



www.sicop.go.cr

## Manual de configuración general SICOP

### DIRECCIÓN DE OPERACIONES SICOP

Elaborado por:	Revisado por:	Aprobado por:
Firma	Firma	Firma
Kevin Ruiz Umaña	Guiselle López Rubí	Guiselle López Rubí
Código: P-PS-146-05-2016	Versión: 02	Diciembre 2023



www.racsa.go.cr



RACSA\_CR



## Contenido

1. Descripción General .....	2
2. Firma Digital.....	2
2.1. Requerimientos del Sistema .....	2
2.2. Instalación .....	2
2.3. Consultar estado de la firma con “ID Proctect PINTools” .....	8
3. Componente de Firma.....	9
4. Comprobar versión del navegador.....	13
4.1 Versión de Chrome .....	13
4.2 Verificar la disponibilidad del puerto.....	15
5. Verificar archivo host.....	18
6. Habilitar las ventanas emergentes.....	21
7. Manejo con servidores proxy .....	24
8. Verificar el servicio web TSA .....	29

## 1. Descripción General

El presente documento es una guía con todos los requisitos, procedimientos, configuraciones y consideraciones que se deben tener en cuenta para poder utilizar el Sistema Integrado de compras Públicas de forma idónea.

## 2. Firma Digital

### 2.1. Requerimientos del Sistema

<b>Sistema operativo</b>	<ul style="list-style-type: none"> <li>Windows 7 o superior</li> </ul>
<b>Navegador Web compatibles</b>	<ul style="list-style-type: none"> <li>Google Chrome versión 60 o superior</li> </ul>
<b>Controladores</b>	<ul style="list-style-type: none"> <li>Driver firma digital, pueden ser descargados del siguiente enlace: <a href="https://www.soportefirmadigital.com/sfdj/dl.aspx?lang=es">https://www.soportefirmadigital.com/sfdj/dl.aspx?lang=es</a></li> </ul>
<b>Dispositivo</b>	<ul style="list-style-type: none"> <li>Smartcard Reader y tarjeta inteligente emitida por el Sistema Nacional de Firma Digital de Costa Rica.</li> </ul>

### 2.2. Instalación

El primer aspecto que se debe tomar en cuenta es la instalación de los drivers de firma digital, el cual permite al equipo reconocer la lectora y tarjeta inteligente.

Para poder realizar esta configuración se debe seguir los siguientes pasos:

1. Diríjase a la página oficial de SICOP e ingrese al botón de inicio de sesión indicado en la imagen.

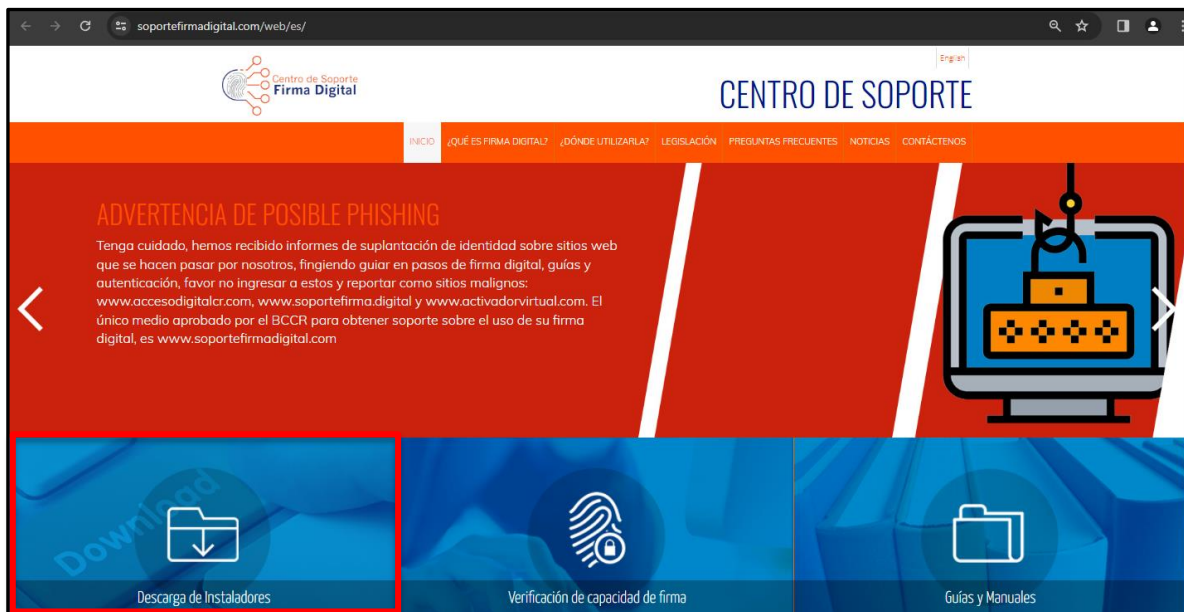


2. En la ventana siguiente se le mostrará los requisitos para el acceso a SICOP, dirigirse al recuadro indicado en la imagen, el cual lo redirigirá a la página de soporte de firma digital de Costa Rica donde se puede descargar el driver.



3. En la página de soporte de firma digital buscar la opción de descarga de instaladores e ingresar.





4. Seguidamente se le mostrará la página de descarga donde debe elegir el sistema operativo con el que cuenta, introduce el número de serie de la tarjeta como se lo indica el paso 2 y por último oprimir en la opción “Proceder con la descarga del instalador elegido”.

### Descarga de instaladores de Firma Digital



(1) Elija el instalador deseado  
 Usuarios Windows - 108 MB

SISTEMAS OPERATIVOS HOMOLOGADOS  
 Windows 10 y Windows 11  
 Tener en cuenta que Windows 7/8/8.1 no cuentan con soporte de Microsoft  
 Soporte únicamente en máquinas



(2) Número serial de la tarjeta:  
 El número de tarjeta está al reverso, no incluya espacios o guiones.

Estimado Usuario:

Los instaladores que se encuentran en este sitio Web son creados por el Centro de Soporte de Firma Digital, el cual forma parte de la empresa NETCOM S.A.

Le informamos que el uso de estos instaladores es exclusivo para usuarios que han adquirido su Certificado de Firma Digital en una institución que cuente con un contrato de soporte vigente con nuestra compañía.

Por favor marque el check a continuación para confirmar la lectura, comprensión y aceptación del mensaje.

He leído, comprendo y acepto el mensaje anterior.



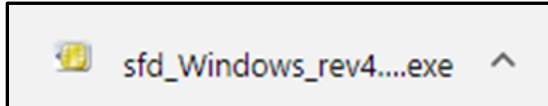
Proceder con la descarga de instalador elegido

### Aviso importante



- Solo se ofrecen los instaladores para las instituciones que tienen un acuerdo vigente de soporte para sus clientes.
- Las descargas que usted realice quedarán registradas en nuestras bitácoras, asociadas a su dirección IP y su número de tarjeta.
- Las descargas para Windows se ofrecen como archivos EXE. Sugerimos salvarlas a su disco duro y ejecutarlas desde allí.
- Si tiene alguna dificultad para descargar o instalar, no dude contactar a nuestro centro de soporte.

5. Una vez que se haya completado la descarga, se procede a instalarlo oprimiendo dos veces seguidas con el botón izquierdo del mouse **(Para realizar una instalación satisfactoria es necesario ejecutar el instalador con una cuenta de usuario con privilegios de administrador y el antivirus del equipo desactivado).**



