



GUÍA de USUARIO
**CONEXIÓN REMOTA AL AYUNTAMIENTO DE
VALLADOLID (CRAVA)**
PLATAFORMA PULSE SECURE VODAFONE

Elaborado por

Departamento de Tecnologías de la Información y las Comunicaciones. Ayuntamiento de **VALLADOLID**

CONTROL DE VERSIONES

| Versión | Autor | Descripción de la Modificación | Fecha |
|---------|----------------|---|------------|
| 1.0 | CMV (Vodafone) | Primera versión a partir de la versión para ARU | 04/02/2022 |
| 1.1 | BGB | Revisión | 11/02/2022 |
| 1.2 | BGB | Nueva url | 21/02/2022 |



CONTENIDO

| | |
|--|-----------|
| 1.- INTRODUCCIÓN..... | 3 |
| 2.- OBJETO | 3 |
| 3.- CONFIGURACIÓN DE LA AUTENTICACIÓN EN DOS PASOS | 3 |
| 3.1 Requisitos | 3 |
| 3.2 Descarga e instalación..... | 4 |
| 3.3 Configuración | 4 |
| 4.- CONFIGURACIÓN DE LA CONEXIÓN AL ORDENADOR DEL TRABAJO | 5 |
| 4.1 Primer Acceso a la plataforma y asociación cuenta personal con Google Authenticator | 5 |
| 4.2 Configuración de la conexión a su ordenador del trabajo | 10 |
| 4.3 Primer Acceso a su ordenador del trabajo..... | 12 |
| 5.- ACCESOS SIGUIENTES A LA PLATAFORMA..... | 17 |
| 5.1 Acceso a la plataforma PULSE SECURE..... | 17 |
| 5.2 Acceso a su ordenador de trabajo..... | 19 |
| 6.- PROCEDIMIENTO de DESCONEXIÓN..... | 22 |
| 6.1 Desconexión de la sesión en el PC de trabajo..... | 22 |
| 6.2 Cierre de conexión en la plataforma PULSE SECURE..... | 23 |



1.- INTRODUCCIÓN

Este documento muestra los pasos necesarios para acceder al ordenador personal del trabajo desde fuera de la red corporativa del Ayuntamiento.

La plataforma CRAVA (PULSE SECURE de Vodafone) permite el acceso remoto a los ordenadores personales del trabajo desde redes externas a la red del Ayuntamiento.

Dicha plataforma utiliza una autenticación en dos pasos, para aumentar la seguridad, basada en “Google Authenticator”. Como paso previo, se mostrará cómo instalarlo y usarlo.

2.- OBJETO

- Mostrar el proceso de instalación y uso de *Google Authenticator*.
- Mostrar los pasos para acceder al ordenador personal.

3.- CONFIGURACIÓN DE LA AUTENTICACIÓN EN DOS PASOS

La “autenticación de doble factor” o “validación en dos pasos” es un sistema de validación que añade una capa extra de seguridad al tradicional uso de usuario y contraseña.

Para realizar la conexión desde el exterior de la red corporativa del Ayuntamiento de Valladolid, además de nuestras credenciales, será necesario introducir un código de 6 cifras que obtendremos en cada conexión, mediante la aplicación “Google Authenticator” instalada en un dispositivo móvil.

“Google Authenticator” es una aplicación de software libre y gratuito desarrollada por Google para dispositivos móviles que genera códigos de verificación. Esta aplicación genera un código personal que cambia cada 30 segundos y solo es válido durante ese periodo de tiempo. Además, se proporcionan 6 códigos de emergencia de un solo uso, que serán válidos sin límite de tiempo.

La aplicación está disponible para Android e iOS, aunque existen implementaciones de terceras partes para otras plataformas como por ejemplo algunas extensiones de Chrome.

3.1 Requisitos

- Dispositivos **Android**, versión 2.3.3 o superior.
 - Acceder a Google Play.
 - Descargar e instalar la aplicación.
- Dispositivos **iPhone, iPod Touch o iPad**, versión iOS 7.0 o superior.
 - Acceder a App Store.
 - Descargar e instalar la aplicación.



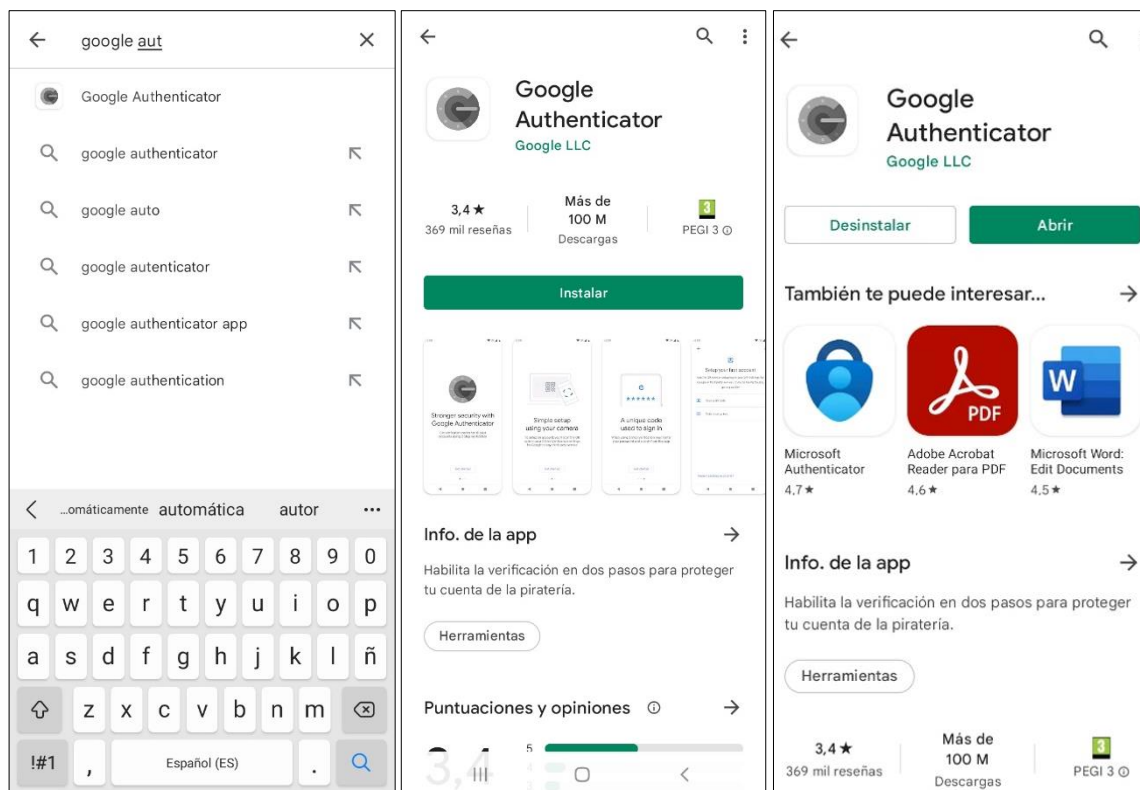
3.2 Descarga e instalación

Acceder a la tienda correspondiente a nuestro dispositivo para instalar la aplicación.

Ejemplo de instalación en un móvil Android.

Acceder a Google Play, buscar e instalar la aplicación “Google Authenticator”.

(Las pantallas pueden diferir en función de la versión)



3.3 Configuración

Para asociar nuestro usuario y crea una nueva cuenta de *Google Authenticator*, tendremos que seguir con los siguientes pasos de este manual hasta llegar al apartado “4.1 Primer Acceso a la plataforma y asociación cuenta personal con Google Authenticator”.

En dicho apartado se explica el procedimiento para realizar el primer acceso y la configuración de la conexión al ordenador del trabajo. En uno de los pasos nos aparecerá un código de barras (QR). En ese momento, y con la aplicación ya instalada, tendremos que escanear dicho código (según se explica en dicho apartado).

IMPORTANTE: la configuración de Google Authenticator es independiente de otros sistemas del Ayuntamiento (por ejemplo, VMWare Horizon o la antigua plataforma ARU) por lo que tendrá que configurar otra cuenta de Google Authenticator aunque ya tuviera una cuenta previa.

