

Guía de usuario para acceder a IESFACIL desde CASA vía <https://remotocentros.educa.jcyl.es>

1. PROCEDIMIENTO PRIMERA VEZ:

Paso 0: Pida al Equipo Directivo de su centro que le proporcione la carpeta con la aplicación IESFACIL. Es una aplicación portable, es decir, no necesita instalación. Simplemente hay que copiar la carpeta en el Disco duro C:\. Si lo desea, puede sacar un acceso directo al Escritorio haciendo clic derecho sobre el archivo ejecutable > Enviar a > Escritorio (crear acceso directo).

Paso 1: Instale en su teléfono móvil la aplicación Google Authenticator. Esta aplicación incrementa la seguridad en el proceso de identificación del usuario mediante la generación de códigos aleatorios temporales (segundo factor de autenticación o 2FA) y será necesaria si se valida con usuario y contraseña de 'educa' o con certificado electrónico de la FNMT. No necesitará estos códigos de Google Authenticator si va a autenticarse utilizando su DNIe (DNI electrónico).



¡ATENCIÓN! El uso de estos códigos temporales necesita que los **sistemas estén sincronizados**. Por ello, se le recomienda tener configurado el ESTABLECIMIENTO AUTOMÁTICO DE FECHA Y HORA tanto en el equipo con el que accede en remoto como en el dispositivo móvil que le proporciona el código aleatorio temporal.

Paso 2: Acceda desde el navegador web de su PC a la siguiente dirección URL:
<https://remotocentros.educa.jcyl.es>.



PORTAL DE ACCESO REMOTO
A LA RED CENTROS EDUCATIVOS
DE LA JUNTA DE CASTILLA Y LEÓN

Portal de Acceso Remoto a Centros Educativos

Usuario

Contraseña

Método de autenticación

Seleccione el método de autenticación que va a utilizar.

En caso de utilizar un método de autenticación distinto a certificado electrónico (FNMT o DNIe) indique sus credenciales y asegúrese de que el equipo que está usando y el dispositivo móvil que le proporciona el segundo factor de autenticación (2FA) tienen los dos la hora correcta.

Mantenga la posibilidad de usar varios métodos de autenticación por si en algún momento no pudiera usar alguno de ellos, pero sí otro de los demás.

[Información sobre protección de datos](#)



Nota 1: Si lo desea, puede crear un acceso directo a la dirección URL haciendo clic derecho en una zona libre del Escritorio > Nuevo > Acceso Directo > En 'Escriba la ubicación del elemento' escribir <https://remotocentros.educa.jcyl.es> > En 'Escriba un nombre para este acceso directo' escribir Remoto centros > Finalizar.

Seleccione el método que vaya a utilizar y selecciones Acceder (en caso de usar Remoto-2FA, tendrá que introducir su usuario y contraseña de 'educa').

Nota 2: Si en lugar de seleccionar Remoto-2FA selecciona Remoto-DNIE, podrá utilizar su DNI electrónico para identificarse (necesitará un lector y la contraseña de su DNIE). Si selecciona Remoto-FNMT-2FA podrá utilizar su certificado electrónico de la FNMT y el código generado por Google Authenticator para identificarse. Usando estas opciones no tendrá que introducir usuario y contraseña.

Paso 3: En el caso de que utilice uno de los métodos que requieren segundo factor de autenticación, tras validarse la primera vez le aparecerá un código QR que deberá escanear con la aplicación Google Authenticator instalada en el Paso 1, para vincular su usuario a su teléfono móvil.


Agregar _____ cuenta de usuario para la aplicación de autenticación de dos factores

Deberá instalar una aplicación de autenticación de dos factores (Google Authenticator) en su smartphone o tablet.

1. Configure la aplicación:

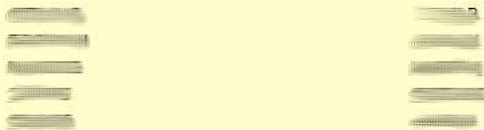
Abra la aplicación de autenticación de dos factores y añada la cuenta de usuario "_____" escaneando el código QR siguiente.