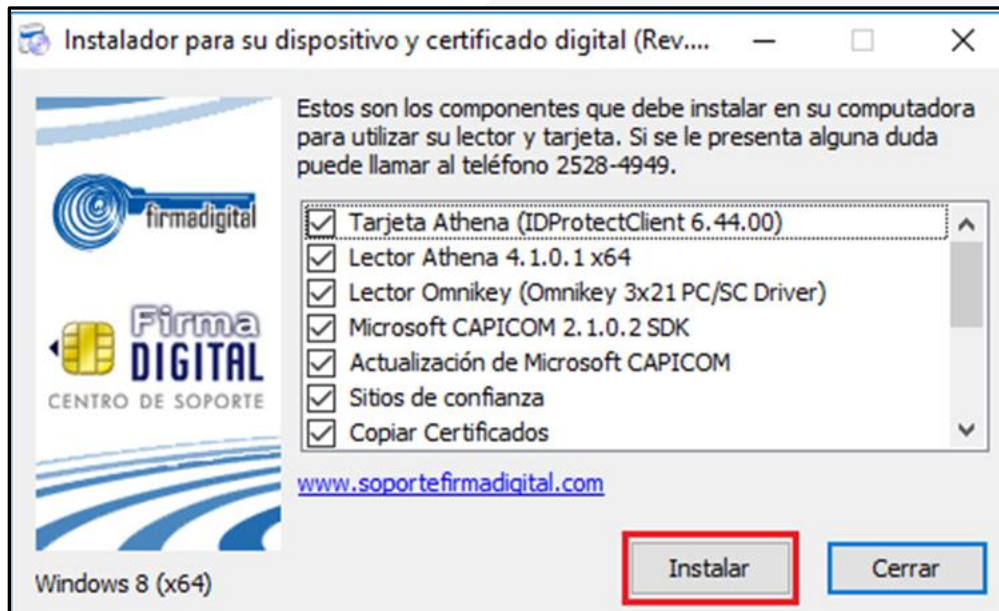
6. Proceder con la instalación del driver, para esto se deben ejecutar los siguientes pasos seleccionando las opciones que se marcan



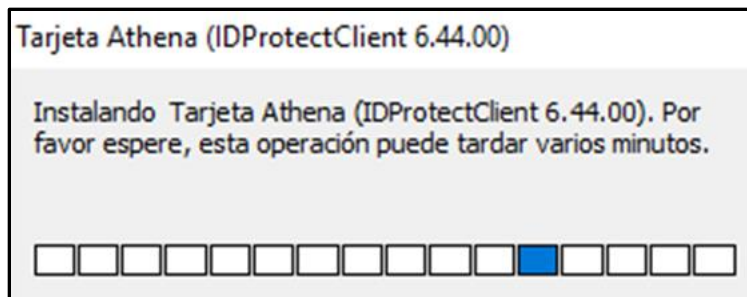
en color rojo en las imágenes:



7. Se especifica que se instalen todos los elementos del driver:



8. Se espera hasta que el proceso de instalación se encuentre finalizado.



**IMPORTANTE:** No cerrar ninguna de las ventanas que ejecute el programa de instalación.

```

C:\WINDOWS\system32\cmd.exe
NO CIERRE ESTA VENTANA NO CIERRE ESTA VENTANA
CA "Entidades de certificación intermedias"
(null)

(null)
(null)
(null) 4e0000002738de677fe8e68400000000002
CN=CA RAIZ NACIONAL - COSTA RICA v2, C=CR, O=MICITT, OU=DCFD, SERIALNUMBER=CPJ-2-100-098311
25/2/2015 12:08 p. m.
25/2/2031 12:18 p. m.
CN=CA POLITICA PERSONA FISICA - COSTA RICA v2, OU=DCFD, O=MICITT, C=CR, SERIALNUMBER=CPJ-2-100-098311
Versión de CA: V0.0
Nombre de plantilla de certificado (Tipo de certificado): SubCA
(null)
(null): SubCA
(null) b0 48 39 ce cf c7 3d 5f b0 db 8d a4 d0 61 3d 69 0f 60 4c b7

(null)
(null)
    
```

- Una vez terminada la instalación se mostrará la página para verificar que se haya instalado correctamente el driver. Seguir los pasos que se indican y presionar en la opción “Continuar”.