IMPORTANTE: si ya tenía cuenta en ARU, se recomienda borrar antes la configuración de esa cuenta.



4.- CONFIGURACIÓN DE LA CONEXIÓN AL ORDENADOR DEL TRABAJO

En el primer acceso a la plataforma es necesario realizar una serie de configuraciones que se explican en esta sección. Si se concluye con éxito, las siguientes conexiones son más sencillas (ver apartado 5).

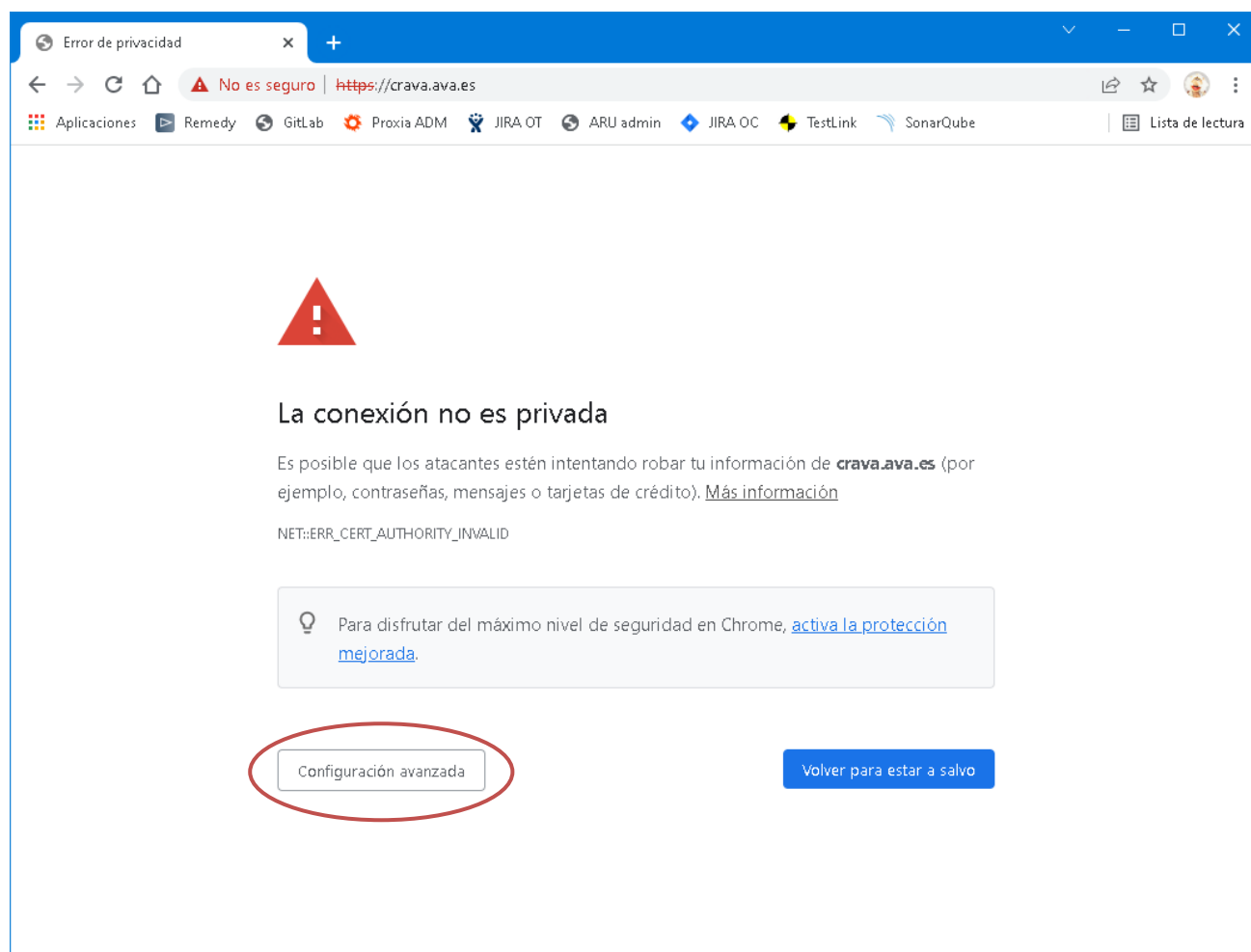
4.1 Primer Acceso a la plataforma y asociación cuenta personal con Google Authenticator

El primer paso es acceder a la página de la plataforma, para ello introducir la siguiente dirección web en el navegador (o pinchar en el siguiente enlace):

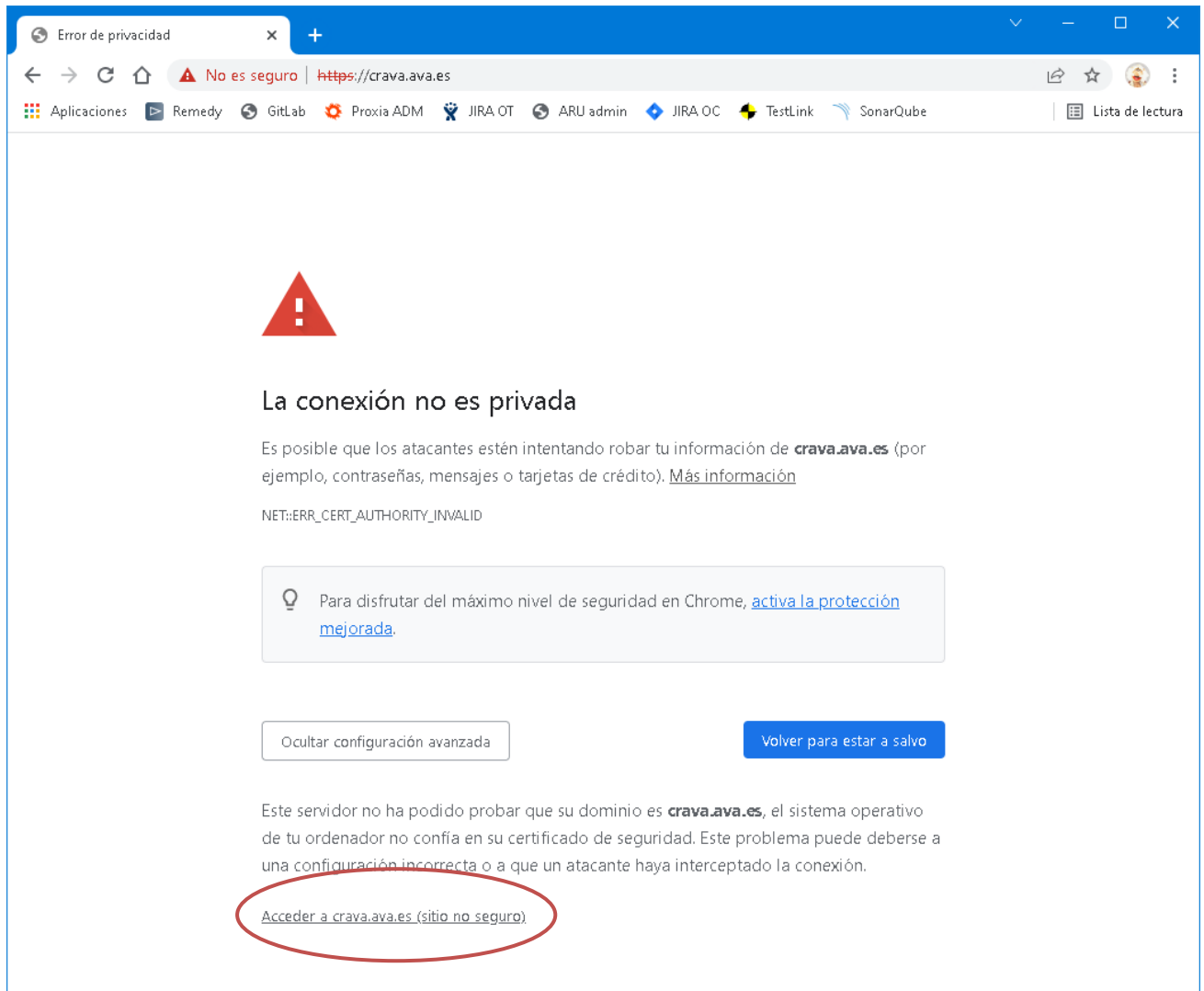
<https://crava.ava.es/> (o alternativamente <https://77.227.130.153/>).

