Procedimiento Múltiple Factor de Autentificación

Servei de Salut de les Illes Balears

16 de marzo del 2022

Versión del documento: 0.1

Histórico de versiones:

Control de Versiones

Versión	Autor	Fecha	Descripción	Revisor	Aprobador
v.0.1	Oficina de Seguridad	16/03/2022	Versión inicial	Jesús Úbeda	

Índice

1. Introducción

El IB – Salut, en su nueva política de seguridad de la información, ha implantado el múltiple factor de autentificación para los accesos remotos a los Sistemas de Información de la organización.

Se debe diferenciar 4 tipos de accesos remotos:

- Acceso a través de VPN, mediante la herramienta FortiClient.
- Acceso a través de escritorio remoto para Teletrabajo.
- Acceso a través de Citrix.
- Acceso a aplicaciones Office365.

Para ello, será imprescindible cumplir con los siguientes requisitos:

1. Tener usuario S.
2. Tener el **teléfono móvil** informado en OIM. En caso de no tenerlo, el personal interno debe acudir a RRHH de su gerencia y los externos deben ponerse en contacto con su Responsable directo.
3. Tener el **correo electrónico** informado en OIM. En caso de no tenerlo, el personal interno debe acudir a RRHH de su gerencia y los externos deben ponerse en contacto con su Responsable directo.

Para utilizar el **múltiple factor de autenticación**, además de cumplir con los requisitos anteriores, deberá inscribirse un dispositivo en el portal dónde se recibirán las confirmaciones necesarias para cada acceso:

El método que se debe seleccionar es el de **Teléfono inteligente**. Para ello será necesario:

1. Instalar en el smartphone inscrito la aplicación **NetIQ Advanced Authentication**.
2. Inscribir un Smartphone en el **portal del Segundo Factor de Autenticación** del IB-Salut (https://mfa.ssib.es/account/), que proporcionará un código QR.
3. Escanear el código QR obtenido en el portal del Segundo Factor de Autenticación, en la aplicación NetIQ instalada previamente en el dispositivo.

NOTA: también será necesario instalar en el dispositivo con el que se realice el acceso remoto, las herramientas necesarias para el tipo de acceso que se quiera realizar. La instalación de estas herramientas, **se explica en su manual correspondiente**.

En caso de no tener Teléfono inteligente, debe utilizarse el método TOTP explicado en el anexo de este manual.

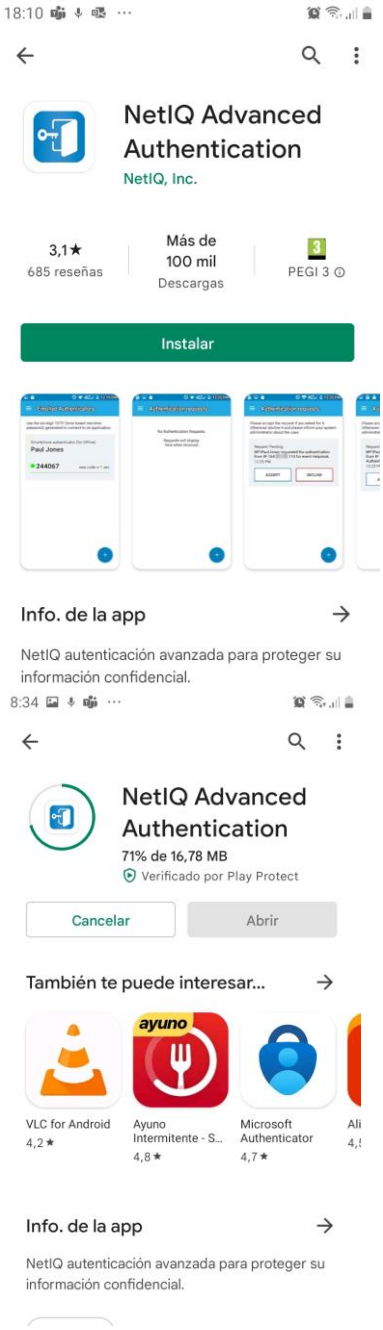
2. Instalar herramienta NetIQ Advanced Authentication

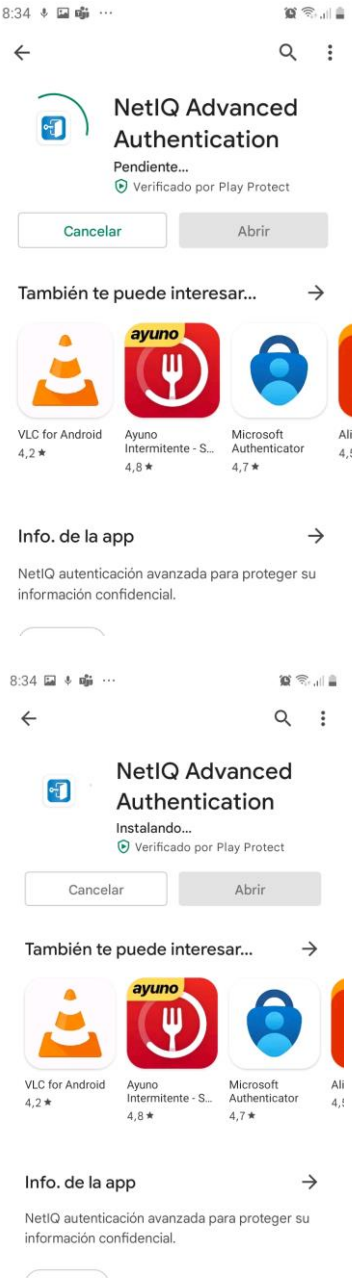
La instalación de la herramienta se diferenciará:

