tratamiento de alto riesgo en la medida que puede suponer un gran impacto en los derechos fundamentales. La verificación de edad

para el acceso a contenidos inadecuados para personas menores no puede implicar la identificación de las personas usuarias de Internet, su detección (especialmente si se trata de personas menores de edad), la vinculación de su actividad en diferentes servicios, el tratamiento excesivo de sus datos, su perfilado, el uso de sistemas potencialmente discriminatorios que limiten la capacidad de obrar en el mundo digital, etc.

El Decálogo de principios publicado por la AEPD establece la manera de conciliar ambos aspectos: el interés superior del menor y los derechos fundamentales de todas las personas usuarias de Internet. Este Decálogo establece las condiciones mínimas que ha de cumplir un sistema de verificación de edad y de protección ante contenidos inadecuados para personas menores, entre otras, impedir que una persona menor de edad pueda ser localizada a través de Internet utilizando estos sistemas, garantizar el anonimato de todas las personas usuarias adultas, minimizar los datos tratados o desvelados a terceros, velar por que las familias sean partícipes de los criterios para proteger a las personas menores de edad o establecer sistemas que generen confianza, sean idóneos y que protejan el interés superior del menor y los derechos fundamentales de la ciudadanía.

II. PRUEBAS DE CONCEPTO

Con el propósito de demostrar que es posible el cumplimiento del Decálogo, y que este tipo de soluciones ya podrían ofrecerse en Internet, la AEPD, en colaboración con el Consejo General de Colegios Profesionales de Ingeniería Informática, ha desarrollado una serie de pruebas de concepto que implementan un sistema de protección que se deriva de dicho Decálogo.

Las pruebas de concepto desarrolladas en la AEPD demuestran que es posible llevar estos principios a la práctica en escenarios reales, probando su idoneidad, y la aplicación del principio de necesidad y de minimización de datos de forma efectiva.

Las pruebas de concepto se basan, fundamentalmente, en que es posible una separación clara entre la gestión de la identidad, la verificación de la edad y el filtrado de contenidos. Por lo tanto, demuestran que los proveedores de identidad que actualmente implementan el derecho a la propia identidad de la ciudadanía española y europea ya son suficientes, y que no es necesario construir sistemas paralelos de identidad digital para el propósito específico de acceso a contenidos inadecuados para menores. Un aspecto fundamental para evitar la discriminación y los sesgos es que la solución de verificación de edad pueda interaccionar con aquellos proveedores de identidad que sean más adecuados para el usuario y que le den una mayor confianza. En particular, orientados a ser compatibles con la cartera digital y con las garantías a la intimidad en Internet que guían la iniciativa eIDAS2 y, a la vez, que se puedan extrapolar a proveedores universales de identidad, como los que expiden pasaportes u otras soluciones físicas o digitales.

Las pruebas de concepto también se basan en que la protección ante contenidos inadecuados puede realizarse en el propio dispositivo, teniendo las personas el control total sobre el uso de su identidad y su edad, de forma que los sistemas sean totalmente auditables y transparentes.

Finalmente, las pruebas de concepto demuestran que no es necesaria la localización, seguimiento y perfilado de menores en Internet (ni de las personas usuarias en Internet en general), para implementar la protección ante contenidos inadecuados.

La confianza que se genere en la ciudadanía con respecto a estos sistemas es fundamental para garantizar la idoneidad de estos. Un sistema que no genere la suficiente confianza en las personas usuarias provocará discriminación, autocensura y, finalmente, rechazo por las mismas.

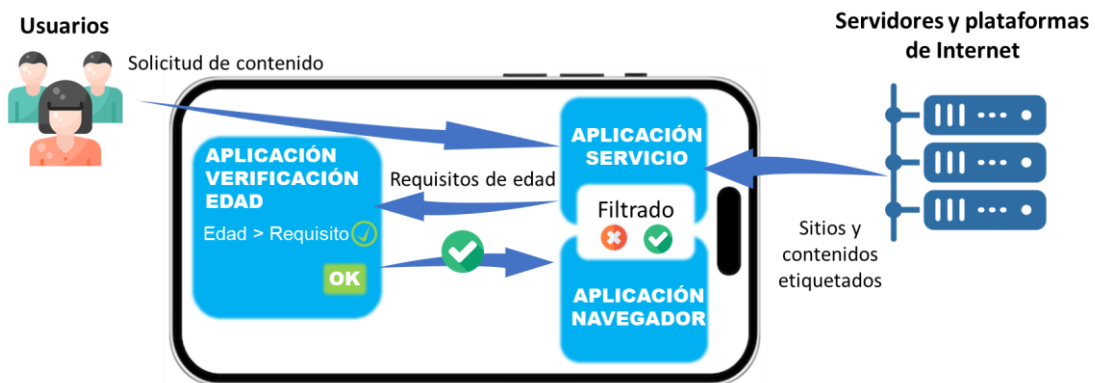
Estas pruebas de concepto dejan la puerta abierta a otras soluciones o alternativas que puedan cumplir también con los principios optando por otras arquitecturas o decisiones de diseño.