(la guía se ha realizado con Google Chrome, si utiliza otros navegadores las pantallas pueden ser diferentes, por lo que se recomienda su uso).

Puede aparecer la siguiente pantalla. Pulsar en el botón “Configuración Avanzada”:



Se mostrará un texto explicativo de aviso y al final del mismo, pinchar sobre el enlace “[Acceder a crava.ava.es](https://crava.ava.es) (sitio no seguro)”:



Aparecerá la siguiente pantalla, utilice su usuario y la contraseña que usa para acceder en los ordenadores del Ayuntamiento:



Si ha introducido correctamente su usuario/contraseña, aparecerá una pantalla similar a la siguiente, que le permite configurar su cuenta en *Google Authenticator* (si no la tuviera instalada, ver apartado 3):

IMPORTANTE: la configuración de Google Authenticator es independiente de otros sistemas del Ayuntamiento (por ejemplo, VMWare Horizon) por lo que tendrá que configurar otra cuenta de Google Authenticator aunque ya tuviera una cuenta previa.

IMPORTANTE: si ya tenía cuenta en ARU, se recomienda borrar antes la configuración de esa cuenta.



Servidor de acceso al Ayuntamiento de Valladolid. Este es un servidor de acceso restringido. Por favor, desconecte inmediatamente si no tiene permiso explícito de acceso.
Plataforma Ayto. Valladolid


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

You will need to install a two factor authentication application (Google Authenticator) on your smartphone or tablet.

1. Configure la aplicación:

Abra la aplicación de autenticación de dos factores y añada la cuenta de usuario "bgbaixauli" 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.

| | |
|--------|--------|
| 123456 | 789012 |
| 345678 | 901234 |
| 567890 | 123456 |
| 789012 | 345678 |
| 901234 | 567890 |

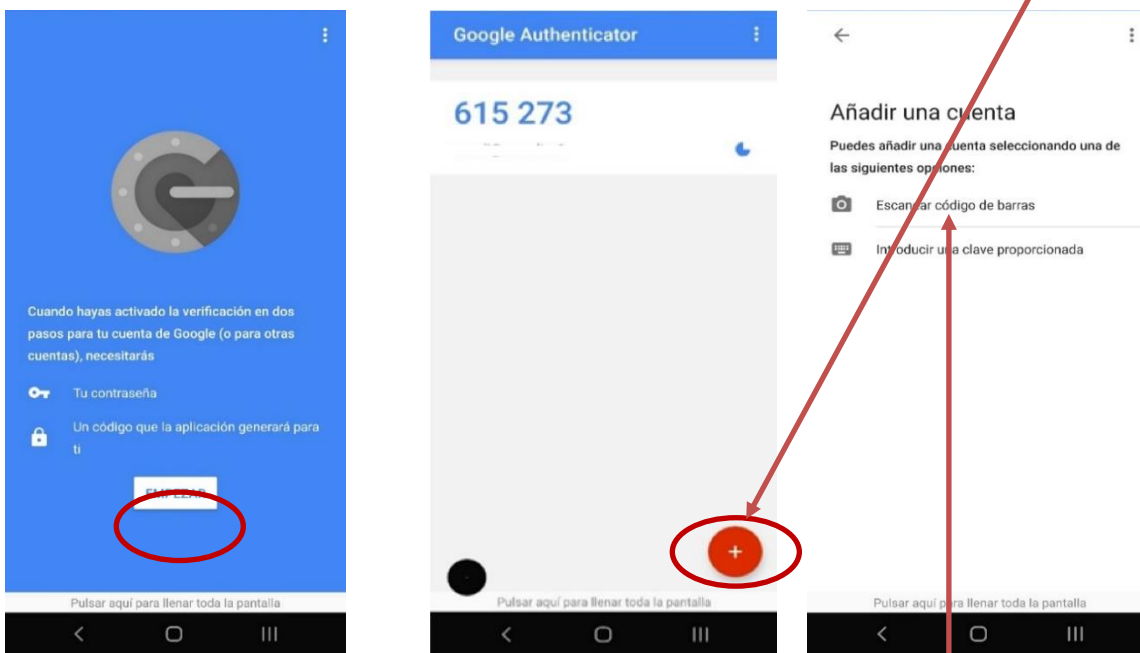
3. Introducir el código token que genera la aplicación:

IMPORTANTE: el código QR y los datos han sido desenfocados por cuestiones de seguridad. NO UTILIZAR esta imagen, si no la que aparece en la pantalla de su ordenador.

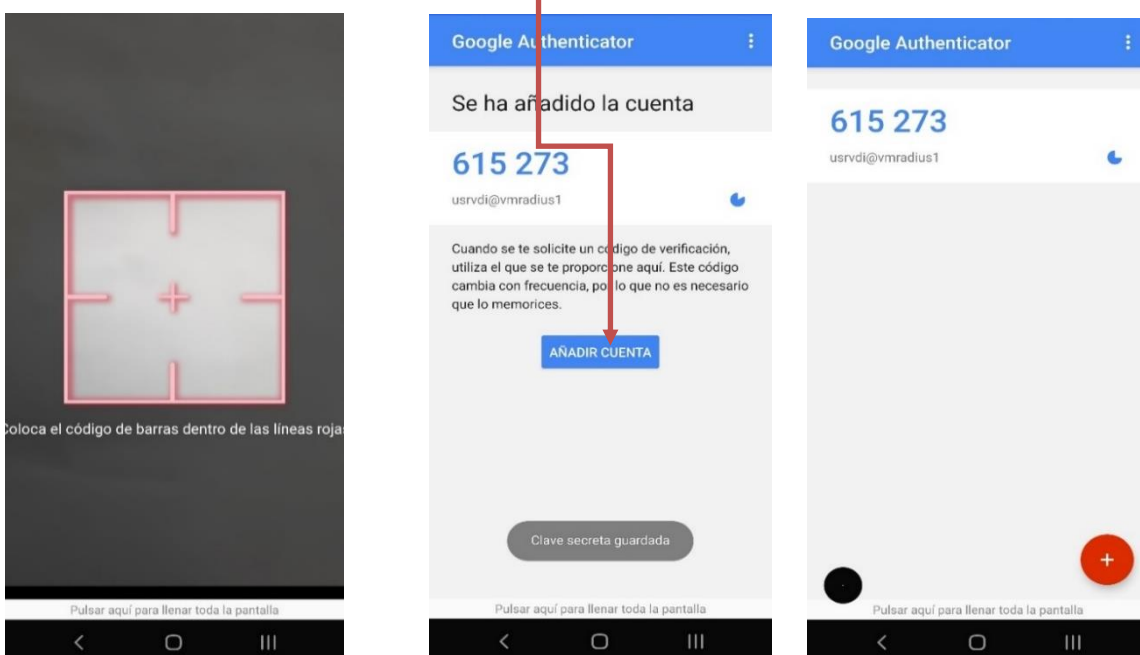


Para configurar su cuenta en *Google Authenticator* siga los siguientes pasos:

- Arranque la aplicación *Google Authenticator* en el móvil.
 - Si no tiene configurada ninguna cuenta le aparecerá una pantalla azul, pulse el botón “Empezar”.
 - Si ya tiene configurada alguna cuenta pulse sobre el botón rojo con el símbolo +



- En la pantalla Añadir una cuenta, pulsar Escanear código de barras:
- Nos aparecerá una pantalla para colocar el código de barras (QR) dentro de las líneas rojas. Apuntar con el móvil al código de barras (QR), que aparece en la pantalla del ordenador.
- En la pantalla siguiente dar al botón AÑADIR CUENTA:





Ahora ya podemos acceder a la aplicación, pero primero, como indica en las instrucciones de la página es recomendable guardar los códigos de copia de seguridad que aparecen (punto 2). Estos códigos le permitirán (una única vez por código) acceder sin utilizar la aplicación de *Google Authenticator*. Guárdelos en un documento de texto. También es posible volver a consultar los códigos o regenerar el código QR para volver a asociar la cuenta (vea el documento de *“PREGUNTAS FRECUENTES Acceso Remoto CRAVA Usuarios”* disponible en el cloud de Ayuntamiento de Valladolid).