- Sistema Operativo Android
- Sistema Operativo iOS

2.1. Sistema Operativo Android

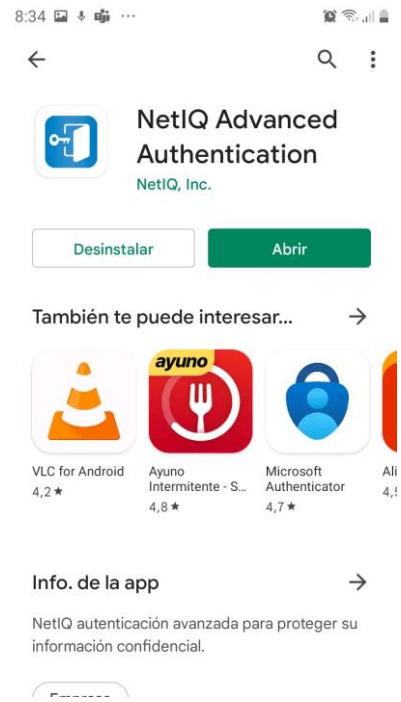
1. Se debe buscar la aplicación **NetIQ Advanced Authentication** en el Play Store y pulsar el botón **Instalar**:

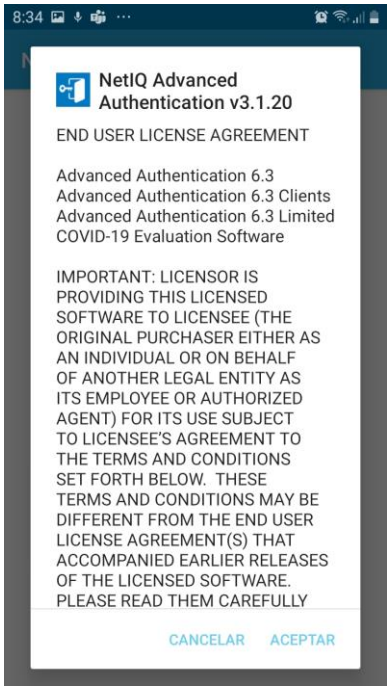


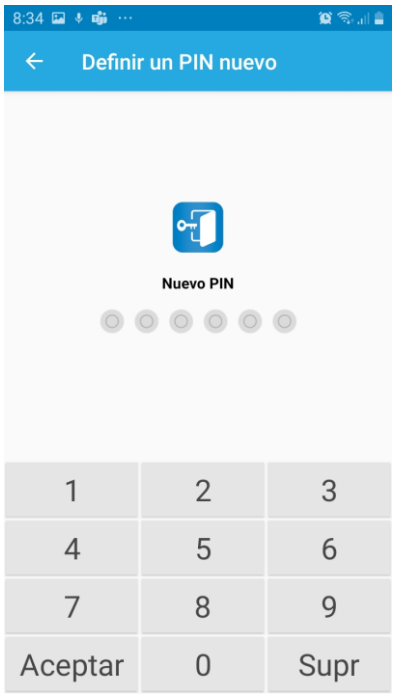


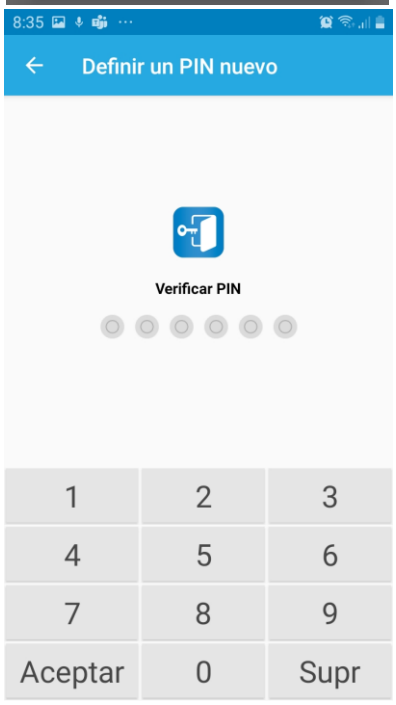
2. Una vez instalada la aplicación **NetIQ Advanced Authentication**, se debe proceder a su configuración en el dispositivo.

