GENERALITAT VALENCIANA
Conselleria de Sanitat Universal i Salut Pública

DEPARTAMENT DE SALUT DE LA RIBERA

Guía usuario VPN

Clasificación	Manual
Título del documento	HR-MAN-Guia Usuario VPN 5.0.docx
Autor	Sistemas
Fecha	24/03/2020
Páginas	12

ÍNDICE DEL DOCUMENTO

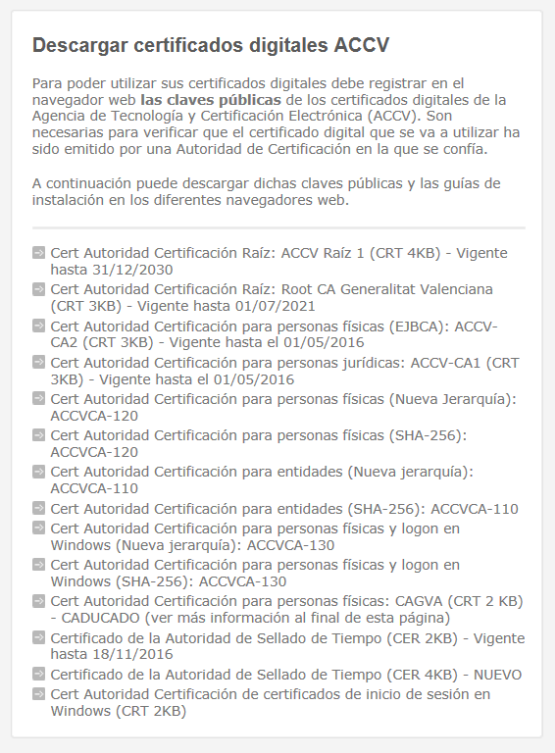
1. Objeto

El objeto de la siguiente guía, es detallar las acciones a realizar para configurar el acceso VPN al Hospital Universitario de la Ribera.

2. Guía de usuario

A continuación se detallan los requisitos indispensables para la conexión a la VPN:

1. **Conexión a Internet**.
2. **Alta en la VPN de la Conselleria tramitada por el jefe de servicio**. Una vez tramitada el alta, el usuario recibirá un correo del equipo de Arterias (CGRA) indicando que se ha creado el usuario y que se deben poner en contacto con ellos (llamando el teléfono 902 20 20 03) para establecer la contraseña del servicio de VPN. Este usuario y contraseña serán necesarios para realizar la posterior conexión a la VPN.
3. **Certificado de firma digital ACCV** (solicitar a RRHH).
4. Para la **lectura del certificado**:
   i. solicitar en RRHH (certificado en fichero) o
   ii. descargar certificado con tarjeta https://www.accv.es/ciudadanos/area-personal-de-servicios-de-certificacion/ o
   iii. lector de firma digital y tarjeta ACCV.
5. **Instalar certificados ACCV**.
   https://www.accv.es/ayuda/descargar-certificados-digitales/



En este punto se tienen que descargar los certificados:

- ACCVCA-110
- ACCVCA-120
- ACCVRAIZ1
- ROOTCA

Para instalar los certificados descargados, se hace doble click en cada uno de los ficheros descargados correspondientes a los certificados, y se pulsa en "Siguiente" en todas las pantallas manteniendo los valores por defecto, sin realizar ningún cambio.

6. Instalar Cliente VPN – Cisco AnyConnect.

Acceder a la URL → http://www2.san.gva.es/accesos/

Descargar el correspondiente según sistema operativo e instalar. Para realizar la instalación hay que pulsar en "Siguiente" en todas las pantallas y poniendo los valores por defecto sin realizar ningún cambio.