Por último, para acceder a la aplicación, en el campo *“3. Introducir el código token que genera la aplicación”* ponemos el código que muestra la aplicación móvil:

Logo Ayuntamiento de Valladolid

Servidor de acceso al Ayuntamiento de Valladolid. Este es un servidor de acceso restringido. Por favor, desconecte inmediatamente si no tiene permiso explícito de acceso.

Plataforma Ayto. Valladolid


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

You will need to install a two factor authentication application (Google Authenticator) on your smartphone or tablet.

1. Configure la aplicación:

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

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



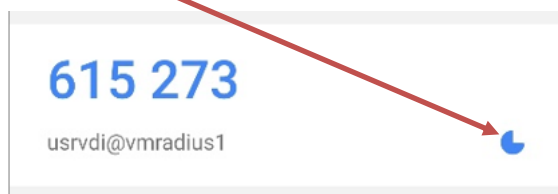
2. Guardar códigos de copia de seguridad:

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.

| | |
|--------|--------|
| 123456 | 789012 |
| 345678 | 901234 |
| 567890 | 123456 |
| 789012 | 345678 |
| 901234 | 567890 |

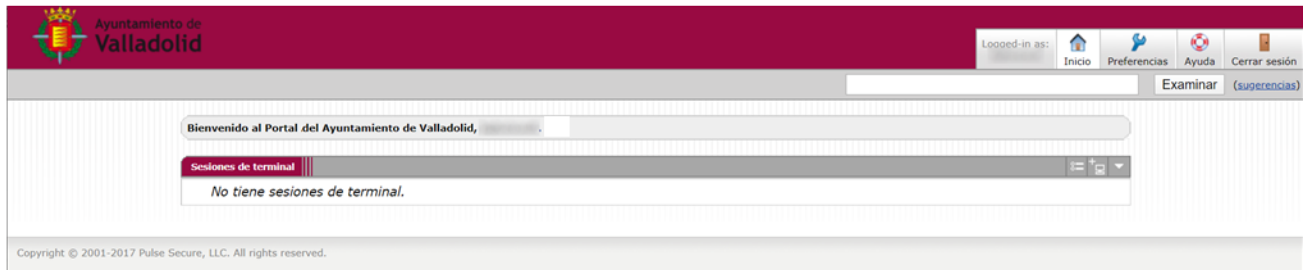
3. Introducir el código token que genera la aplicación:

Hay que tener cuidado porque el código de *Google Authenticator* cambia rápidamente, en la parte inferior derecha hay un pequeño contador gráfico que indica el tiempo que le queda a ese código. Lo recomendable es esperar a que cambie:




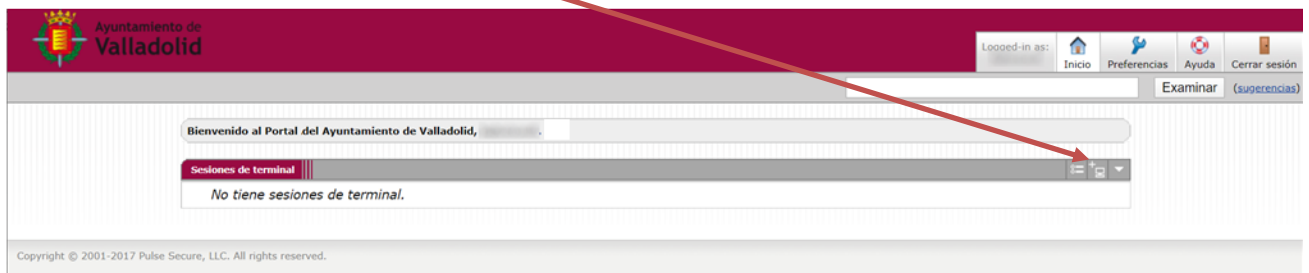


Si todo ha funcionado bien, al pulsar en el botón acceder, accederemos a la plataforma en una pantalla como la siguiente:



4.2 Configuración de la conexión a su ordenador del trabajo

El siguiente paso es configurar la conexión a su ordenador del trabajo (solo es necesario hacerlo la primera vez). Para ello pulse en el botón .





Le aparecerá la pantalla:

Para configurar la conexión introduzca los siguientes datos:

- **Nombre de marcador:** *Conexión Ayto.*
- **Host:** introduzca el identificador de su ordenador del trabajo. Ese identificador es el código de mantenimiento del ordenador codificado de la forma **VAXXXXXX.ava.gov**, donde XXXXXX es un número de **6 cifras** formado por el número de mantenimiento precedido de 1 o 2 ceros, dependiendo de si nuestro número de mantenimiento es de 4 o 5 cifras.

Ejemplo: VA001234.ava.gov o VA012345.ava.gov.
- **Puerto del servidor:** 3389
- **Profundidad de color:** seleccione la opción *32 bits (color verdadero)*
- **Nombre de usuario:** *DOMAYTOVA\<USERNAME>*

IMPORTANTE: en Nombre de usuario introduzca el texto tal cual (no cambie <USERNAME> por su usuario), compruebe que la barra es la correcta (barra invertida o '\') y NO ponga espacios antes y después de la barra invertida (va todo junto sin espacios).

El resultado final, con los campos a modificar marcados, debería ser el siguiente (**lo único que debe cambiar es el Host, que será el correspondiente a su ordenador del trabajo**):



Agregar sesión de servicios de terminales

Tipo de sesión: Servicios de terminales de Windows
Nombre de marcador: **Conexión Ayto**
Descripción:

Ajustes

* Host: **vaXXXXXX.ava.gov** Nombre o dirección IP de host remoto
Puerto del cliente: Si un puerto de cliente está especificado y el cliente de servicios de terminales Pulse Secure no puede vincularse a este puerto, entonces el cliente de servicios de terminales tendrá error. Sin embargo, si se deja vacío, el cliente de servicios de terminales de Pulse Secure seleccionará dinámicamente un puerto disponible.
Puerto del servidor: **3389**
Tamaño de pantalla: **Pantalla completa** Tamaño en caracteres y filas
Profundidad de color: **32 bits (color verdadero)**

Sesión

Autenticación:
Nombre de usuario: **DOMAYTOVA\<USERNAM** Nombre de usuario o <USER> para nombre de usuario de sesión IVE
Contraseña:

Iniciar aplicación:

Abrir una ventana "seamless"
[NOTA: La casilla de verificación de ventana integrada sólo se aplica a servidores que ejecutan Windows 2008 y posteriores]

Ruta de la aplicación:
Directorio de trabajo:

Conectar dispositivos:

Usar varios monitores

Mostrar configuración:

¿Agregar sesión de servicios de terminales?

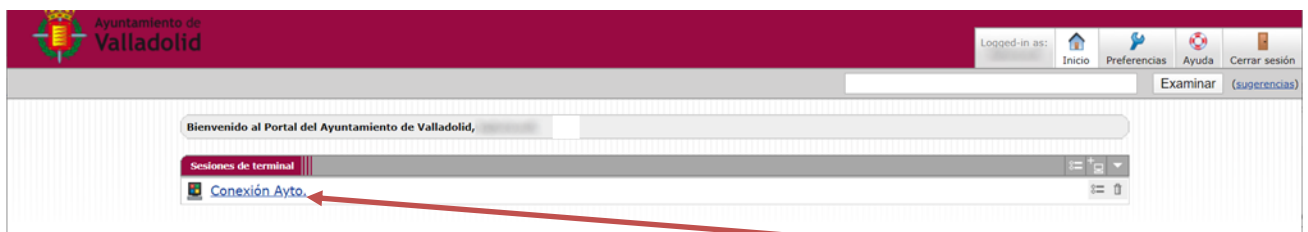
* indica que es un campo necesario

Copyright © 2001-2017 Pulse Secure, LLC. All rights reserved.

Para finalizar, presione el botón *Agregar* (en la parte inferior izquierda):

4.3 Primer Acceso a su ordenador del trabajo

Si todo ha funcionado correctamente, le aparecerá una pantalla como la siguiente:



Para acceder a su escritorio, pinche en la conexión que acaba de crear (en el enlace "Conexión Ayto.").