A. DESCRIPCIÓN GENERAL DE LAS PRUEBAS DE CONCEPTO

Las pruebas de concepto se basan en la utilización de dos aplicaciones:

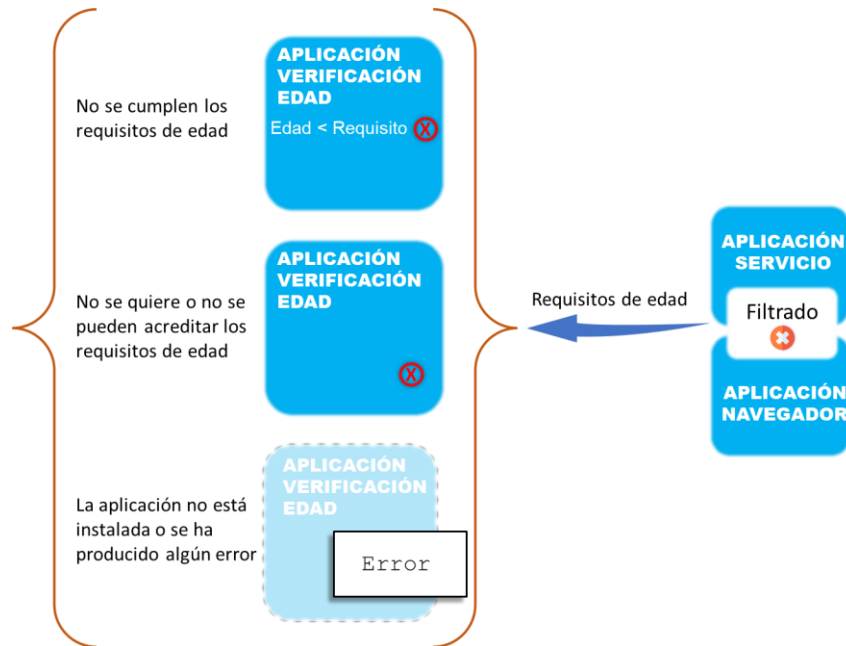
- Una aplicación de acceso a contenidos, de tipo navegador o *app* específica de un servicio de Internet (la *app* para acceder a una red social, por ejemplo). Esta aplicación recibe contenidos desde el proveedor de contenidos en Internet. Si están etiquetados como “todos los públicos”, los muestra sin limitaciones. Si están etiquetados como “para personas adultas” o “inadecuados para menores”, sólo los muestra tras una verificación de edad de la persona usuaria.
- Una aplicación de verificación de edad, que recibe la solicitud de verificación de la aplicación anterior, comprueba la edad de la persona usuaria y genera la condición de persona “autorizada a acceder” si la persona usuaria puede acreditar la edad necesaria para acceder a ese contenido (podrían ser 14 años, 18 años u otras condiciones).

Un aspecto fundamental es que todo el proceso de verificación de edad y protección ante contenidos inadecuados se realiza sin salir del dispositivo de la persona usuaria ni realizar accesos a recursos externos.



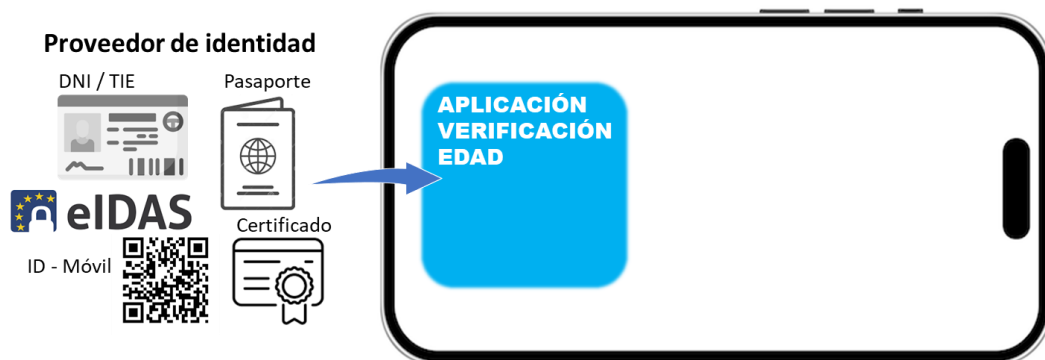
Descripción a alto nivel del sistema implementado en las pruebas de concepto

Para evitar la señalización de menores en Internet, es importante tener en cuenta que cuando la aplicación de verificación de edad no responde con la condición de persona “autorizada a acceder”, puede ser por varias razones: porque la persona usuaria no tenga la edad requerida, pero también porque no haya podido o querido acreditarla, porque se haya producido un error, etc. Todas estas situaciones no se deben poder distinguir entre ellas.