7. Instalación del Agente Cytomic EndPoint Agent

Los siguientes enlaces le permitirán descargar el instalador en su equipo. Una vez descargado tendrá que ejecutarlo (doble click) para proceder a su instalación. A partir de ese momento el programa estará activo y arrancará automáticamente cada vez que encienda el equipo. Para elegir el instalador adecuado dispone de varias opciones:

En caso contrario, o si hubiera tenido alguna dificultad con el anterior:

1. En equipos con Windows: https://manage.cytomicmodel.com/api/v1/accounts/8dcd781b-068e-4c3f-b6b0-9246dc69e613/sites/a3c25366-c340-41d4-9805-4e8d8075fc63/installers?installerType=2&platform=1&managedConfigurationId=106815ce-6fb6-4efa-9b09-e2cb309f7444&customGroupId=5a00c15a-2dd8-42cb-9abe-89e812cb8b05&integrationGroupType=0
2. En equipos con MacOS:

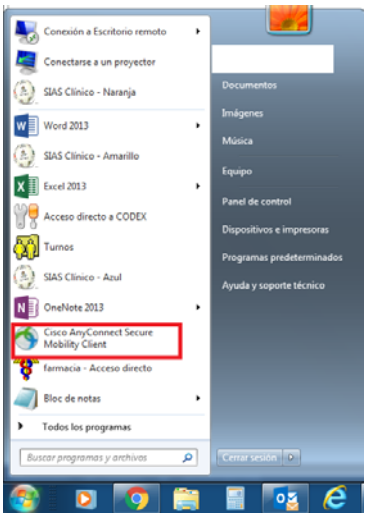
https://manage.cytomicmodel.com/api/v1/accounts/8dcd781b-068e-4c3f-b6b0-9246dc69e613/sites/a3c25366-c340-41d4-9805-4e8d8075fc63/installers?installerType=2&platform=3&managedConfigurationId=106815ce-6fb6-4efa-9b09-e2cb309f7444&customGroupId=9fe2917e-346b-4a14-a827-eca2446cf5d5&integrationGroupType=0

3. En equipos con Linux:
https://manage.cytomicmodel.com/api/v1/accounts/8dcd781b-068e-4c3f-b6b0-9246dc69e613/sites/a3c25366-c340-41d4-9805-4e8d8075fc63/installers?installerType=2&platform=2&managedConfigurationId=106815ce-6fb6-4efa-9b09-e2cb309f7444&customGroupId=9fe2917e-346b-4a14-a827-eca2446cf5d5&integrationGroupType=0

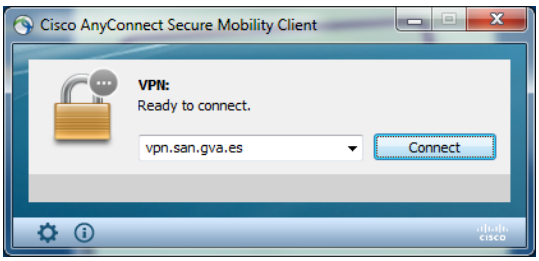
8. Conexiones de trabajo.

Una vez instalado todo, para realizar la conexión a la VPN se tienen que seguir los siguientes pasos:

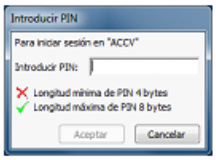
- Para conectarse a la VPN, se debe abrir el programa **AnyConnect de Cisco** (instalado en el punto anterior), que estará iniciado en la barra de tareas, junto al reloj de Windows (abajo, a la derecha). También ejecutar el programa desde los accesos directos creados tras la instalación

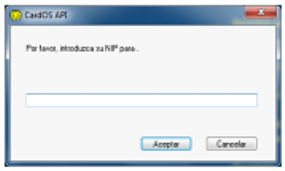


- **Antes de pulsar el botón** Connect. El usuario tiene que tener insertada la tarjeta de firma electrónica y la aplicación solicitará el PIN de la tarjeta. O tener instalado el certificado software en su equipo.
- Indicar la dirección de la VPN a la que conectarse. Introducir “vpn.san.gva.es” y pulsar en Connect.

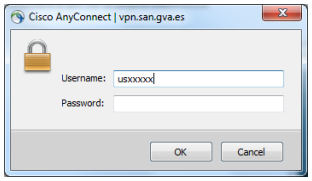


- Si se tiene el certificado instalado en el equipo se pedirá el usuario y contraseña de la VPN y no se pedirá el PIN de la tarjeta.





- En el siguiente paso, Cisco AnyConnect nos pide las credenciales de usuario VPN. Estas credenciales se nos han debido de proporcionar como parte del proceso de alta en la VPN (punto 2). En caso de que el usuario haya sido dado de alta en la VPN y no disponga o recuerde dichas credenciales, tendrá que ponerse en contacto con el equipo de Arterias (CGRA) 902202003/961961555.