La primera vez, se tiene que instalar un software nuevo para acceder a su equipo. Aparecerá la siguiente pantalla:



Ayuntamiento de Valladolid

Buscando el iniciador de aplicaciones...

41

Si sabe que el iniciador de aplicaciones no está instalado, omite la espera y descárguelo ahora

Descargar

Si no desea continuar, haga clic [aquí](#) para regresar.

Presione en el botón *Descargar* y una vez descargado, ejecute la aplicación pulsando sobre la descarga:

Ayuntamiento de Valladolid

Cuando se haya completado la descarga del iniciador de aplicaciones, siga estos pasos para la instalación

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

Si no desea continuar, haga clic [aquí](#) para regresar.

PulseSecureAppLa...msi Mostrar todo

Es posible que le aparezcan varios mensajes de Windows con advertencias. Acepte todos.

Una vez finalizado el proceso, le mostrará un mensaje en el que le informa que el programa se ha instalado con éxito:



Cuando se haya completado la descarga del iniciador de aplicaciones, siga estos pasos para la instalación.

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

Si no desea continuar, haga clic [aquí](#) para regresar.

Presione el botón *Aceptar* y, después, pulse en el enlace "[haga click AQUÍ](#)".

Le aparecerá una nueva pantalla en la que le indica que se va a ejecutar la aplicación *Pulse Secure Application Launcher*, active el cuadro "Permitir siempre que crava.ava.es abra este tipo de enlaces en la aplicación asociada" y pulse en "Abrir Pulse Secure Application Launcher":

Si sabe que el iniciador de aplicaciones no está instalado, omita la espera y descárguelo ahora

Descargar

Si no desea continuar, haga clic [aquí](#) para regresar.

Nota: sea paciente. Puede que tarde unos momentos aparecer la siguiente pantalla. NO PULSE el botón "Descargar" (ya lo hizo en pasos anteriores).



Probablemente salga un nuevo mensaje indicando que hay un problema con el certificado de seguridad del servidor. Active el cuadro "Guardar ajustes" y al botón "Sí":

Buscando el iniciador de aplicaciones...

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

Si no desea continuar, haga clic [aquí](#) para regresar.

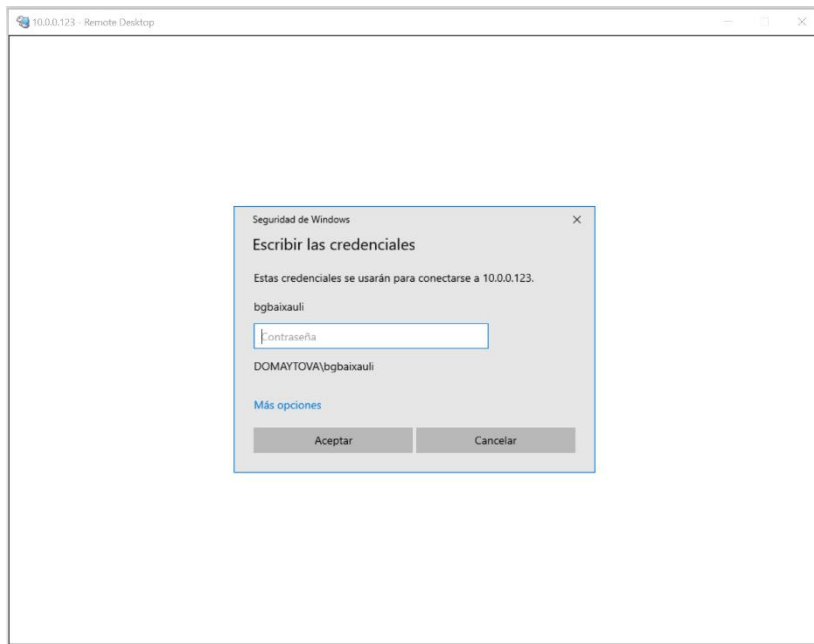
Probablemente le aparezca otro mensaje preguntando si quiere que *Pulse Secure* se conecte al servidor. Pulse "Siempre":

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

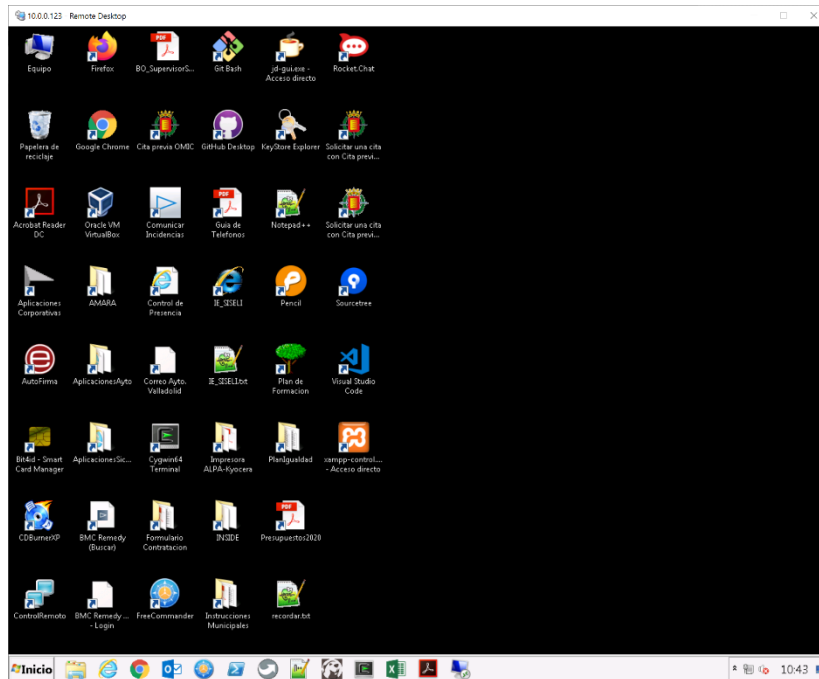
Si cree que el iniciador de aplicaciones ya está instalado, seleccione [Intentar de nuevo](#) para encontrarlo.

Si no desea continuar, haga clic [aquí](#) para regresar.

Ya está configurada su conexión. Se iniciará el acceso al ordenador de trabajo en el Ayuntamiento y para acceder tiene que introducir de nuevo su contraseña del Ayuntamiento:



Si todo ha ido bien, se mostrará su escritorio. Por ejemplo:



Una vez acaben de trabajar en su escritorio remoto, es importante que cierren correctamente la sesión. (ver apartado 6 más adelante en este manual).