### Paso 1: datos básicos

(1) Número serial de su tarjeta:

El número está al reverso de la tarjeta, digite números y letras, omita guilones, asteriscos y espacios.

(2) Conecte el lector a su computadora.

(3) Inserte la tarjeta en el lector.

(Usar firmador universal en Java)

O alternativamente...

>> Validar usando CAPICOM/CRYPTOAPI >> (No utiliza Java)

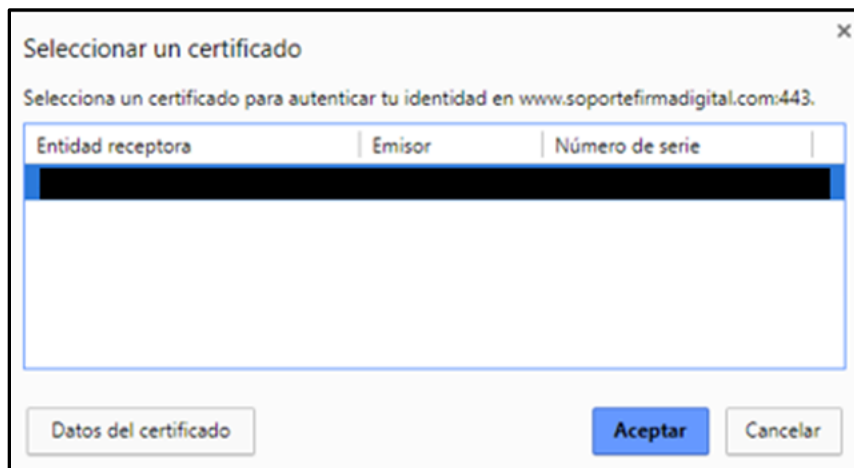
#### Información importante

- Debe haber completado la instalación de los drivers de su tarjeta (y lector si lo adquirió) antes de proceder con la verificación. Si no ha hecho esto aún, puede solicitar un CD a la entidad emisora o descargar el instalador.
- Las pruebas de autenticación y verificación quedarán guardadas en nuestras bitácoras, asociadas a su dirección IP y número de tarjeta.
- Siempre retire su tarjeta físicamente del lector cuando termina su sesión en esta página o en la de cualquier entidad.
- Si tiene problemas con la instalación, contacte al centro de soporte.





10. Si el proceso de instalación terminó correctamente se le mostrará una pantalla indicando el final exitoso del programa, desplegando la ventana del certificado.