3. Para ello, pulsar el botón **Abrir**, aceptar las **condiciones** e introducir el **PIN** de 6 dígitos que se desee:

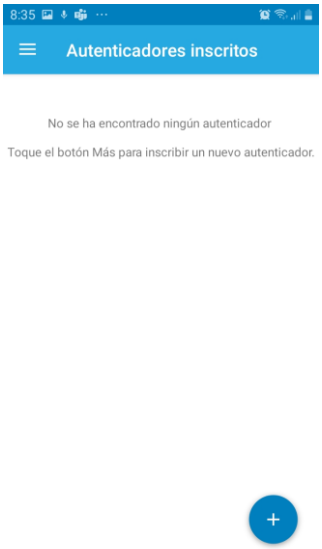


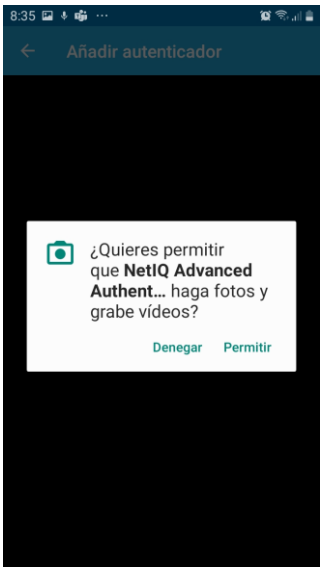


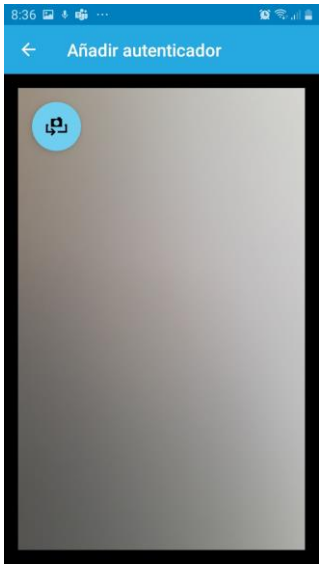




4. A continuación, inscribiremos el dispositivo en el portal del Segundo Factor de Autenticación del IB – Salut. Para ello, pulsar el botón **+**, dar permiso para el uso de la cámara y escanear el **código QR** obtenido en el portal:



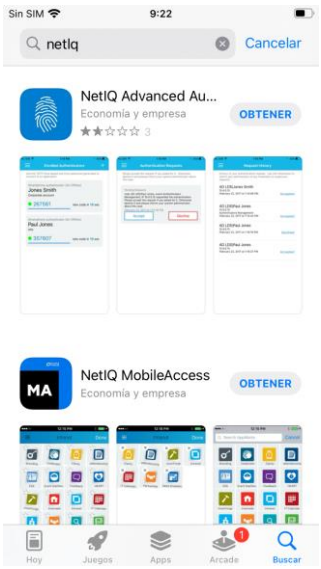


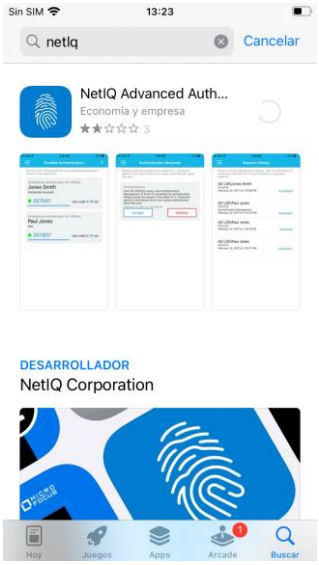


NOTA: para obtener el código QR necesario de la imagen inferior, ir a 3. Portal Segundo Factor Autenticación, apartado método inscripción de **Teléfono inteligente**.

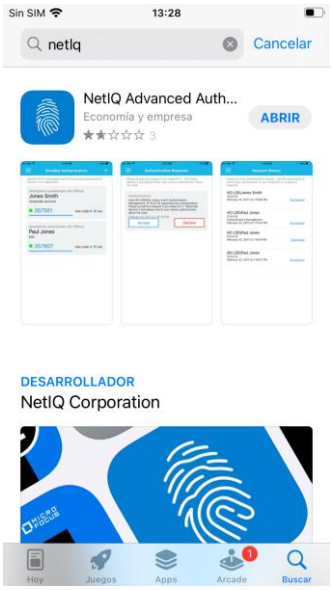
2.2. Sistema Operativo iOS

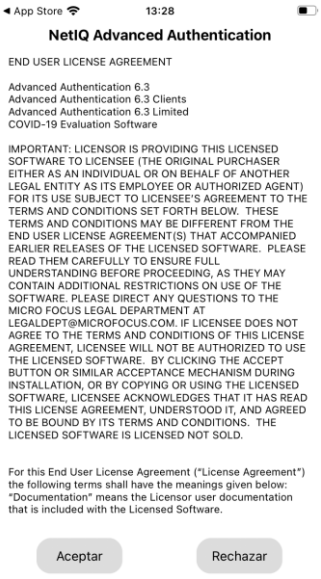
1. Se debe buscar la aplicación **NetIQ Advanced Authentication** en la App Store y pulsar el botón **Obtener**:

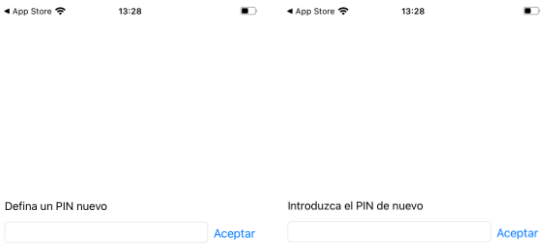




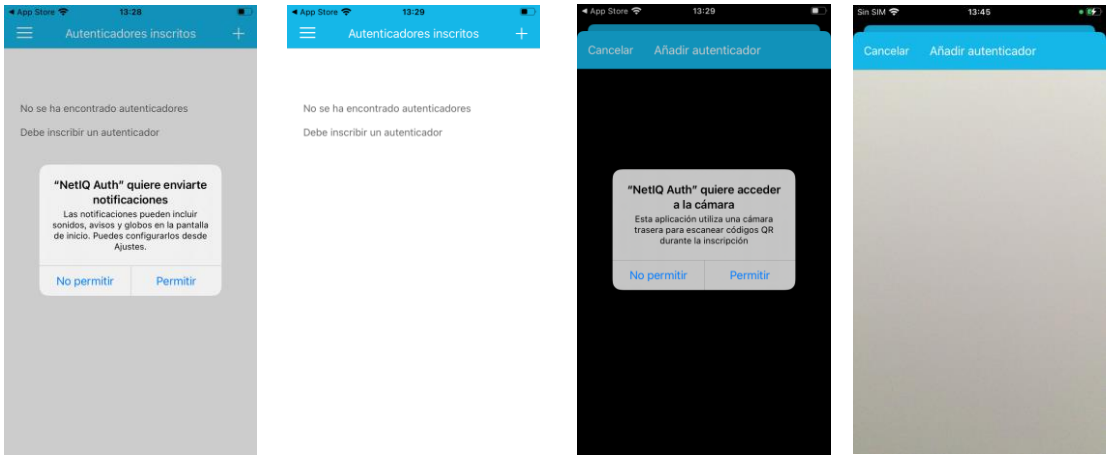
2. Una vez instalada la aplicación **NetIQ Advanced Authentication**, se debe proceder a su **configuración** en el dispositivo.
3. Para ello, pulsar el botón **Abrir**, aceptar las condiciones e introducir el **PIN** que se desee:







4. A continuación, inscribiremos el dispositivo en el portal del Segundo Factor de Autenticación del IB – Salut. Para ello, primero solicita permisos para que la aplicación envíe notificaciones. Una vez permitidas las notificaciones, pulsar el botón **+**, dar permiso para el uso de la cámara y escanear el código QR obtenido en el portal:



NOTA: para obtener el código QR necesario de la imagen inferior, ir a 3. Portal Segundo Factor Autenticación, apartado método inscripción de **Teléfono inteligente**.

3. Portal Segundo Factor de Autenticación

A través del Portal Segundo Factor de Autenticación del IB – Salut, el usuario podrá obtener el código QR para inscribir el dispositivo.

Se ha seleccionado el método de **Teléfono inteligente** como principal método, para facilitar al usuario el uso del múltiple factor de autenticación, ya que de este modo le llegará un mensaje a través de la aplicación instalada en el dispositivo, que sólo tendrá que confirmar o rechazar.

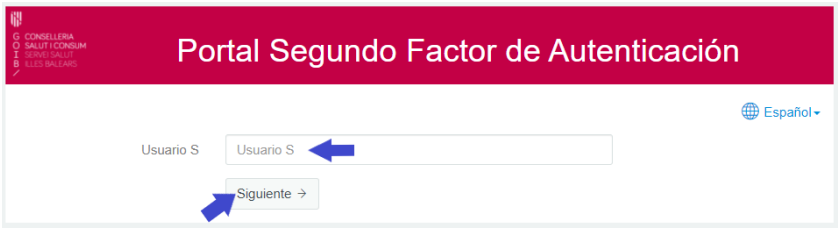
Para el resto de métodos (ver Anexo), la utilización es más tediosa para el usuario, por lo que no se recomiendan.

Destacar que, sólo debe realizarse la inscripción del dispositivo en este portal, **una vez**, excepto si se cambia de dispositivo, que deberá volver a realizar el proceso de inscripción del nuevo dispositivo.

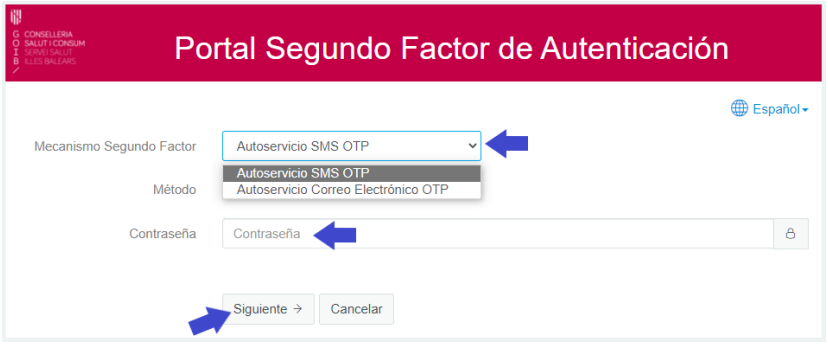
Cada usuario sólo podrá tener un único dispositivo inscrito.

Para acceder al portal, se debe ir a la dirección: https://mfa.ssib.es/

1. Introducir el **usuario S** en el campo y pulsar el botón **Siguiente**:



2. Introducir la **contraseña** del usuario S y pulsar el botón **Siguiente**:



En este punto, el portal enviará un SMS por defecto al teléfono informado en OIM con la clave para poder seguir el proceso, de ahí la importancia de tenerlo bien informado.