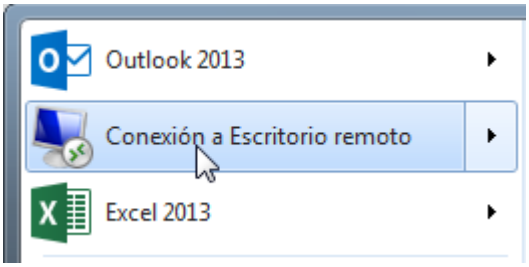


- Cuando se establezca la conexión VPN, se mostrará un mensaje como el que se puede ver a continuación.

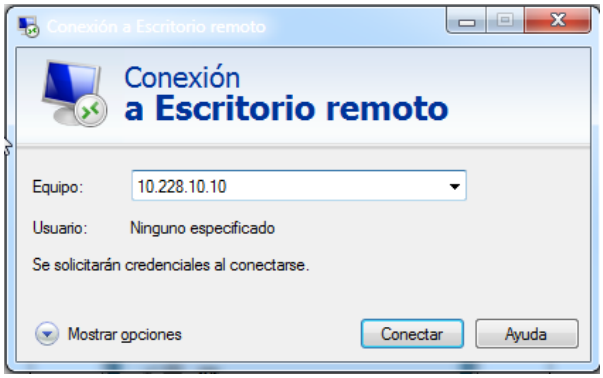
- Cuando se finalice con el trabajo diario, se tiene que cerrar la conexión del Cliente Cisco AnyConnect.

- Una vez establecida la VPN hay que realizar la conexión por Escritorio Remoto (para estos se necesitaran los datos de Nombre de equipo / IP del equipo al que hay que conectarse) o conectarse a través de citrix **(http://172.18.15.18).**

  A continuación se detallan los pasos para **realizar la conexión por Escritorio Remoto**:

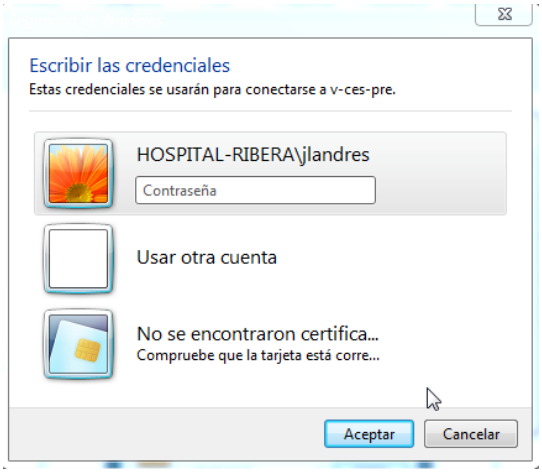


- En la pantalla siguiente introducir los datos de nombre de equipo / IP.