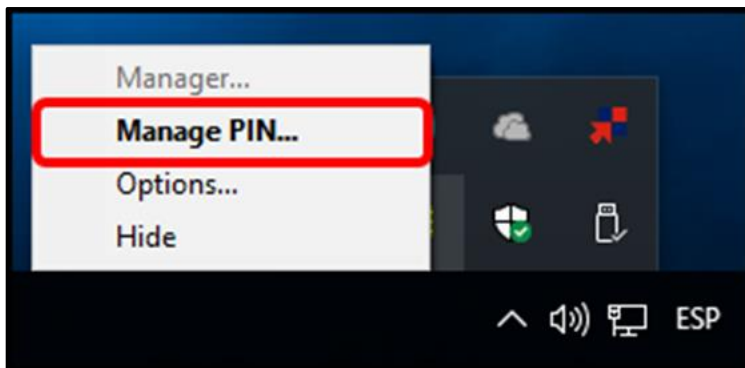


### 2.3. Consultar estado de la firma con "ID Protect PINTools"

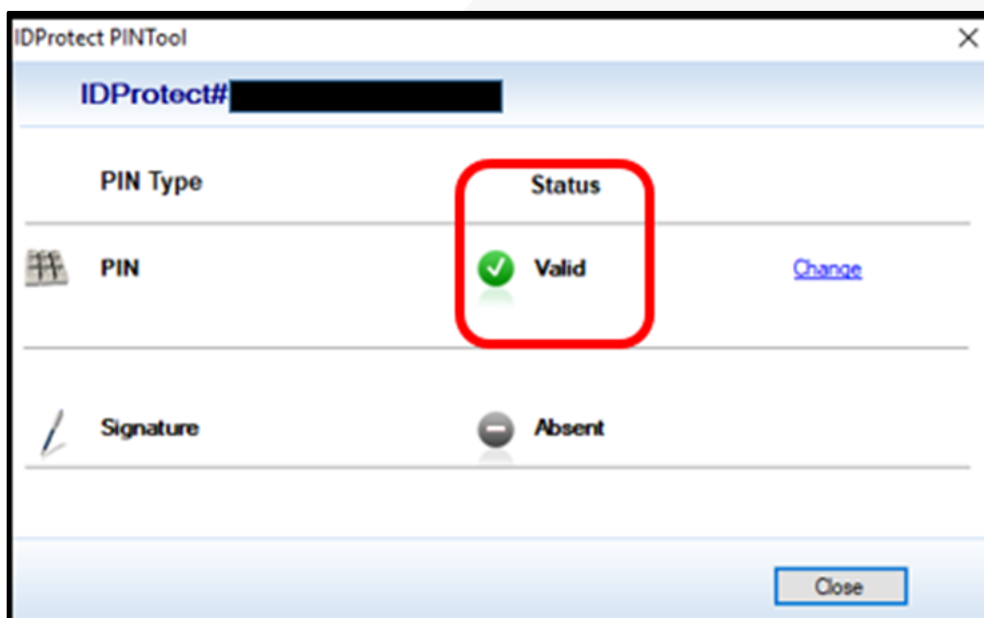
1. Primero se debe verificar que el lector y la tarjeta se encuentren conectados en el equipo.
2. En la esquina inferior derecha de la pantalla buscar el icono "IDProtect Monitor".



3. Presionar el icono y seleccionar la opción "Manage Pin".



4. En el espacio de "Status" podrá visualizar el estado de la firma.



### 3. Componente de Firma

- a. Es recomendable visitar la pagina donde se encuentra disponible los manuales e instalador del componente de firma actualizado:  
<https://www.sicop.go.cr/componenteFirmaCR/>
- b. En el manual de instalación se indica detalladamente cada uno de los pasos que se deben seguir para instalar exitosamente el software del Componente de Firma.

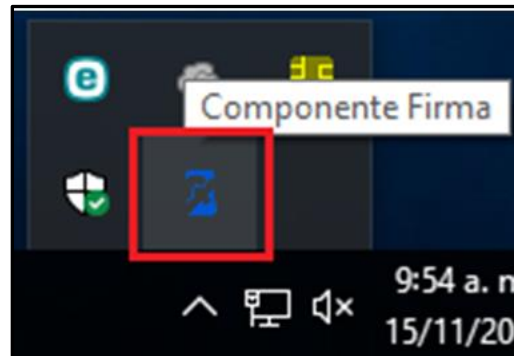
### 3.1 Requerimientos del sistema para poder utilizar el componente de firma

<b>Sistema operativo</b>	<ul style="list-style-type: none"> <li>• Windows 7</li> <li>• Windows 8</li> <li>• Windows 10</li> <li>• Windows 11</li> </ul>
<b>Navegadores Web compatibles</b>	<ul style="list-style-type: none"> <li>• Google Chrome</li> </ul>
<b>Controladores</b>	<ul style="list-style-type: none"> <li>• Driver firma digital, pueden ser descargados del siguiente enlace: <a href="https://www.soportefirmadigital.com/sfdj/dl.aspx?lang=es">https://www.soportefirmadigital.com/sfdj/dl.aspx?lang=es</a></li> </ul>
<b>Java</b>	<ul style="list-style-type: none"> <li>• A partir de la versión 3.0.4 no se requiere instalarlo.</li> </ul>
<b>Dispositivo</b>	<ul style="list-style-type: none"> <li>• Smartcard Reader y tarjeta inteligente emitida por el Sistema Nacional de Firma Digital de Costa Rica.</li> </ul>