Situaciones en las que no se acredita la condición de persona “autorizada a acceder”

También es importante mencionar que la aplicación de verificación de edad necesita que la persona usuaria acredite su edad de manera cierta, pero sin exponer su identidad. Para ello se emplea una *app* de verificación de edad, que hace de intermediaria entre diferentes proveedores de identidad y la aplicación que debe verificar la edad para permitir el acceso a ciertos contenidos. Las pruebas de concepto desarrolladas se han basado en el uso de códigos QR, identidades digitales almacenadas en carteras electrónicas o documentos de identidad físicos. Ambos procesos, el de alta en un sistema de gestión de identidades y uso de dicha identidad, y el de verificación de edad, se consideran independientes. La *app* de verificación de edad, ejecutándose únicamente en el dispositivo personal, y proporcionada por una entidad seleccionada por la persona usuaria, evita la difusión de la identidad. Dicha *app*, al situarse entre la identidad y la generación de la condición de persona “autorizada a acceder” permite auditar que nunca se desvele la identidad a los proveedores de contenidos o terceras entidades.



Acreditación de identidad independiente de la verificación de edad para el acceso a contenidos que, por tanto, será anónima

Para implementar estrategias que eviten la exposición de la condición de menor de la persona usuaria, es decir, para evitar que haya forma de localizar menores a través de Internet, las políticas de filtrado de contenido se ejecutan también en el propio dispositivo. La protección del menor no tiene como objetivo que los proveedores de Internet localicen, identifiquen y puedan perfilar a menores. Al contrario, los proveedores deben permanecer ignorantes de la condición de menor de las personas usuarias. Además, la ejecución de las políticas de filtrado de contenidos en el propio dispositivo tiene otras ventajas colaterales: mayor transparencia, auditabilidad de la ejecución de las políticas, ajuste parental de las mismas para menores con vulnerabilidades especiales, etc.

En las pruebas de concepto se han simulado proveedores de Internet que proporcionan contenidos etiquetados de una manera sencilla. Por ejemplo, se puede utilizar el esquema propuesto por Age.xml¹, surgido en el contexto del proyecto MIRACLE (Machine-readable and interoperable age classification labels in Europe), financiado por la Comisión Europea.

B. PRUEBA DE CONCEPTO ORIENTADA A ORDENADORES O CONSOLAS DE VIDEOJUEGOS

La primera prueba de concepto está orientada a demostrar una solución al problema del acceso a contenidos desde un dispositivo como un ordenador o consola de videojuegos, con un sistema operativo de la familia Windows instalado. En el siguiente [enlace](#) se puede visualizar un ejemplo de ejecución de la solución desarrollada.

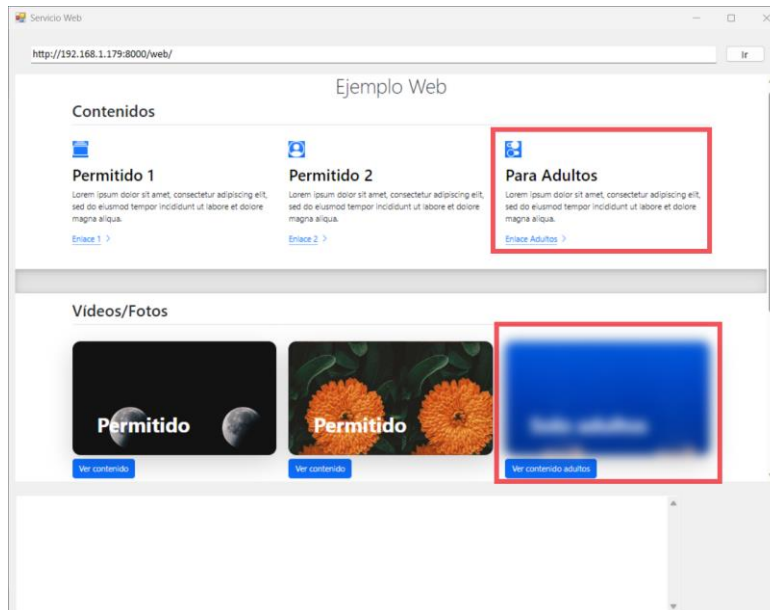
La persona usuaria debe tener instalada en dicho dispositivo la aplicación de verificación de edad que se ha desarrollado en la Agencia y un navegador modificado para poder trabajar con ella.

La descripción somera de esta prueba de concepto es la siguiente. Antes de usar el sistema, la persona usuaria obtendría un código QR, proporcionado por ejemplo por los desarrollos de la FNMT para el Ministerio de Interior en su teléfono móvil. La información del QR podría ser anónima o no, ya que la aplicación de verificación bloqueará la difusión de la identidad. El atributo de edad del usuario se almacenará en la aplicación de verificación por un periodo de tiempo limitado para evitar correlaciones entre las solicitudes del QR y el acceso a contenido inadecuado.