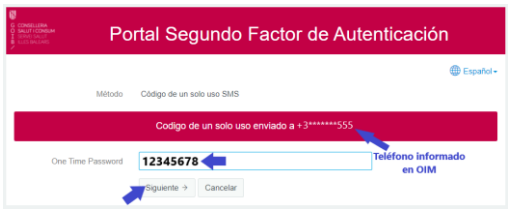
Ejemplo SMS

En el caso de que no se tenga el teléfono móvil informado en OIM, se debe seleccionar "**Autoservicio Correo electrónico OTP**". En este caso, llegará un mensaje al correo electrónico informado en OIM:

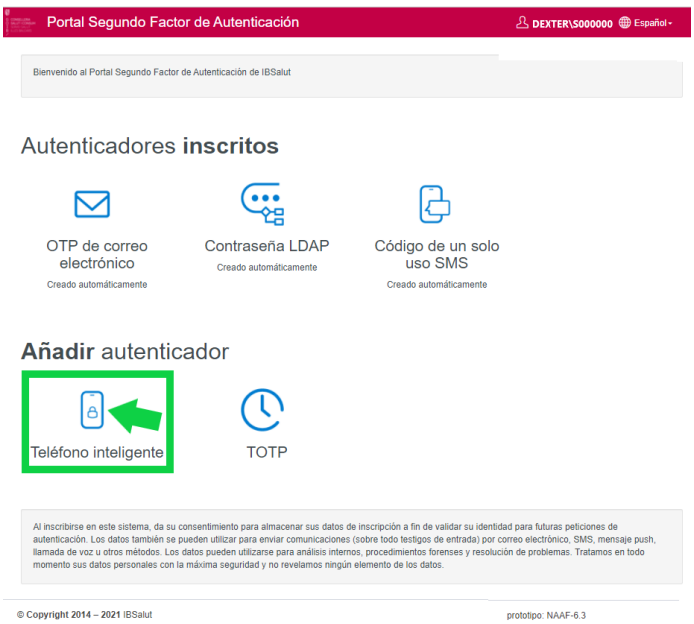
Ejemplo SMS

La clave de un solo uso, es imprescindible para poder continuar el proceso, ya que en el siguiente paso hay que introducirla. Se recuerda que esta clave es temporal, sólo dura 2 minutos.

3. Introducir la **clave de 8 dígitos recibida por SMS o por correo electrónico** y pulsar el botón **Siguiente** (Recordar, la clave sólo será válida durante 2 minutos):



4. Aparecen los métodos para inscribirse en el portal del Segundo Factor de Autenticación del IB – Salut. Seleccionar el método **Teléfono inteligente**:



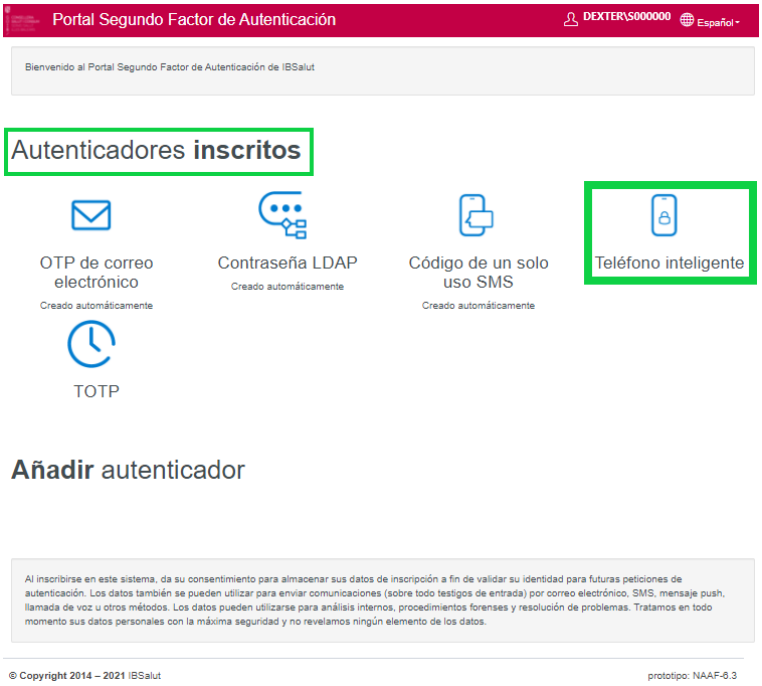
5. A continuación, se debe pulsar sobre el botón **Guardar** para que aparezca el código QR que debemos escanear en la aplicación **NetIQ Advanced Authentication** instalada en el dispositivo que se está inscribiendo:

6. Abrir la aplicación NetIQ Advanced Authentication instalada en el Smartphone, pulsar el **botón +** para inscribir un Autenticador y acercar el Smartphone a la pantalla del ordenador para que se lea el código QR:

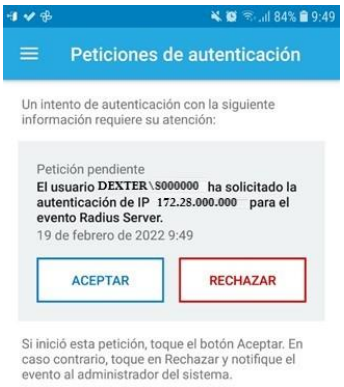
NOTA: el código QR sólo dura **1 minuto** en la pantalla. En caso de que desaparezca, volver a pulsar el botón "**Guardar**" para generar otro nuevo.

En el caso de que se supere el tiempo límite de inscripción, se debe volver a pulsar el botón **Guardar** para generar un nuevo código QR.