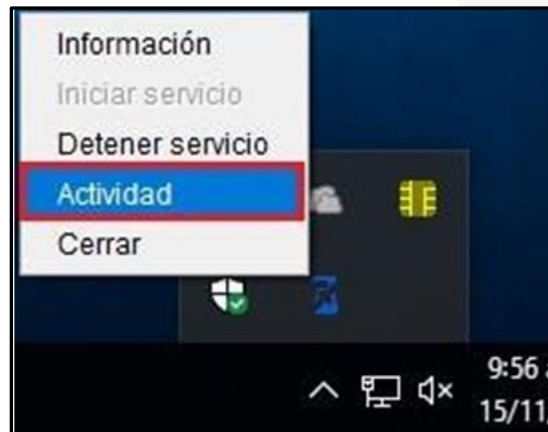
### 3.2 Consultar el log del componente

Una vez instalado el componente de firma digital se podrá consultar la bitácora de actividad, donde quedan registrados eventos como cambios o errores. Para realizar consulta del log de la aplicación se deben seguir los siguientes pasos:

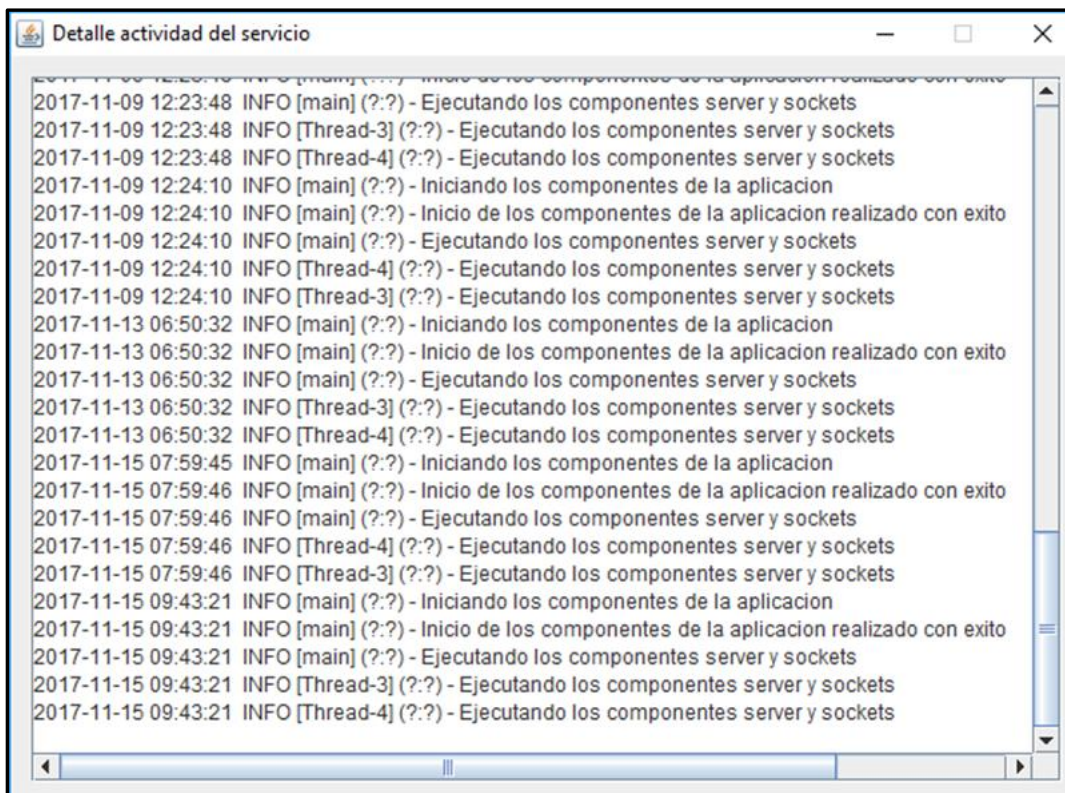
1. Ir a la barra de tareas de Windows y presionar el icono que se encuentra en la esquina inferior derecha, buscar el icono nombrado "Componente Firma".