A continuación:

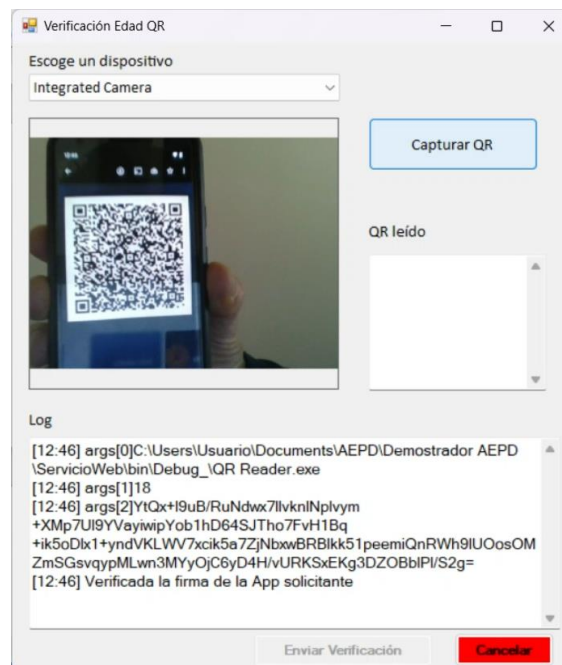
1. La persona solicita acceder a un contenido etiquetado para personas adultas desde el navegador.
2. Se recibe el contenido con su etiqueta y se bloquea preventivamente la exhibición del contenido en el dispositivo (en la prueba de concepto simplemente se muestra el contenido borroso o difuminado). De esta forma, no se desvela la condición de menor al servicio de Internet, el contenido se sirve siempre.

¹ <https://age-label.com/>



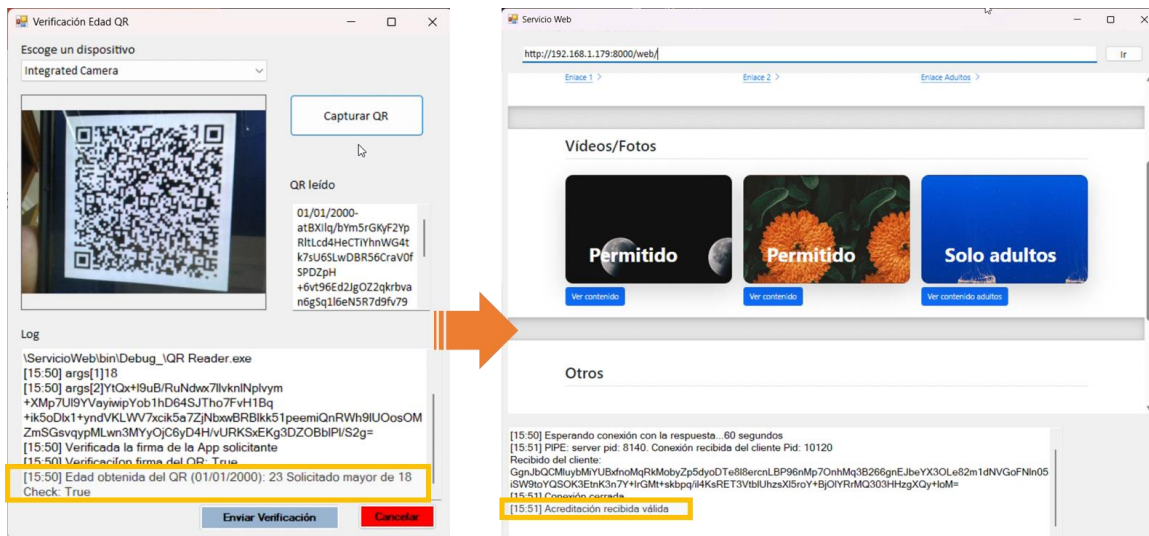
Navegador que descarga contenido etiquetado, pero no lo muestra si requiere verificación de edad

3. El navegador llama a la *app* de verificación para determinar si la persona usuaria tiene la edad adecuada para acceder a los contenidos (mayor de 14, mayor de 18 u otras condiciones). La aplicación de verificación de edad le pide a la persona usuaria que acerque su código QR (en su teléfono móvil) a la cámara del ordenador o de la consola.