Si no puede utilizar un código QR, introduzca [este texto](#)



2. Guardar códigos de copia de seguridad:

Los códigos de copia de seguridad se pueden utilizar para acceder a su cuenta en caso de que pierda el acceso al dispositivo y no pueda recibir los códigos de autenticación de dos factores. Los siguientes códigos de copia de seguridad son solo para un uso. Le recomendamos que los guarde de forma segura.



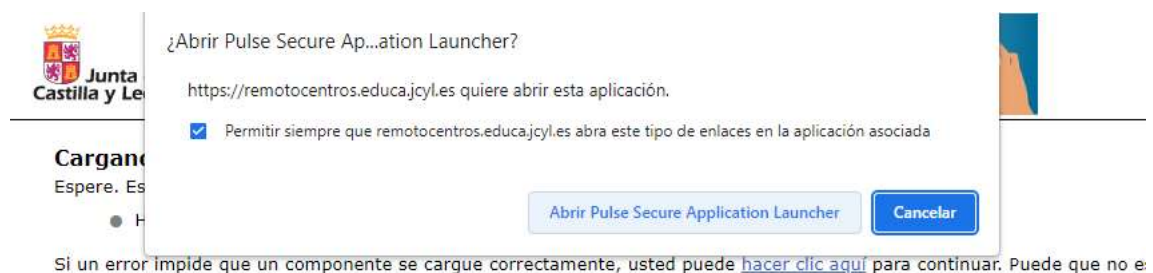
3. Introducir el código token que genera la aplicación:



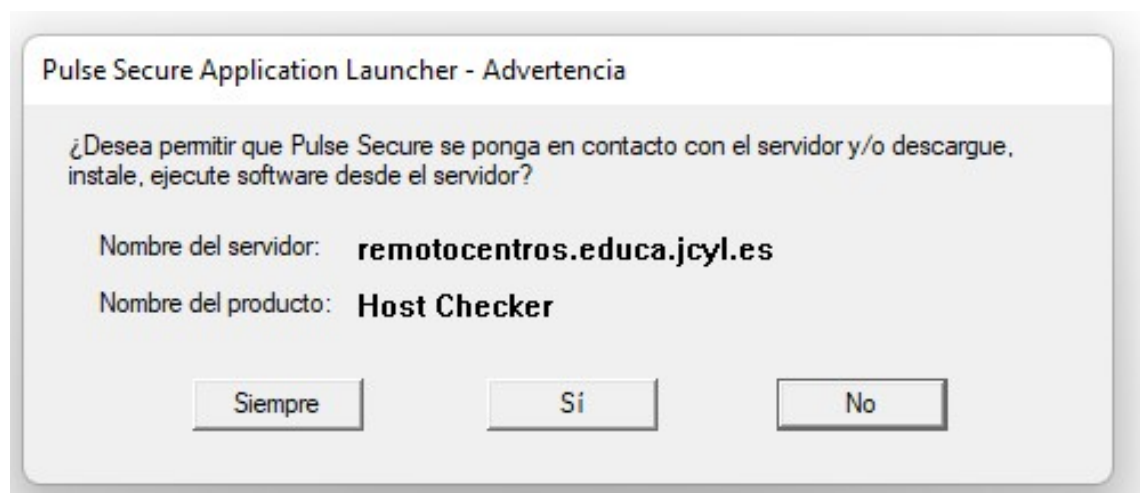
Una vez vinculada su aplicación Google Authenticator, vuelva al sistema de acceso remoto (navegador web) y, como le indican las instrucciones que aparecen en pantalla, copie en un lugar seguro los 10 códigos de copia de seguridad. Son códigos de un solo uso que podría utilizar en caso de que no pueda generar códigos aleatorios temporales con su aplicación Google Authenticator, por ejemplo, porque ha tenido un problema con su dispositivo móvil. Estos códigos de copia de seguridad son, por tanto, alternativos a los códigos aleatorios temporales generados con su aplicación Google Authenticator.