2. Oprimir con el botón derecho del mouse sobre el icono, seleccionar la opción "Actividad".

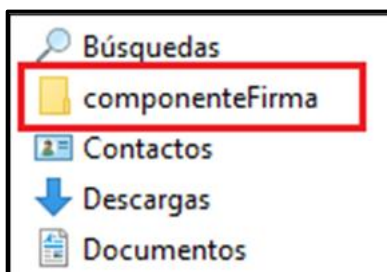


3. Se muestra una ventana donde se visualiza todos los procesos y errores que se han ejecutado en el componente.



Otra manera de consultar el log del componente es desde el archivo `debitácoras` directamente. Para esto puede seguir los siguientes pasos.

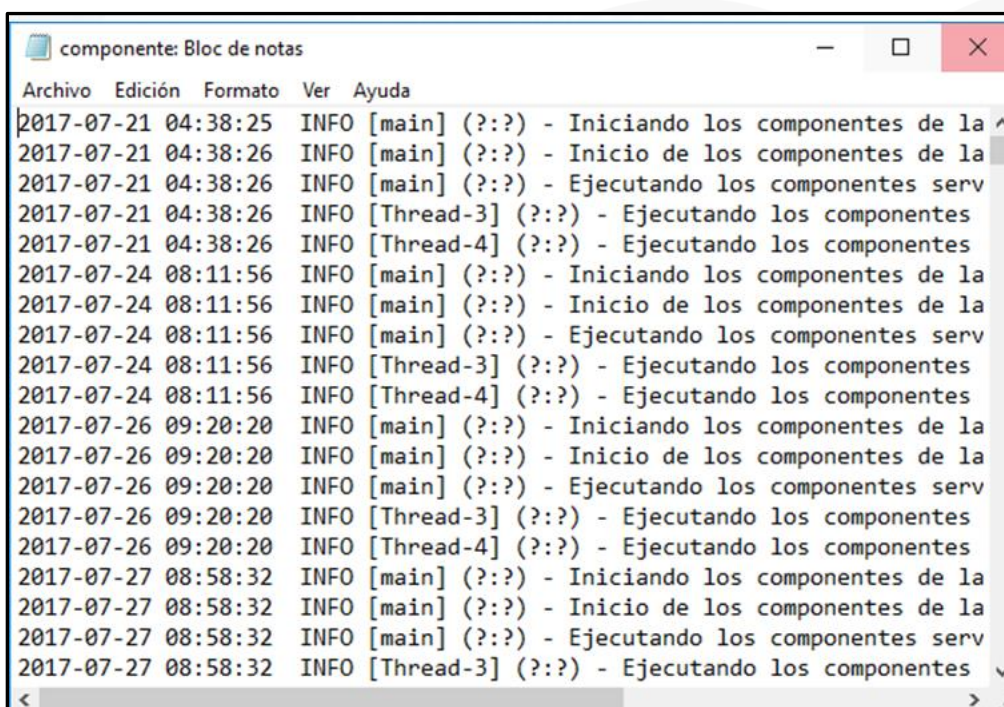
1. Ubicarse en "Mi PC"-> Carpeta de usuario -> `componenteFirma`.