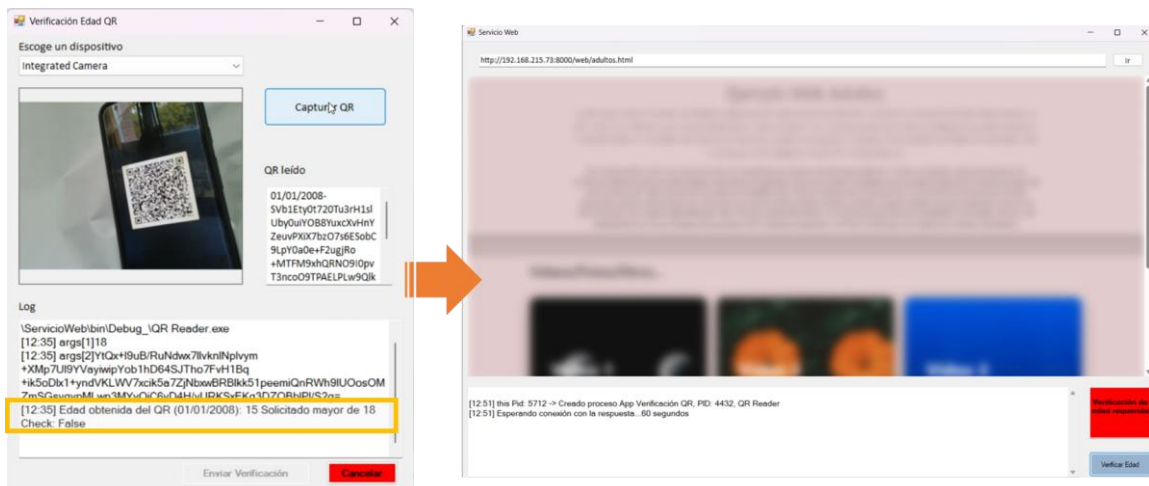


Lectura y comprobación del QR en la aplicación de verificación de edad

4. A continuación, pueden darse dos situaciones diferentes:
 - a. La aplicación de verificación responde con la condición de persona “autorizada a acceder”, sin revelar información de identidad. El navegador retira el filtro y se accede al contenido sin ningún tipo de restricción.



- b. La aplicación de verificación no responde con la condición de persona “autorizada a acceder”. De hecho, no responde de ninguna manera, por lo que pasado un tiempo el navegador deja de esperar respuesta y mantiene el filtro al contenido. Esto puede ocurrir porque la persona no tiene la edad requerida (pero no se desvela la condición de menor), o porque no se ha instalado la aplicación de verificación de edad, o porque no se autoriza a su uso, o no se dispone del código QR o por cualquier otra circunstancia.



C. PRUEBA DE CONCEPTO ORIENTADA A TELÉFONOS MÓVILES CON ANDROID

En la segunda prueba de concepto el acceso a contenidos se realiza con un teléfono móvil con el sistema operativo Android instalado. La persona usuaria debe instalar en este

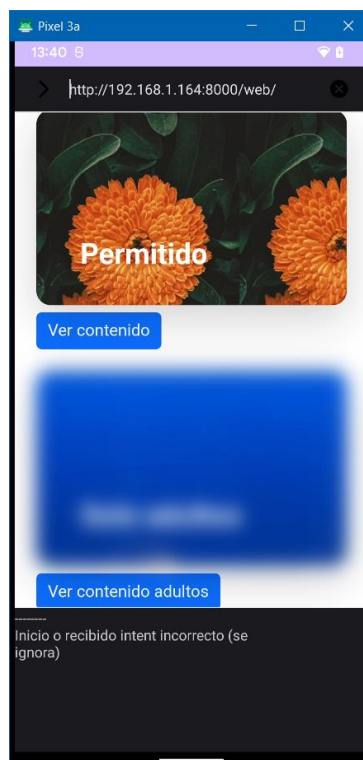
teléfono la *app* de verificación de edad desarrollada por la AEPD y un navegador modificado para trabajar con ella. En el siguiente [enlace](#) se puede visualizar un ejemplo de ejecución de la prueba de concepto.

La descripción somera de esta prueba de concepto es la siguiente. Antes de usar el sistema, la persona usuaria necesita disponer en su teléfono de una *app* de tipo cartera digital (*ewallet*), por ejemplo, una de ellas será la cartera que proporcionará la Secretaría General de Administración Digital (SGAD) compatible con la regulación europea eIDAS2. Esta aproximación es válida para su uso con cualquier documento o certificado emitido por una entidad o proveedor de confianza que incluya la información de edad.

La cartera digital proporcionará un atributo de edad que podría ser anónimo o no, ya que la *app* de verificación bloqueará la difusión de la identidad. El atributo de edad del usuario se almacenará en la *app* de verificación por un periodo de tiempo limitado para evitar correlaciones entre las solicitudes a la cartera digital y el acceso a contenido inadecuado.