Acto seguido, introduzca el código generado por Google Authenticator (que cambian cada 30 segundos, ¡ATENCIÓN! Si queda poco tiempo para que terminen los 30 segundos de validez del código aleatorio temporal, le recomendamos que espere a que se inicie el tiempo de validez de un código aleatorio temporal nuevo) y haga clic en 'Iniciar sesión':

Paso 4: La primera vez habrá que permitir que se instale la aplicación 'Host Checker' a través de un Lanzador de Aplicaciones (Se recomienda activar la casilla 'Permitir siempre...'). Haga clic en 'Abrir Pulse Secure Application Launcher'.

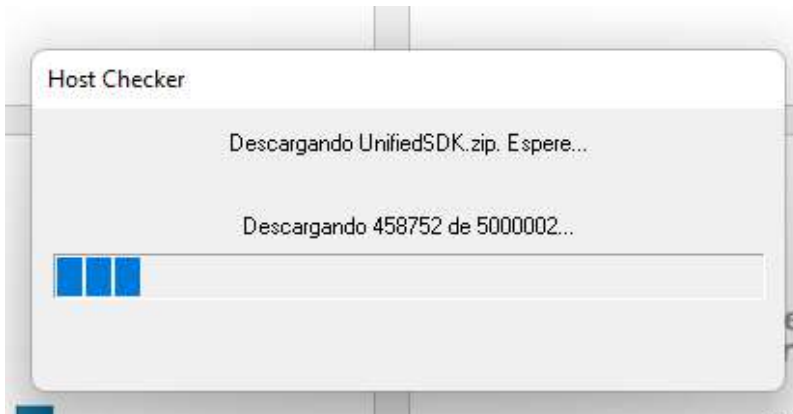


Para que no pregunte más veces, se recomienda hacer clic en 'Siempre':





La aplicación se descargará:



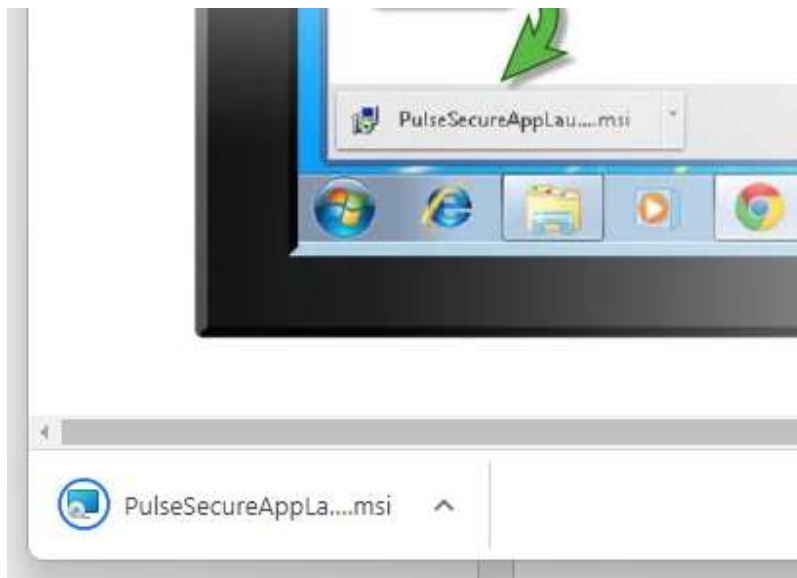
Si no se arranca el iniciador de aplicaciones de forma automática, en la siguiente ventana, haga clic en 'Descargar':

Parece que el iniciador de aplicaciones no está instalado. Descárguelo ahora para continuar.

Descargar

Si cree que el iniciador de aplicaciones ya está instalado, seleccione [Intentar de nuevo](#) para encontrarlo.

Se descargará la aplicación PulseSecureAppLauncher.msi. Ejecútela.