5.- ACCESOS SIGUIENTES A LA PLATAFORMA

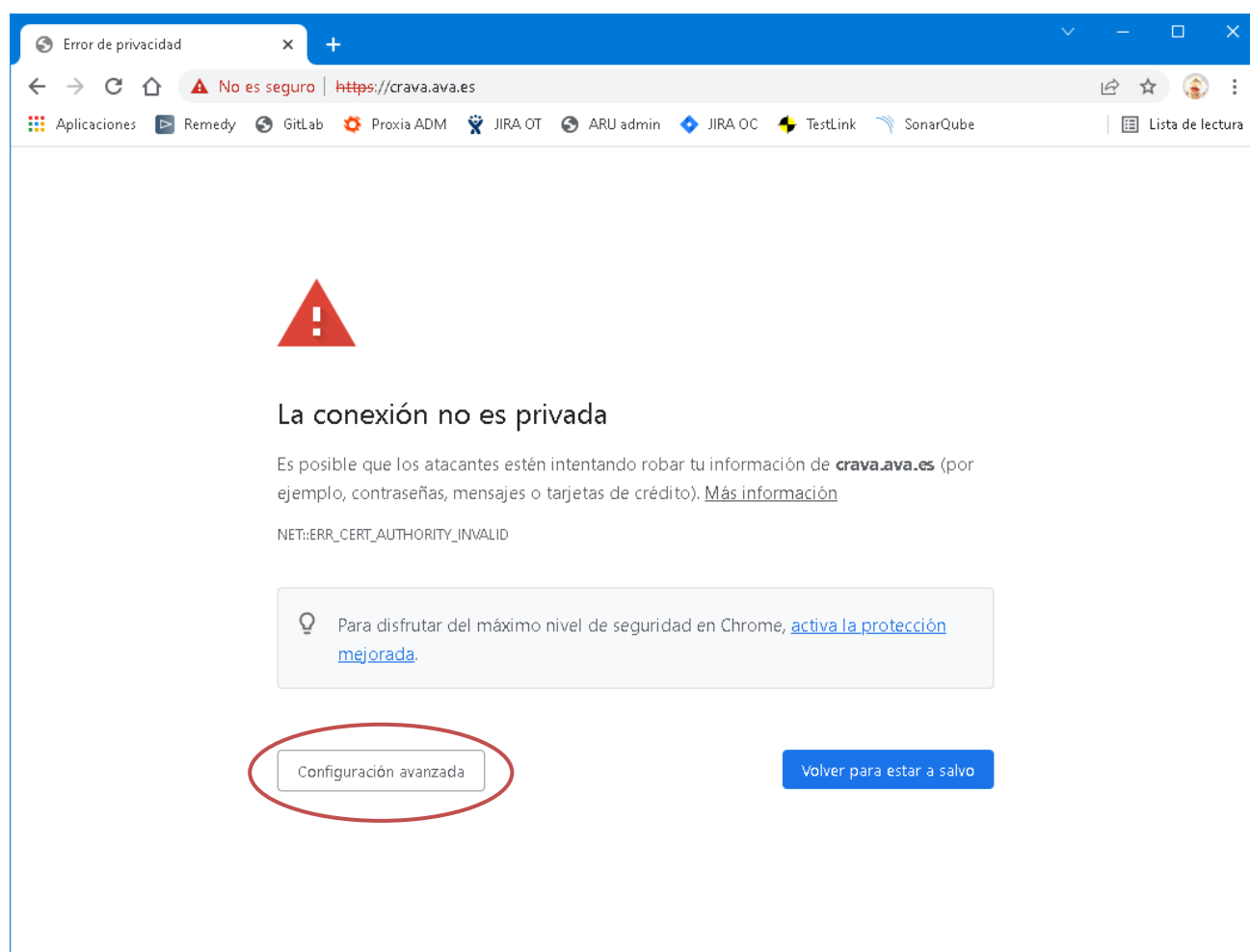
Una vez configurado, los sucesivos accesos a la plataforma son más sencillos:

5.1 Acceso a la plataforma PULSE SECURE

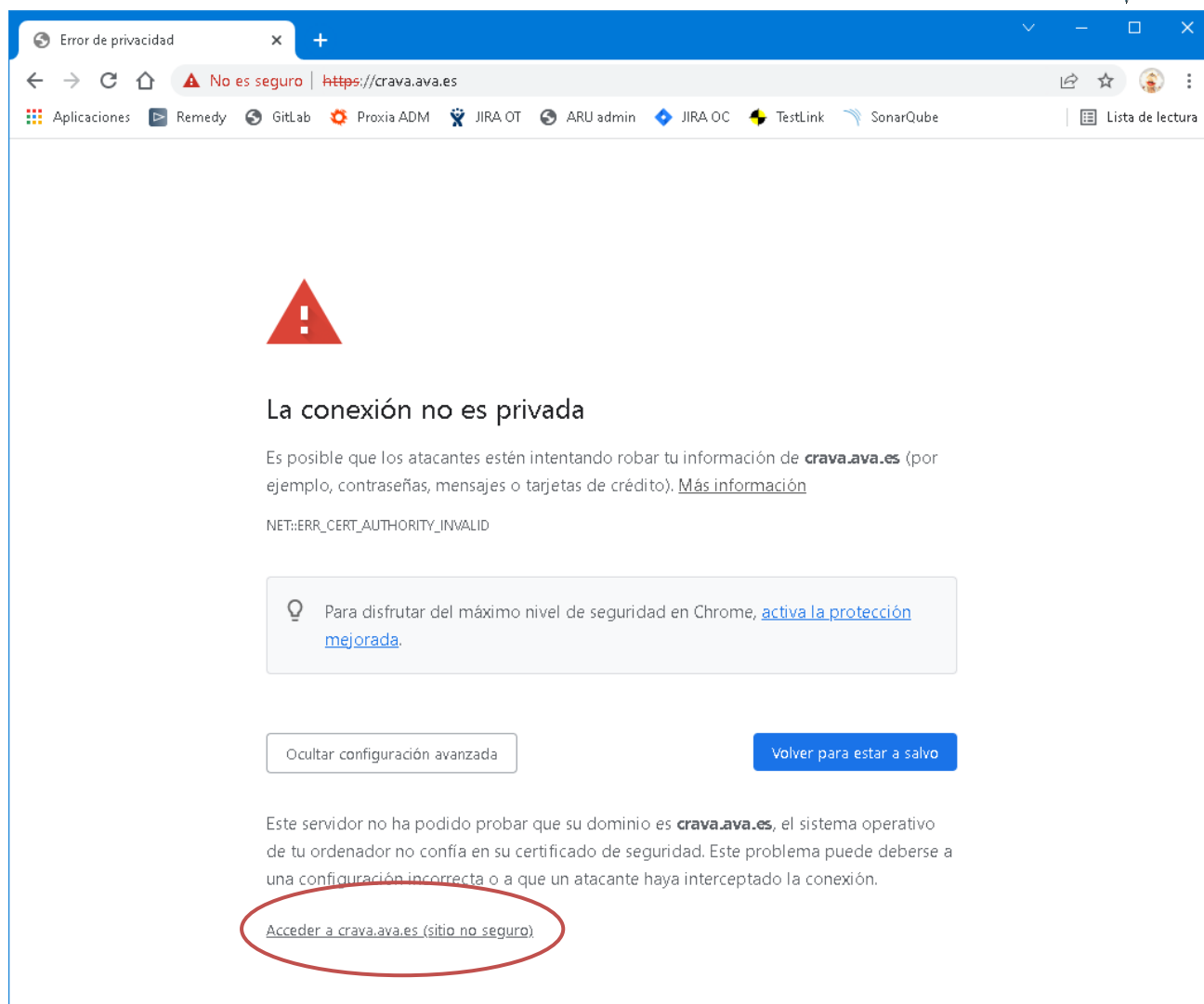
El primer paso es acceder a la página de la plataforma, para ello introducir la siguiente dirección web en el navegador (o pinchar en el siguiente enlace):

<https://crava.ava.es/> (o alternativamente <https://77.227.130.153/>)(la guía se ha realizado con Google Chrome, si utiliza otros navegadores las pantallas pueden ser diferentes, por lo que se recomienda su uso).

Puede aparecer la siguiente pantalla. Pulsar en el botón “*Configuración Avanzada*”:



Se mostrará un texto explicativo de aviso y al final del mismo, pinchar sobre el enlace “Acceder a crava.ava.es (sitio no seguro)”:



Aparecerá la siguiente pantalla. Utilice su usuario y contraseña que usa para acceder en los ordenadores del Ayuntamiento:

Ayuntamiento de Valladolid

Servidor de acceso al Ayuntamiento de Valladolid. Este es un servidor de acceso restringido. Por favor, desconecte inmediatamente si no tiene permiso explícito de acceso.

Plataforma Ayto. Valladolid

Usuario

Contraseña

En la siguiente página web puede encontrar manuales y vídeos para configurar y acceder a su equipo: [Manuales y Vídeos](#) o si le da problemas en [Manuales y Vídeos](#)

Si ha introducido correctamente su usuario/contraseña, aparecerá una pantalla similar a la siguiente donde deberá introducir el código que muestra en ese momento la app *Google Authenticator*:

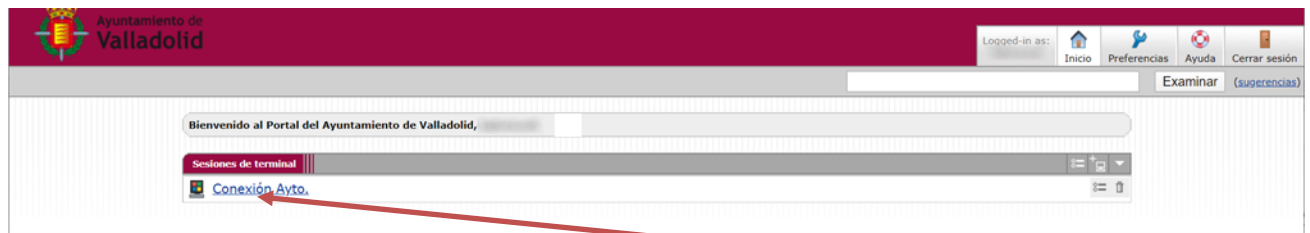


Y pulsar en el botón *Iniciar sesión*.