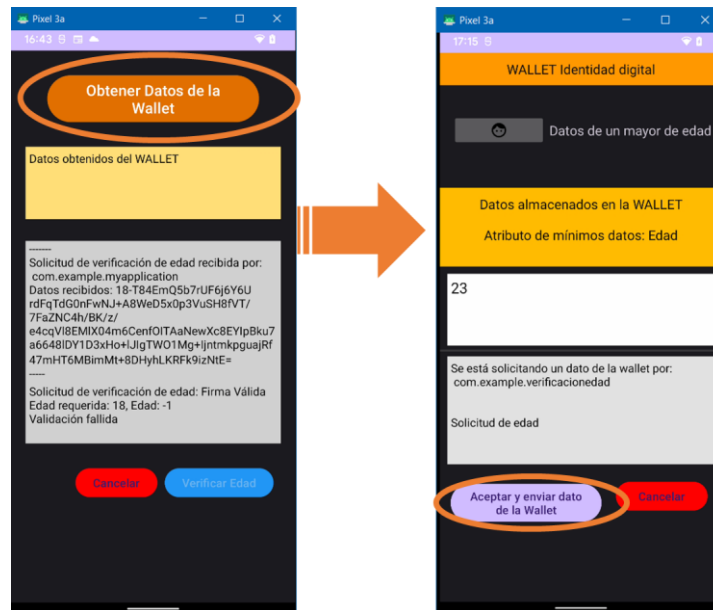
A continuación:

1. La persona solicita acceder a un contenido etiquetado para personas adultas desde el navegador.
2. Se recibe el contenido con su etiqueta y se bloquea preventivamente la exhibición del contenido en el dispositivo (en la prueba de concepto simplemente se muestra el contenido borroso o difuminado). De esta forma, no se desvela la condición de menor al servicio de Internet, el contenido se sirve siempre.



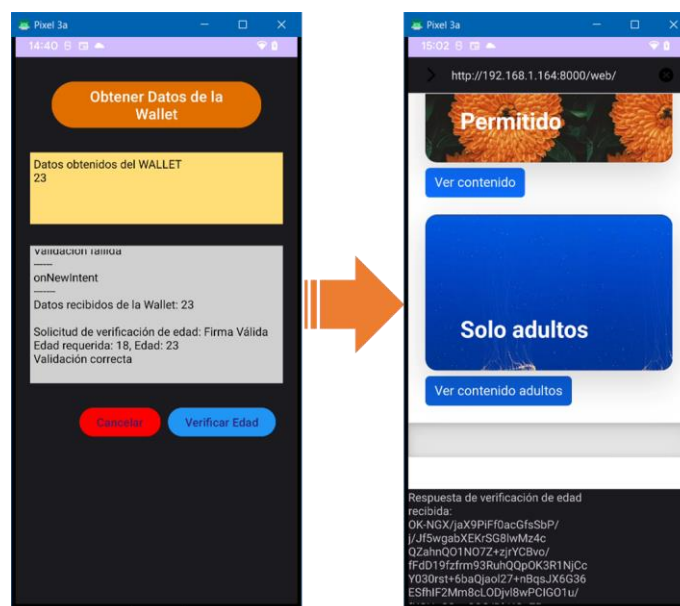
Navegador que descarga contenido etiquetado, pero no lo muestra si se requiere verificación de edad

3. El navegador llama a la *app* de verificación para verificar si la persona usuaria tiene la edad adecuada para acceder a los contenidos (mayor de 14, mayor de 18 u otras condiciones). La aplicación de verificación de edad recurre a la información almacenada en la cartera digital para realizar las comprobaciones oportunas.



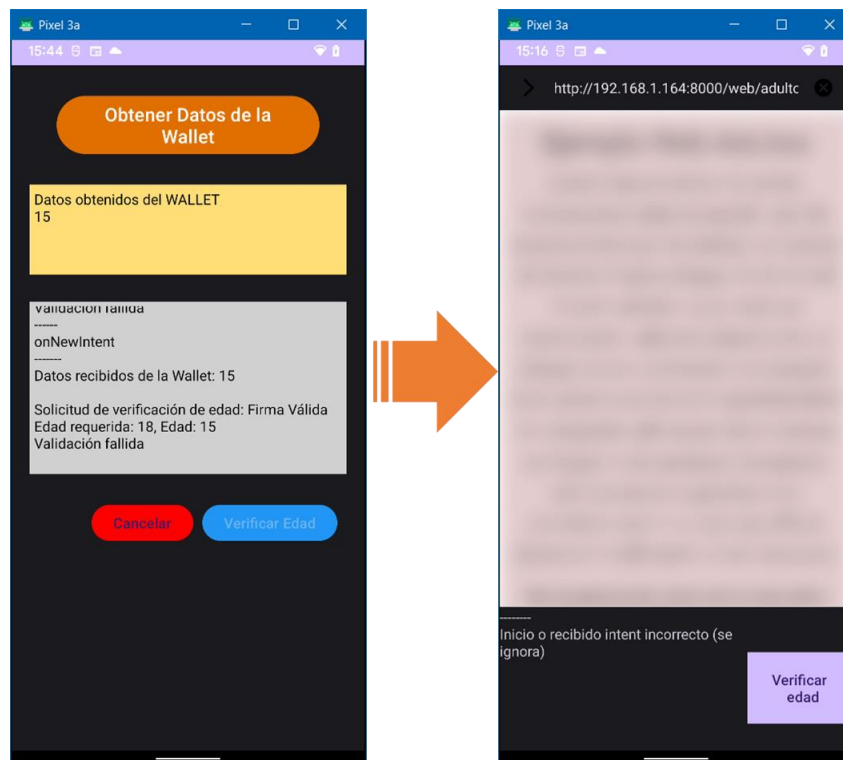
La app de verificación de edad recibe la solicitud del navegador y consulta la cartera digital

4. A continuación, pueden darse dos situaciones diferentes:
 - a. La *app* de verificación responde con la condición de persona “autorizada a acceder”, sin revelar información de identidad. El navegador retira el filtro y se accede al contenido sin ningún tipo de restricción.