Después haga clic en el enlace 'haga clic AQUÍ':

Cuando haya completado los pasos anteriores, [haga clic AQUÍ](#) para continuar iniciando .
Recomendamos seleccionar "recordar" y "siempre" durante el proceso de instalación.

Una vez que Host Checket evalúe el PC desde el que está accediendo ...

Cargando componentes...

Espere. Este proceso puede tardar varios minutos.

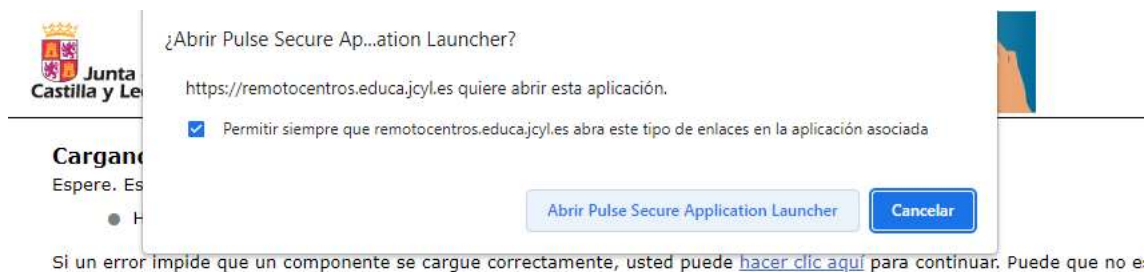
● Host Checker..

Si un error impide que un componente se cargue correctamente, usted pu

... y sea satisfactoria, se llegará a la página:



Seleccionado Pulse para iniciar el cliente Pulse Secure. Puede que haya que permitir de nuevo el Lanzador de Aplicaciones.

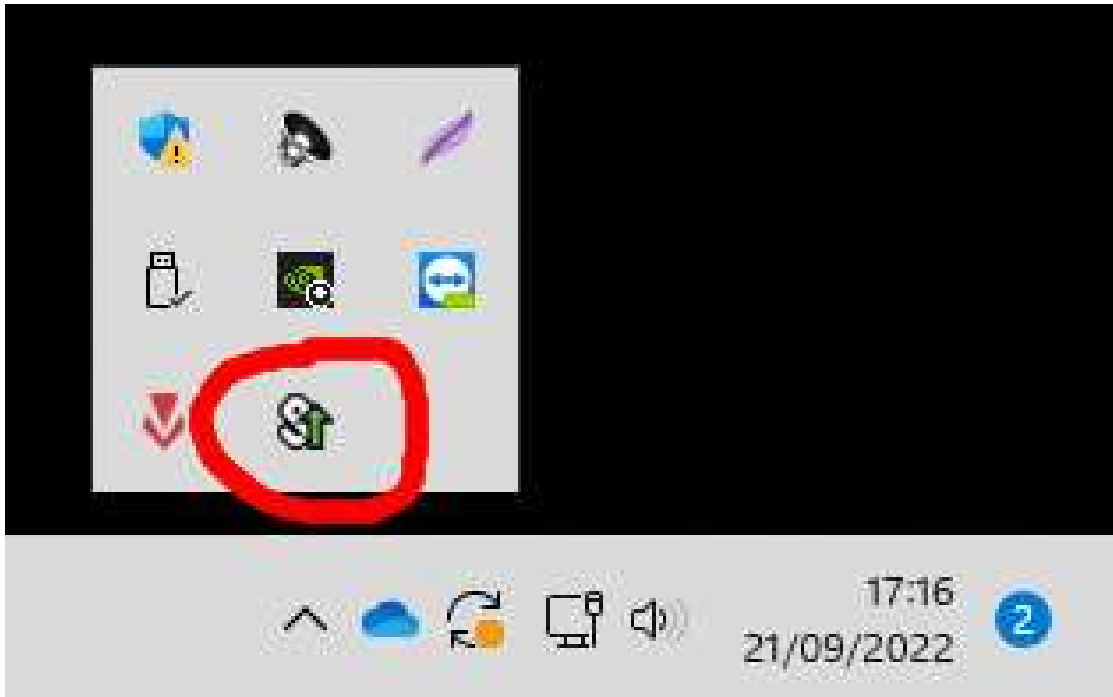


Se descargará e instalará el cliente de Pulse Secure.