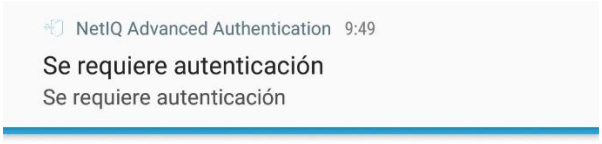
Una vez realizado este proceso, ya tendremos el dispositivo inscrito en el portal y **sólo se tendrá que utilizar la aplicación NetIQ Advanced Authentication**:



Por tanto, cada vez que se realice un acceso remoto, se podrán validar cómoda y fácilmente desde nuestro dispositivo móvil, con tan sólo **Aceptar** o **Rechazar** el mensaje desde la aplicación NetIQ, siempre que se tenga abierta:

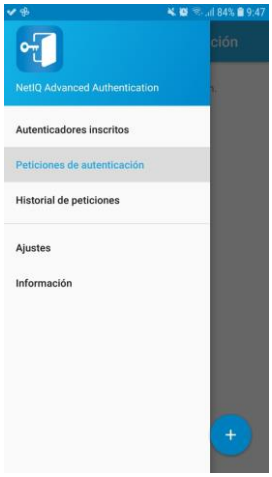


Si la aplicación NetIQ no está abierta, aparecerá el mensaje:



Se debe abrir la aplicación y pulsar **Aceptar** o **Rechazar**.

En el caso del mensaje no se vea, se puede ir al menú y revisar **Peticiones de autenticación**:



Este mensaje, se enviará hasta **3 veces**, para dar el tiempo suficiente al usuario para **Aceptar**. Después de finalizar el tiempo máximo estimado, se denegará el acceso de forma automática.

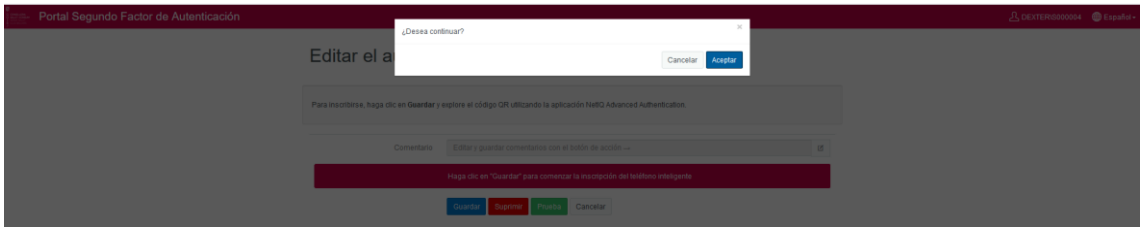
Como se ha indicado, una vez inscrito el dispositivo, no será necesario volver a utilizar el portal del Segundo Factor de Autenticación del IB – Salut, excepto si se quiere cambiar el dispositivo o el método dónde recibir los mensajes de los accesos remotos que se vayan solicitando.

Para ello, se debe entrar al portal de la misma forma que se ha explicado:

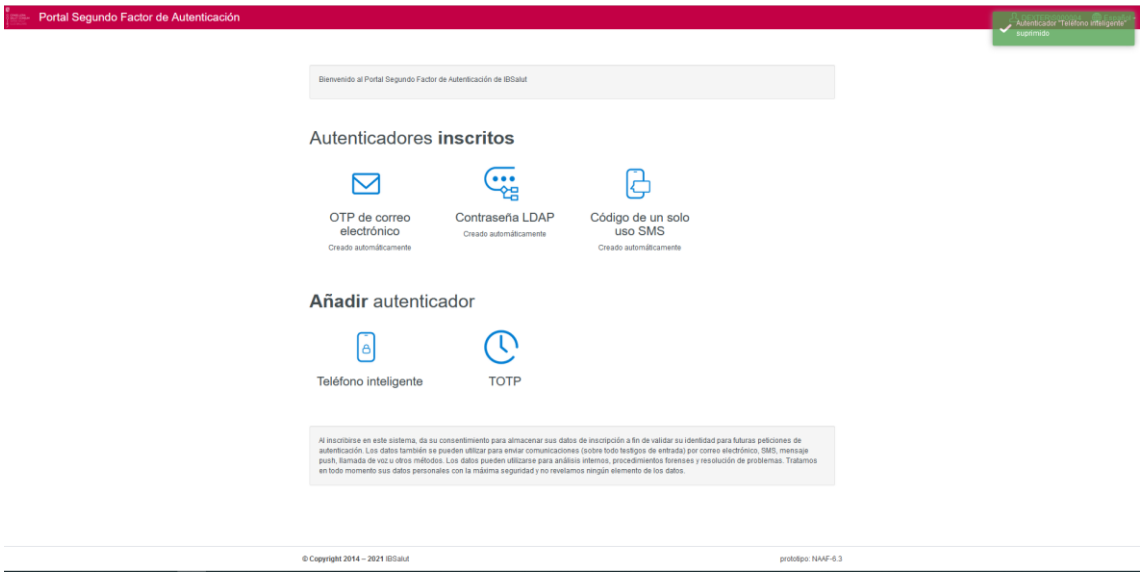
1. Usuario S
2. Contraseña Usuario S
3. Seleccionar la forma en que se quiere recibir la clave (seleccionar SMS o Correo electrónico):