Verificación de edad exitosa, se acredita la condición de persona “autorizada a acceder” y en consecuencia el contenido se muestra sin limitaciones

- b. La *app* de verificación no responde con la condición de persona “autorizada a acceder”. De hecho, no responde de ninguna manera, por lo que pasado un tiempo el navegador deja de esperar respuesta y mantiene el filtro al contenido. Esto puede ocurrir porque la persona no tiene la edad requerida (pero no se desvela la condición de menor), o porque no se ha instalado la *app* de verificación de edad, o porque no se autoriza a su uso, o no se dispone cartera digital o de identidad almacenada en ella que incorpore información sobre la edad o por cualquier otra circunstancia.



Verificación de edad no exitosa, no se acredita la condición de persona “autorizada a acceder” (no se habilita el botón de Verificar Edad, en este ejemplo, porque no se tiene edad suficiente) y en consecuencia el contenido sigue sin mostrarse

D. PRUEBA DE CONCEPTO ORIENTADA A TELÉFONOS MÓVILES CON IOS

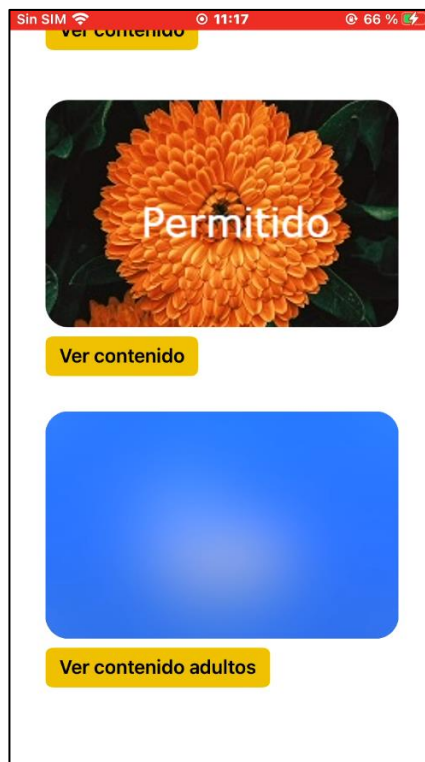
En la tercera y última prueba el acceso a contenidos se realiza de nuevo con un teléfono móvil, pero en este caso, con el sistema operativo iOS instalado. En el siguiente [enlace](#) se puede visualizar un ejemplo de ejecución de la prueba de concepto.

La descripción somera de esta prueba de concepto es la siguiente. Antes de usar el sistema, la persona usuaria necesita disponer en su teléfono de una *app* que pueda recuperar de documentos de identidad físicos (DNI, TIE, pasaporte, etc.) los datos relativos a su edad. Puede hacerse a través de una imagen del documento por OCR o leyendo el certificado de los chips que incluyen por NFC.

A continuación, se autentica a la persona usuaria mediante firma digital o biometría (comparando la foto del documento con la obtenida mediante un selfi) de manera que se comprueba que el documento aportado para la verificación de edad es el suyo. En todos los casos, los tratamientos se realizan en el dispositivo local, incluyendo la biometría, sin

acceso a entidades terceras, por lo que es un tratamiento exclusivamente personal. La *app* de verificación de edad bloqueará la difusión de la identidad obtenida del documento oficial, almacenando el atributo de edad del usuario por un periodo de tiempo limitado.

1. La persona solicita acceder a un contenido etiquetado para personas adultas desde una aplicación de acceso a contenidos.
2. Se recibe el contenido con su etiqueta y se bloquea preventivamente la exhibición del contenido en el dispositivo. De esta forma, no se desvela la condición de menor al servicio de Internet, el contenido se sirve siempre.