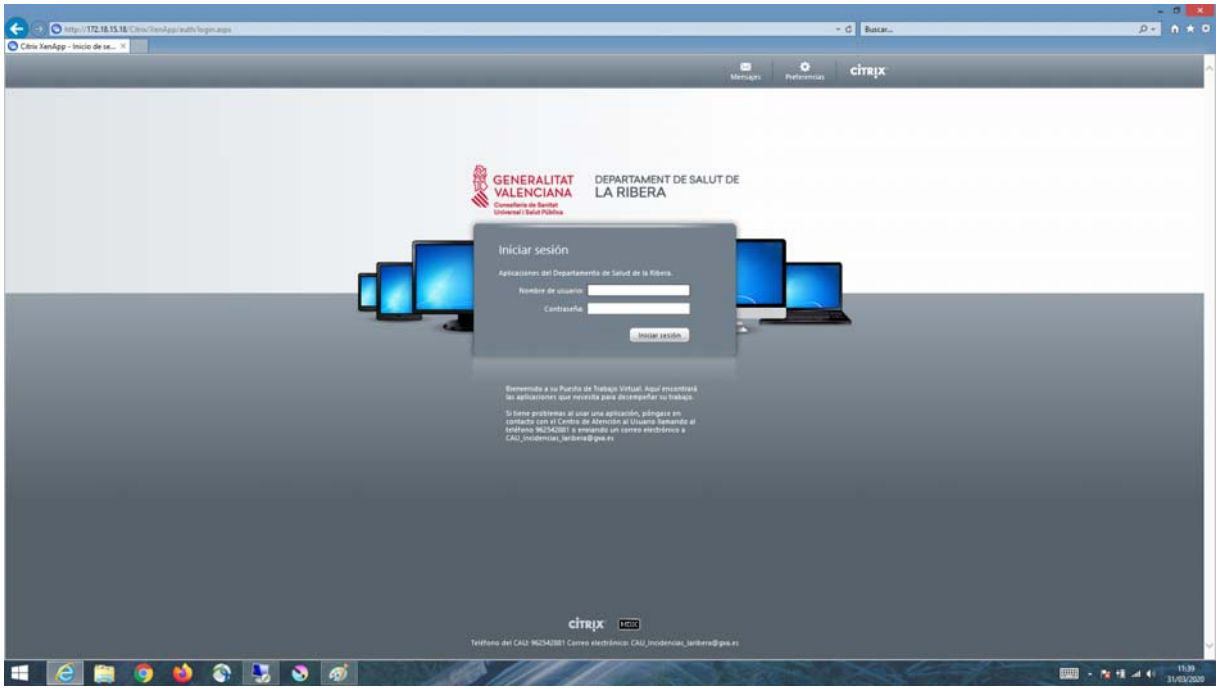


- Y para realizar la conexión poner el usuario y contraseña de inicio de sesión de los equipos del Hospital

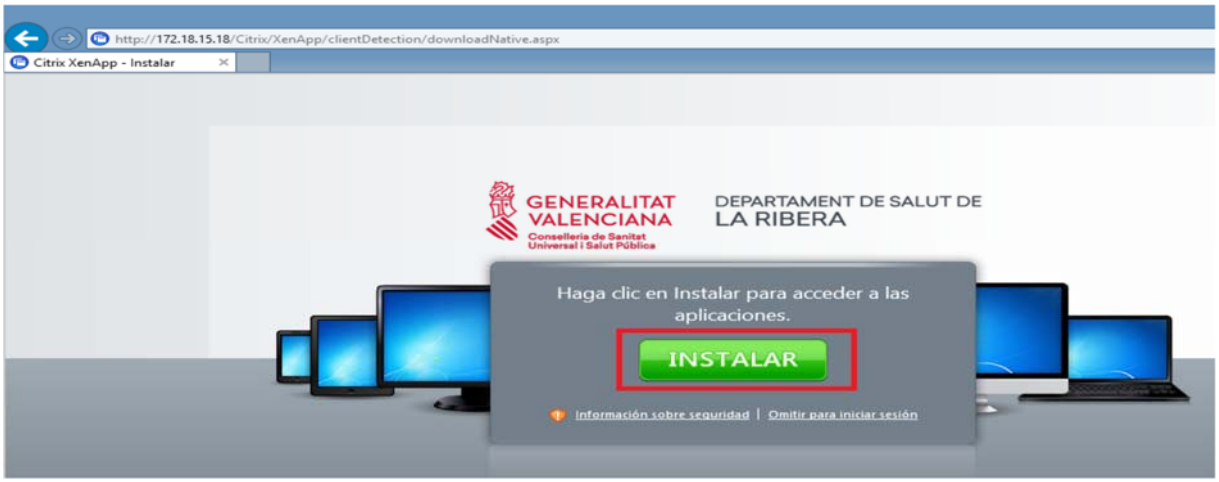
Usuario: Hospital-Ribera\nombre_usuario
Contraseña: (***tu contraseña de inicio de sesión en HR***)



Para conectar a través de citrix hay que conectarse a la siguiente URL desde un navegador
http://172.18.15.18

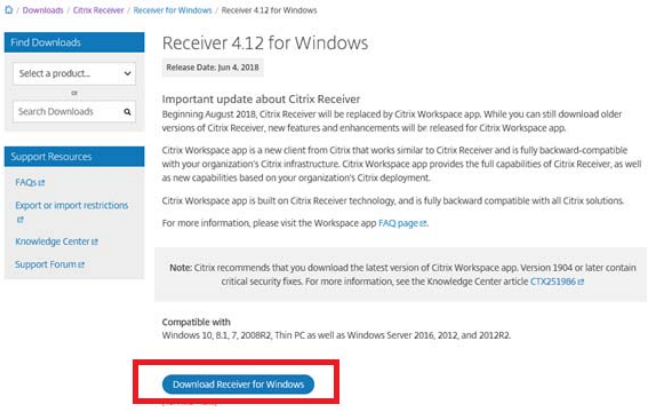


En el caso que aparezca un mensaje como el que aparece en la captura que se muestra a continuación será necesario realizar la instalación que nos indica.