NOTA: si no tiene acceso a Google Authenticator, puede utilizar los códigos de copia de seguridad que guardó al configurar el Google Authenticator (ver apartado 4.1), pero tenga en cuenta que cada código sólo se puede usar una vez. También puede consultarlos siguiendo el método explicado en el documento “PREGUNTAS FRECUENTES Acceso Remoto PULSE SECURE” disponible en el cloud de Ayuntamiento de Valladolid.

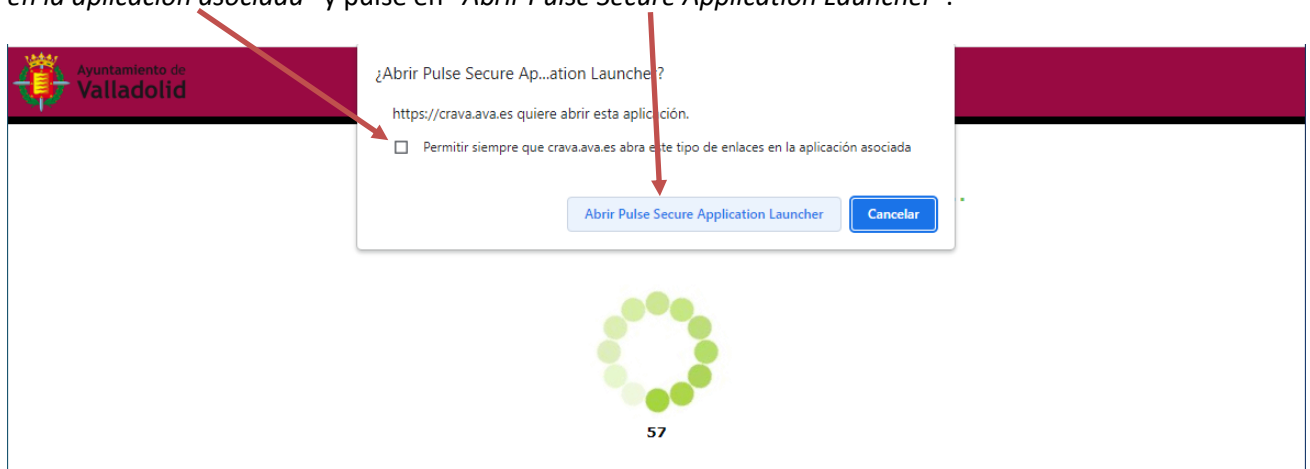
5.2 Acceso a su ordenador de trabajo.

Si todo ha funcionado correctamente, le aparecerá una pantalla como la siguiente:



Para acceder a su escritorio, pinche en la conexión que creó la primera vez (en “*Conexión Ayto.*”).

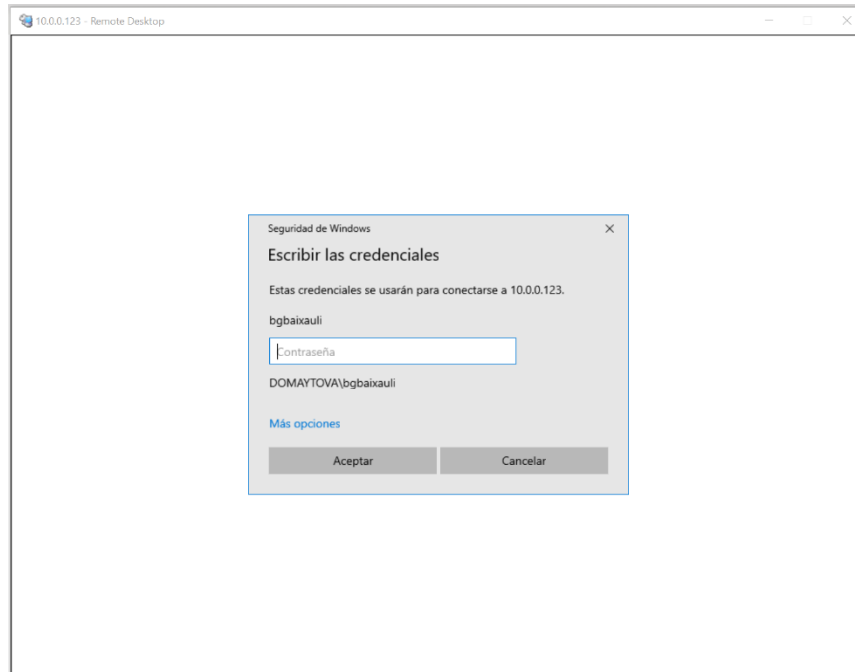
Puede aparecer una nueva pantalla en la que le indica que se va a ejecutar la aplicación *Pulse Secure Application Launcher*, si es así, active el cuadro “*Permitir siempre que crava.ava.es abra este tipo de enlaces en la aplicación asociada*” y pulse en “*Abrir Pulse Secure Application Launcher*”:



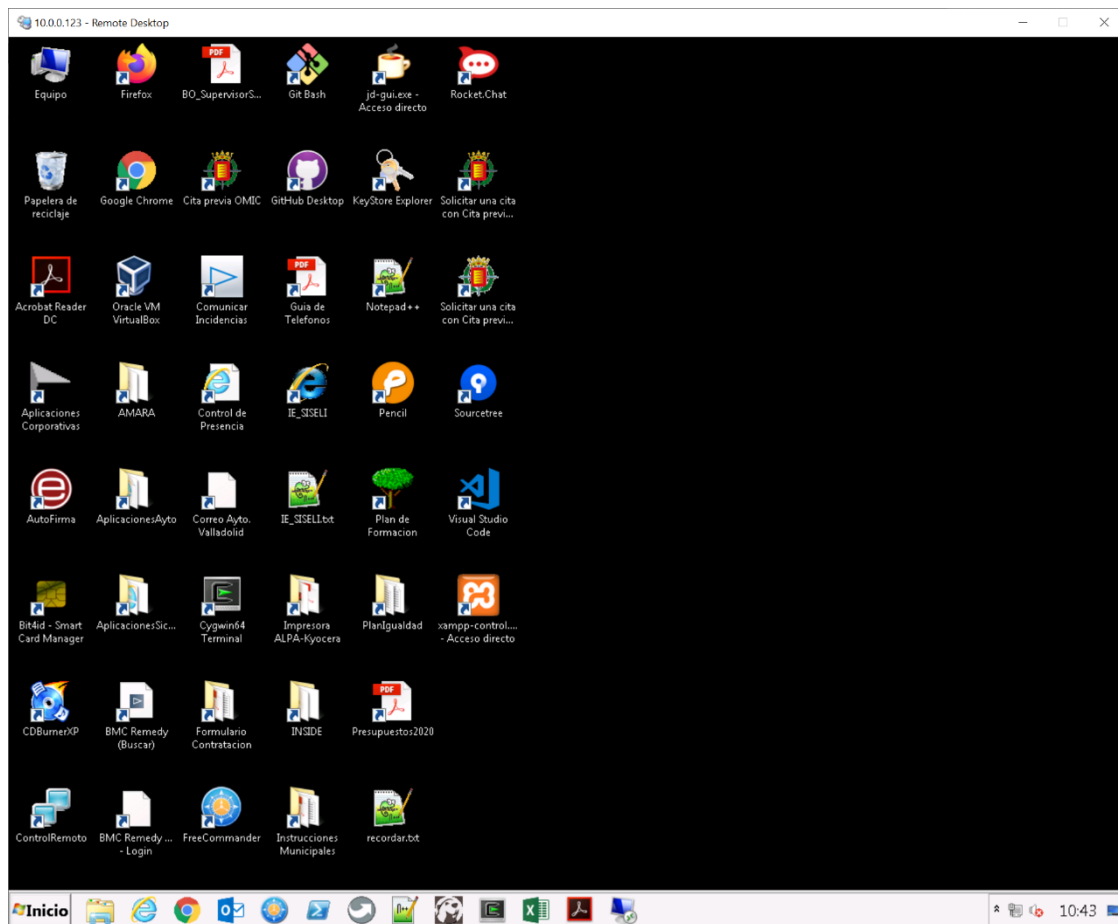


Nota: SEA PACIENTE. Puede que tarde unos momentos aparecer la siguiente pantalla. NO PULSE el botón “Descargar” (ya lo hizo en pasos anteriores).