Aplicación que descarga contenido etiquetado, pero no lo muestra si se requiere verificación de edad

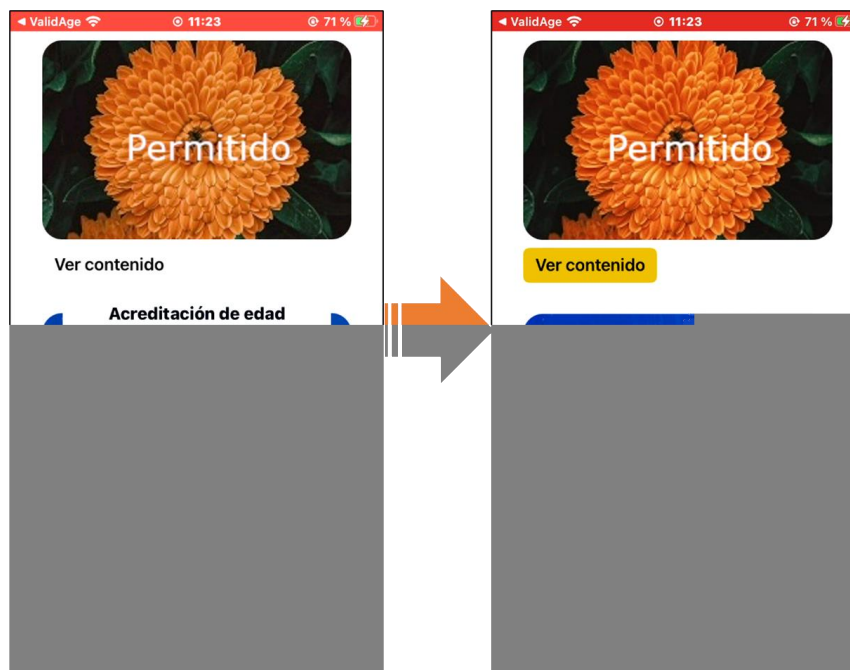
3. La aplicación de acceso a contenidos llama a la *app* de verificación para verificar si la persona usuaria tiene la edad adecuada para acceder a los contenidos (mayor de 14, mayor de 18 u otras condiciones). La *app* de verificación de edad recurre a la información recuperada de los documentos físicos para realizar las comprobaciones oportunas.



La app de verificación recibe la solicitud de la aplicación de acceso a contenidos (todo ocurre con el conocimiento de la persona usuaria, que es consciente del proceso y debe Aceptar la verificación de edad para que se produzca)

4. A continuación, pueden darse dos situaciones diferentes:

- a. La *app* de verificación responde con la condición de persona “autorizada a acceder”, sin revelar información de identidad. La aplicación de acceso a contenidos retira el filtro y se accede al contenido sin ningún tipo de restricción.



Verificación de edad exitosa, se acredita la condición de persona “autorizada a acceder” y en consecuencia el contenido se muestra sin limitaciones

- b. La *app* de verificación no responde con la condición de persona “autorizada a acceder”. De hecho, no responde de ninguna manera, por lo que pasado un

tiempo la aplicación de acceso a contenidos deja de esperar respuesta y mantiene el filtro al contenido. Esto puede ocurrir porque la persona no tiene la edad requerida (pero no se desvela la condición de menor), o porque no se ha instalado la App de verificación de edad, o porque no se autoriza a su uso, o no ha podido recuperar información sobre la edad de la persona usuaria desde el documento físico aportado o por cualquier otra circunstancia.



Verificación de edad no exitosa, no se acredita la condición de persona "autorizada a acceder" y en consecuencia el contenido sigue sin mostrarse

III. CONCLUSIÓN

La protección del menor ante contenidos inadecuados no puede ser una excusa para vulnerar derechos fundamentales. De igual forma, los derechos fundamentales, en particular los relativos a la protección de datos, no se pueden usar como una excusa para no desarrollar las medidas adecuadas para proteger a las personas menores de edad. La protección de los menores tiene que atender al interés superior del menor en todas sus facetas.

La urgencia de la necesidad de soluciones para la protección ante contenidos inadecuados no justifica la utilización de tratamientos de datos que incumplan con los principios, derechos y obligaciones del RGPD, incluyan operaciones de alto riesgo para los derechos y libertades de las personas usuarias y, lo que es peor, establezcan [limitaciones importantes en la protección del interés superior del menor y a los derechos fundamentales](#).

En las tres pruebas de concepto desarrolladas por la AEPD en colaboración con el Consejo General de Colegios Profesionales de Ingeniería Informática se demuestra cómo se puede cumplir de forma efectiva y eficiente el [“Decálogo de principios. Verificación de edad y protección de personas menores de edad ante contenidos inadecuados”](#).

Estas pruebas de concepto demuestran que existen opciones que evitan la exposición del menor, los incumplimientos normativos, los riesgos y amenazas detectados en las soluciones actuales disponibles en el mercado, que además pueden ser transparentes, auditables y que no precisan de el desarrollo de nuevos proveedores de identidad digital distintos a los ya establecidos en Europa. También demuestran que es posible desarrollar soluciones para distintos dispositivos, sistemas operativos y formas de acreditar que se posee edad suficiente para acceder a los contenidos en cada caso ([ordenadores o consolas de videojuegos](#), [móviles Android](#), [móviles iOS](#)), desde una necesaria neutralidad tecnológica.

Para una explicación más extensa de algunas de las dudas que pueden suscitar estas pruebas de concepto, se puede consultar la siguiente [página de preguntas frecuentes](#).