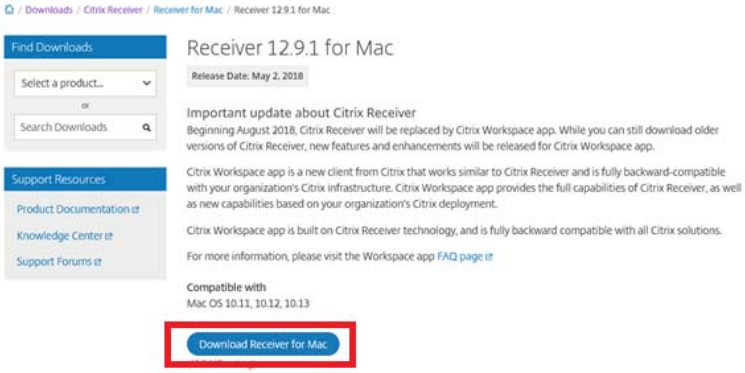


Para realizar esta instalación hay que descargar el cliente de “Citrix Reciver”, para ello, pulsar en los enlaces que se indican a continuación según el sistema operativo que tenga el equipo (si en este punto ya se está conectado a la VPN será necesario desconectarse para acceder a estos enlaces y poder realizar la descarga de los ficheros una vez realizada la descarga e instalación ya se puede volver a conectar como se indica al principio del punto 8 del documento).

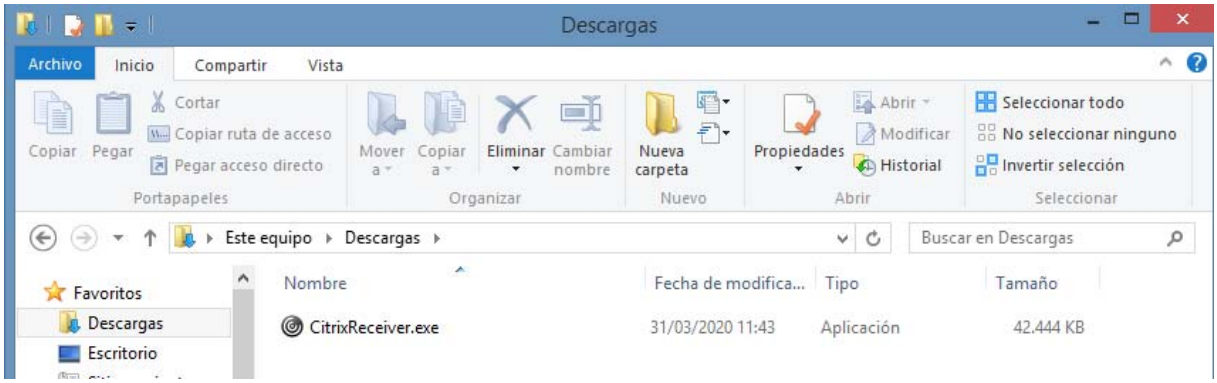
Para WINDOWS → https://www.citrix.com/downloads/citrix-receiver/windows/receiver-for-windows-latest.html



Para MAC → https://www.citrix.com/downloads/citrix-receiver/mac/receiver-for-mac-latest.html#ctx-dl-eula

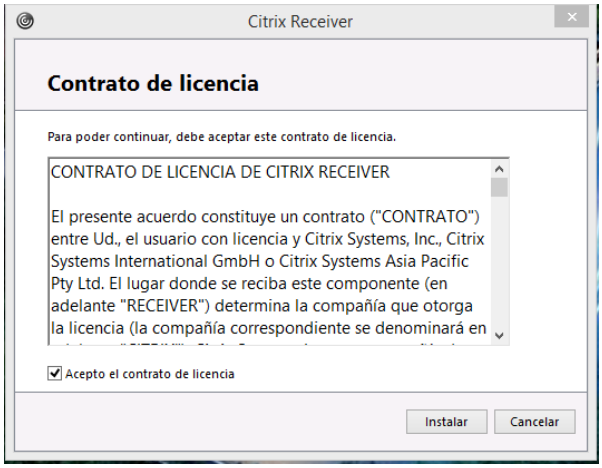


Una vez tenemos el cliente "Citrix Receiver" descargado.