Cuando esté iniciado, aparecerá en los iconos de la barra de tareas la aplicación 'Pulse Secure'



A partir de ese momento, ya se podrá utilizar IESFACIL.



2. PROCEDIMIENTO RESTO DE VECES:

En el Paso 3 aparecerá directamente la ventana para introducir el código generado por Google Authenticator:

Portal de Acceso Remoto a Centros Educativos

Página de credenciales adicionales de Pulse Connect Secure for [redacted]

Abra la aplicación de autenticación de dos factores en el dispositivo para ver su código de autenticación y verificar su identidad.

Si actualmente no tiene acceso al dispositivo, utilice uno de los códigos de copia de seguridad que ha guardado anteriormente.

Código de autenticación:

Se iniciará automáticamente la carga de componentes.

Cargando componentes...

Espere. Este proceso puede tardar varios minutos.

- Host Checker.

Si un error impide que un componente se cargue correctamente, usted puede [hacer clic aquí](#) para continuar. Puede que no estén disponibles todas las funciones.

Y después habrá que hacer clic en iniciar sesión:

Y ya se podrá utilizar IESFACIL.

Nota 3: Si después de agregar su cuenta a Google Authenticator usted cambia de teléfono móvil, puede ir a la opción 'Transferir cuentas' para pasar la cuenta al Google Authenticator del nuevo teléfono móvil.



3. BLOQUEO DE CUENTAS

Su cuenta **se bloqueará durante 30 minutos** si introduce 5 códigos erróneos seguidos. Deberá esperar para poder introducir nuevos códigos.



Portal de Acceso Remoto a la Red Corporativa de la Junta de Castilla y León

Su cuenta TOTP se ha bloqueado.

Usuario

Contraseña

Acceder

Seleccione el método de autenticación que va a utilizar.

En caso de utilizar un método de autenticación distinto a certificado electrónico (FNMT o DNIe) indique sus credenciales.

Estando autenticado, puede ver sus códigos de copia de seguridad o generar nuevos pinchando en “Preferencias”, “General”, “Ver” o “Generar”, respectivamente. Si va generando con suficiente antelación nuevos códigos puede ampliar el tiempo de uso del acceso remoto sin Google Authenticator.

Junta de Castilla y León PORTAL DE ACCESO A LA RED CORPORATIVA DE LA JUNTA DE CASTILLA Y LEÓN

Logged-in as: Inicio Preferencias Sesión 07:59:25 Cerrar sesión Examinar

Preferencias

Inicio del usuario **General** Aplicaciones Avanzado

Cambiar contraseña

Contraseña anterior:

Nueva contraseña:

Confirmar contraseña: Cambiar contraseña

Códigos de copia de seguridad TOTP

Ver Generar

Copiar en el portapapeles



4. SOPORTE A CONSULTAS E INCIDENCIAS

Para recibir soporte debe contactar con su **Centro de Atención a Usuarios**. Indique claramente su **nombre de usuario** y la **dirección web del servicio** de acceso remoto al que accede en:

(<https://remotocentros.educa.jcyl.es>).

Menú

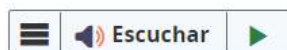
Temas

Elija una opción

Información

Centros Educativos Digitales

Centros Educativos Digitales



Atención a Usuarios

Acceso a ASISTA - Educación (Sólo activo para miembros de equipos directivos de centros públicos)

Tipo de acceso	Forma de acceso	Qué puedo solicitar	Disponibilidad	Horario
Teléfono	983 41 87 45	Consultas e incidencias	De Lunes a Jueves	8:00 a 19:00
			Viernes	8:00 a 15:00

O también puede ponerse en contacto con el coordinador SIGIE de su provincia.