4. Seleccionar el Autenticador inscrito **Teléfono inteligente**:

5. Pulsar el botón **Suprimir**:



6. Pulsar el botón **Aceptar**:



7. Inscribir el nuevo dispositivo o método de la forma explicada.

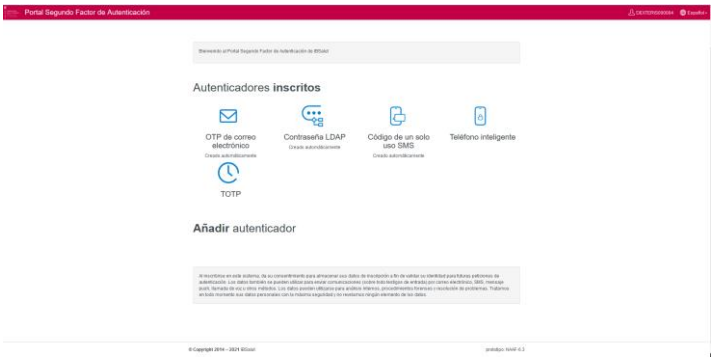
El botón **Prueba** que se observa al editar el autenticador Teléfono inteligente, sirve para comprobar que llega el mensaje a la aplicación NetIQ instalada en el dispositivo inscrito.

Llega el mensaje a la aplicación NetIQ del dispositivo inscrito y espera que se pulse Aceptar o Rechazar en la misma:

En el caso de que se acepte, aparece un mensaje en la parte superior derecha indicando en verde equivalente a que el acceso remoto se ha aceptado:

En el caso de que se rechace, aparece un mensaje en la parte superior derecha indicando en azul equivalente a que el acceso remoto se ha rechazado:

El botón **Cancelar** vuelve a los Autenticadores inscritos:

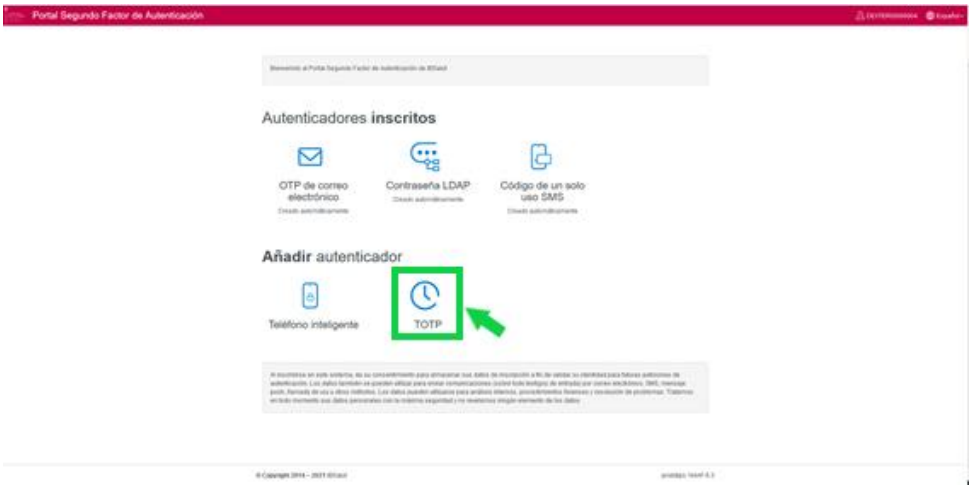


4. Anexo

4.1. Método TOTP

Para utilizar este método, será necesario:

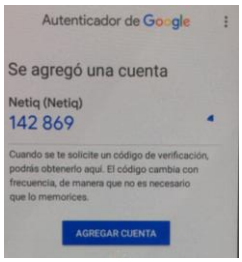
1. Instalar una aplicación compatible de autenticación (Google authenticator para Android e iOS, NetIQ Advanced Authentication para Android e iOS, Yubico para Windows, Authenticator para MacOS, …) en el dispositivo que se deseen recibir las claves para los accesos.
2. Seleccionar el método TOTP en el portal Segundo Factor de Autenticación del IB-Salut (https://mfa.ssib.es/).



3. Escanear el código QR con la aplicación seleccionada en el primer punto. En caso de que la aplicación seleccionada no pueda leer códigos QR, se deberá utilizar el código TOTP generado de forma manual explicado al final de este apartado.

Aparecerá en la aplicación instalada la clave que se debe introducir para realizar el acceso. Esta clave cambiará cada 30 segundos, como por ejemplo:

NetIQ



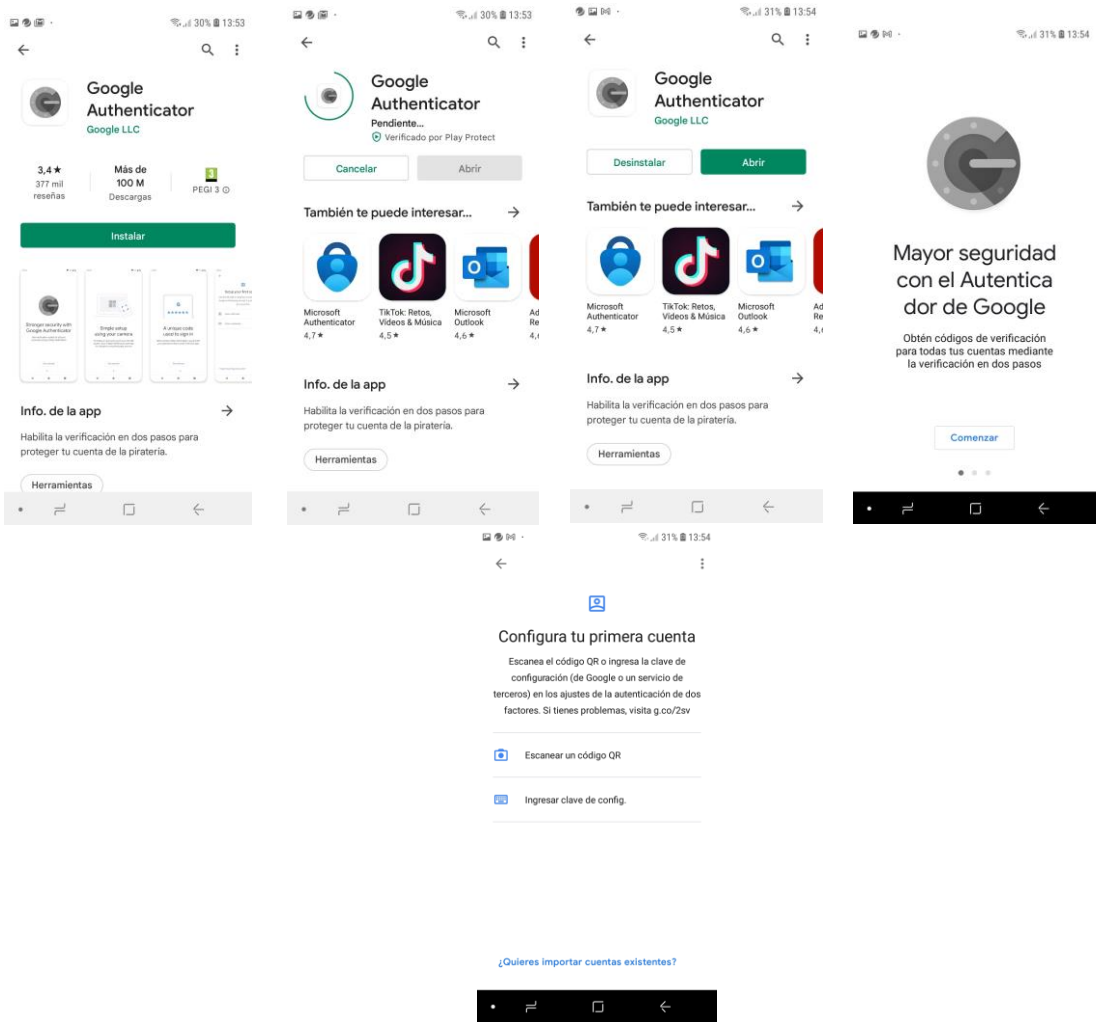
Google Autenticator

4.1.1. Google Authentication

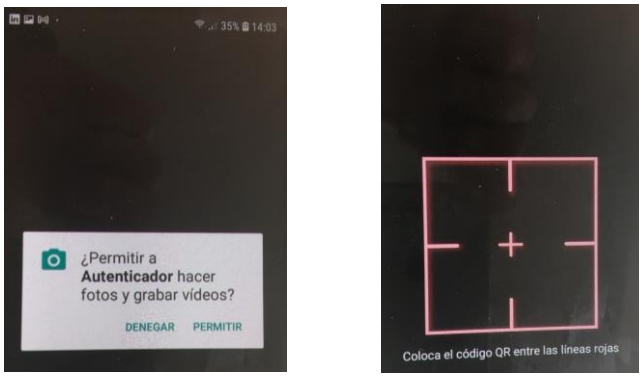
Si se utiliza cualquier otra aplicación de autenticación compatible, en lugar de la recomendada NetIQ Advanced Authentication, como por ejemplo Google Authenticator, el funcionamiento será el mismo.

4.1.1.1. Sistema Operativo Android

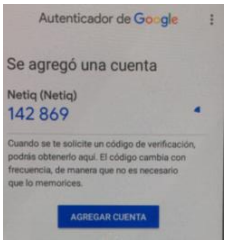
1. Se debe instalar la aplicación en el dispositivo dónde se desean recibir las claves de acceso.



2. Escanear el código QR que se facilita al inscribir el método en el portal Segundo Factor de Autenticación del IB-Salut:



3. Utilizar la clave temporal que aparezca en la aplicación.



4.1.1.2. Sistema Operativo iOS

1. Se debe instalar la aplicación en el dispositivo dónde se desean recibir las claves de acceso.
2. Escanear el código QR que se facilita al inscribir el método en el portal Segundo Factor de Autenticación del IB-Salut.
3. Utilizar la clave temporal que aparezca en la aplicación.

4.1.1.3. Sistema Operativo MacOS

1. Se debe instalar la aplicación Authenticator en el dispositivo dónde se desean recibir las claves de acceso.
2. El código QR que se facilita al inscribir el método en el portal Segundo Factor de Autenticación del IB-Salut debe copiarse (arrastrando) en la aplicación Authenticator.

4.1.1.4. Uso código TOTP de forma manual

Para utilizar el código TOTP generado de forma manual:

1. Se debe pulsar el campo “Secreto”, para que se muestre la clave de acceso temporal para realizar el acceso remoto:

2. Introducir la clave temporal en el autenticador seleccionado (NetIQ, Google Authentication, …) correspondiente.