Hacer doble clic sobre el ejecutable para empezar con la instalación. En la primera pantalla de la instalación pulsar en "Iniciar"

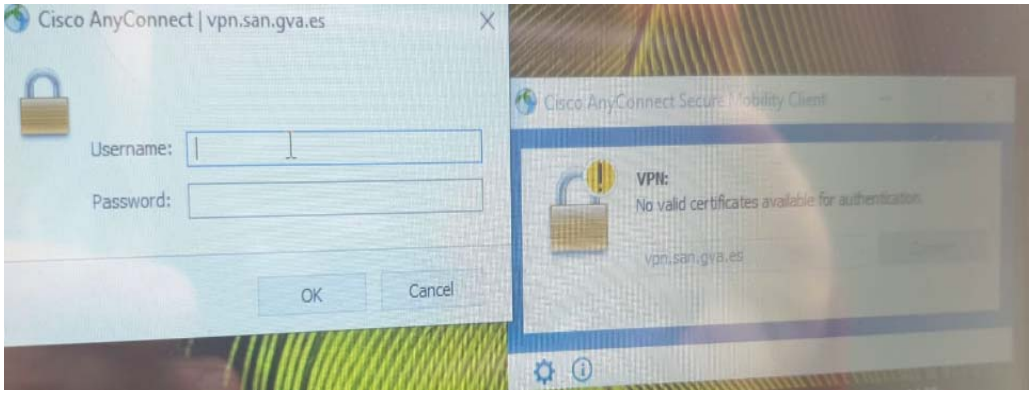
A continuación aceptar las condiciones de contrato e “Instalar”



Una vez terminado el proceso de instalación, pulsar en “Finalizar”. Tras la instalación sería recomendable reiniciar el equipo.

3. Problemas conexión

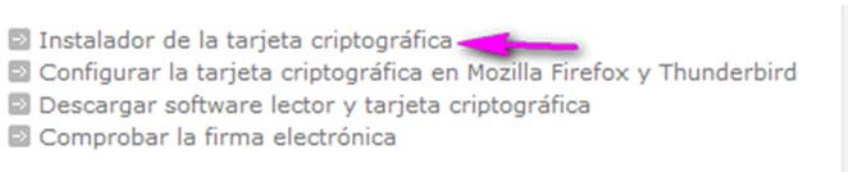
1. VPN
   a. "***No valid certificates available for authentification***". Este error aparece porque existe algún problema relacionado con los certificados, bien por una instalación errónea, por falta de algunos de los mencionados en los apartados anteriores, por problemas lectura tarjetero, etc…, se adjunta imagen:



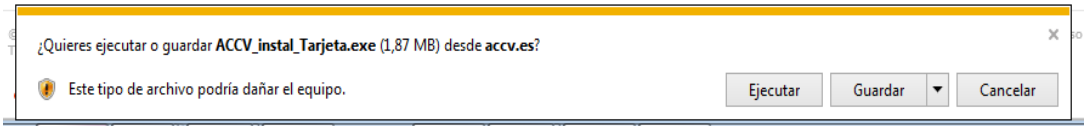
Posiblemente el tarjetero sea el principal problema y más cuando no se ha conectado nunca al PC/portátil con el que se va a establecer la conexión. Puede que con el dni electrónico funcione pero con la tarjeta accv no, resaltar que son drivers diferentes y el sistema operativo según cada caso puede que sea incapaz de instalar los controladores necesarios para poder comunicarse con el tarjetero.

A continuación se facilita una pequeña guía para instalar el driver de la tarjeta accv.

paso 1: abrir el navegador y escribir esta ruta https://www.accv.es/ayuda/instalar-la-tarjeta-criptografica-auto/. También a través de la tecla CTRL + clic en la ruta resaltada, se accederá directamente.
paso 2: situarse al final de la página y marcar la opción que se indica en la captura de pantalla.



paso 3: Ejecutar el archivo indicado o guardarlo donde se prefiera para posteriormente localizarlo y ejecutarlo con doble click. Esta ejecución servirá para instalar el controlador del tarjetero.



paso 4: Conectar VPN según procedimiento descrito en el documento.