Se iniciará el acceso al ordenador de trabajo en el Ayuntamiento y para acceder tiene que introducir de nuevo su contraseña del Ayuntamiento:



Si todo ha ido bien, se mostrará su escritorio. Por ejemplo:



Una vez acaben de trabajar en su escritorio remoto, es importante que cierren correctamente la sesión. (ver apartado 6 más adelante en este manual).

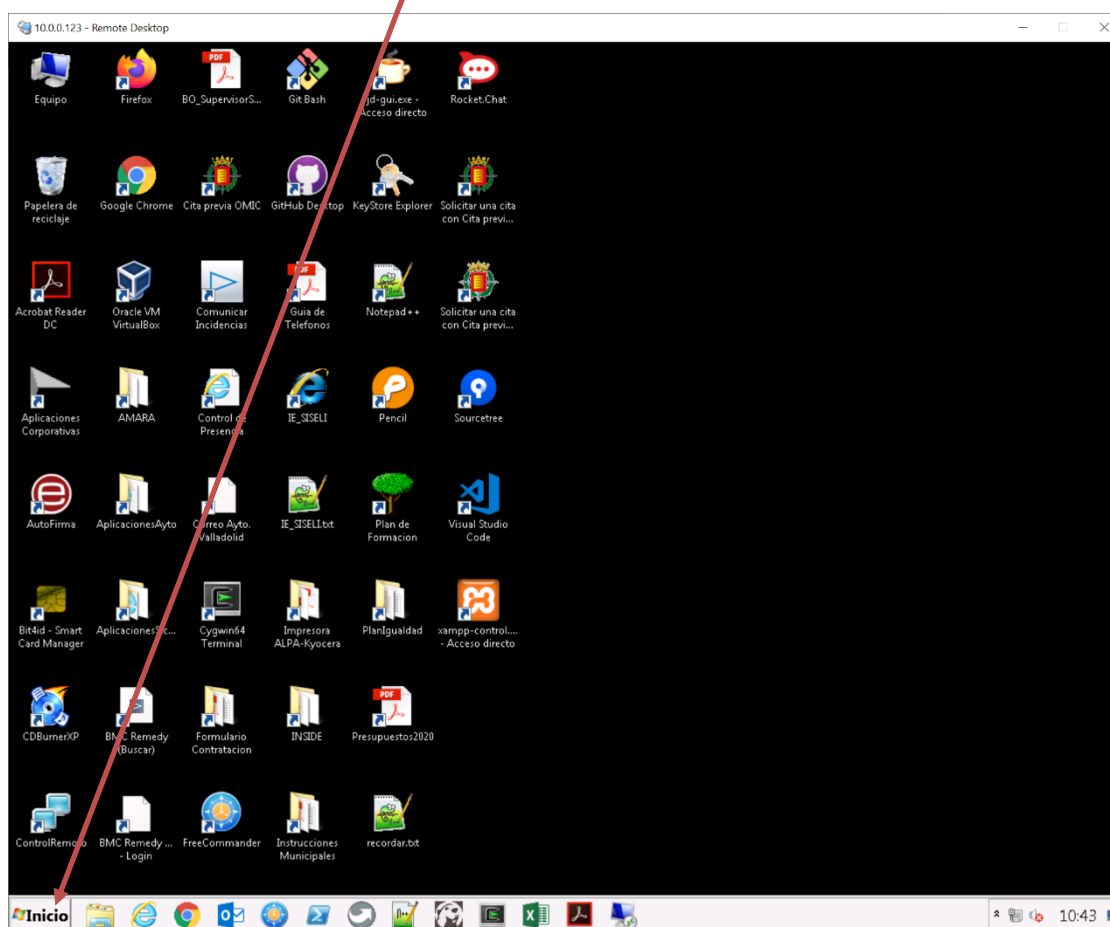


6.- PROCEDIMIENTO de DESCONEXIÓN

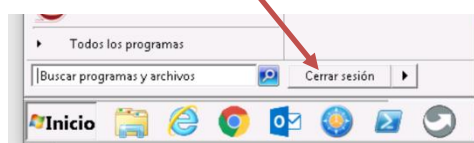
Una vez acaben de trabajar en su escritorio remoto, es importante que cierren correctamente la sesión. Esto se realiza en dos pasos:

6.1 Desconexión de la sesión en el PC de trabajo.

Para ello, pulsen en el botón *Inicio* de Windows



En el menú que aparece, pulsar el botón “Cerrar Sesión”:



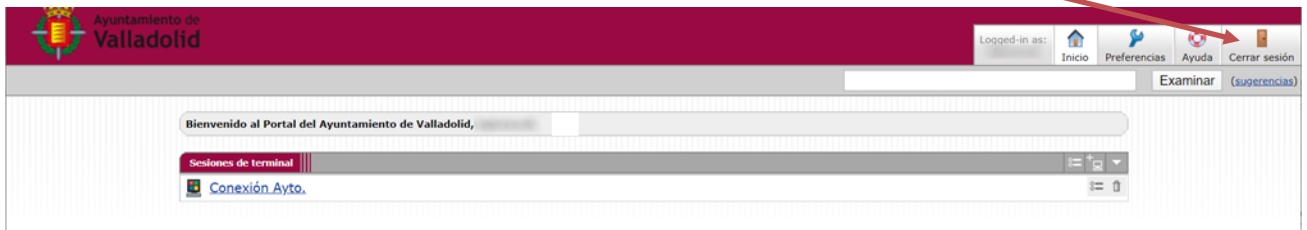
Una vez cerrada la sesión con el PC de trabajo, deberemos cerrar la conexión desde la plataforma PULSE SECURE. (ver apartado siguiente).



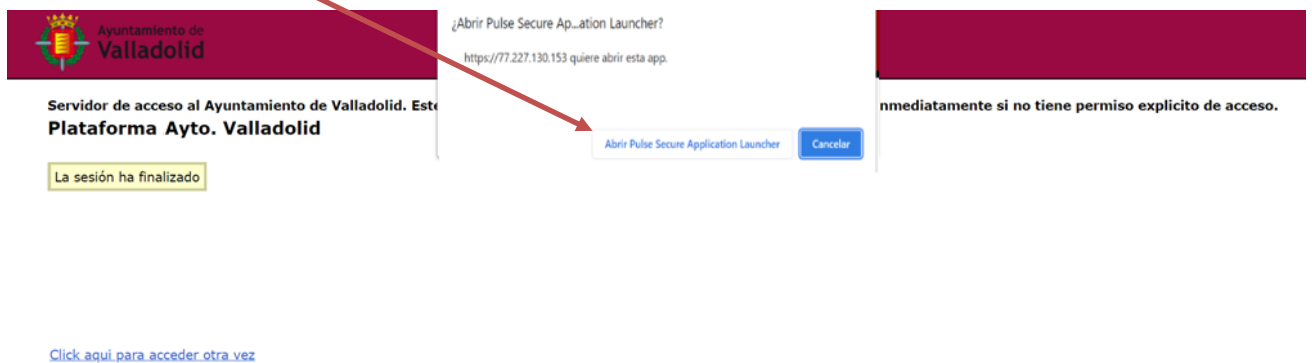
6.2 Cierre de conexión en la plataforma PULSE SECURE

Ahora deberemos cerrar la conexión desde la plataforma PULSE SECURE a la red del Ayuntamiento de Valladolid.

Para ello, en la pantalla de la plataforma CRAVA pulsar el botón “Cerrar Sesión”:



Si aparece una ventana solicitando la autorización para que se ejecute el programa, pulsar el botón “Abrir Pulse Secure Application Launcher”.



Una vez que nos aparezca el mensaje “La sesión ha finalizado” podemos cerrar la ventana del navegador, pulsando la esquina con la X.