2. Cuando ingrese a esta carpeta tendrá varios documentos, debe seleccionar el que se denomina "`componente.txt`".



3. Al abrir el documento se lo mostrará la información del log del componente.

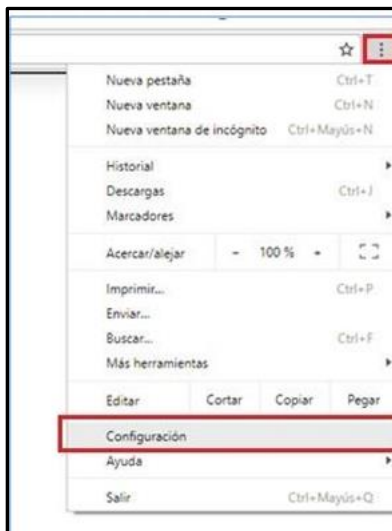


#### 4. Comprobar versión del navegador

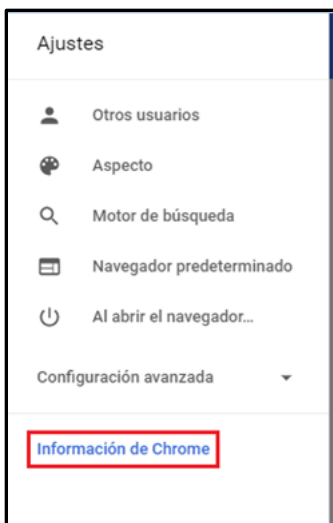
Es de suma importancia que el navegador se utilice con la versión del navegador adecuada, se deben ejecutar los siguientes pasos para verificar la versión según sea el navegador que se está utilizando:

##### 4.1 Versión de Chrome

1. Desde el navegador de Chrome dirigirse al menú de opciones y luego ir a la opción de configuración.

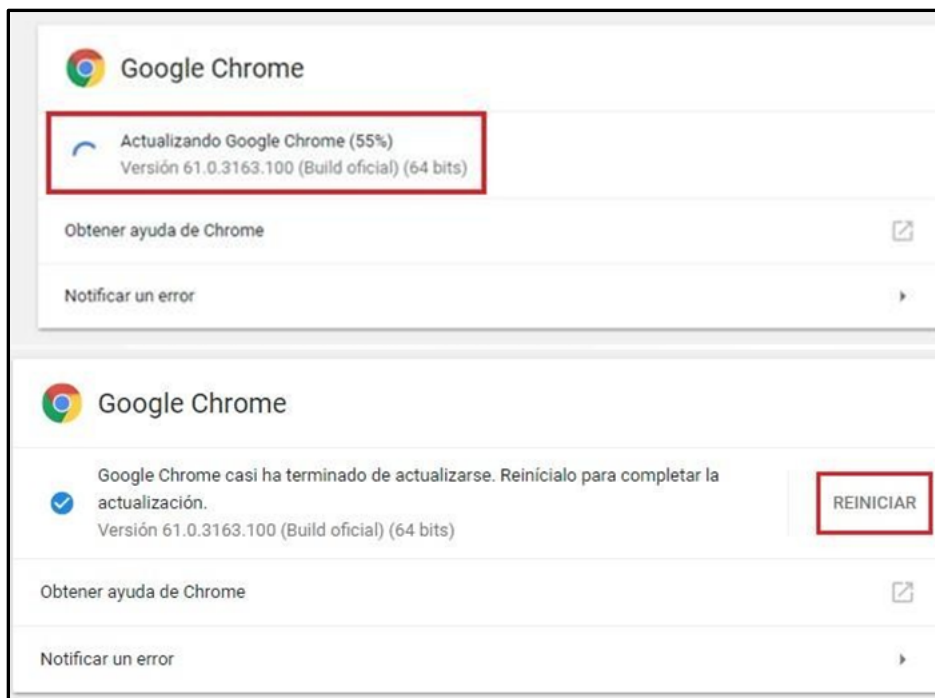


2. Ingresar al menú "Información de Chrome".



3. Se muestra una ventana donde se indica la versión de Chrome, en caso de que no esté actualizado él mismo se actualiza sin necesidad de asistencia. Cuando termine la actualización simplemente presionar en reiniciar, esto hará que se cierre el navegador y vuelva a abrirse aplicando los cambios de la nueva versión.

**Nota:** Para garantizar un correcto funcionamiento de la plataforma se debe tener instalado la versión de Google Chrome 60 o superior.



#### 4.2 Verificar la disponibilidad del puerto

Debe verificar que el puerto de salida que usa su plataforma esté disponible para tener acceso de manera exitosa.

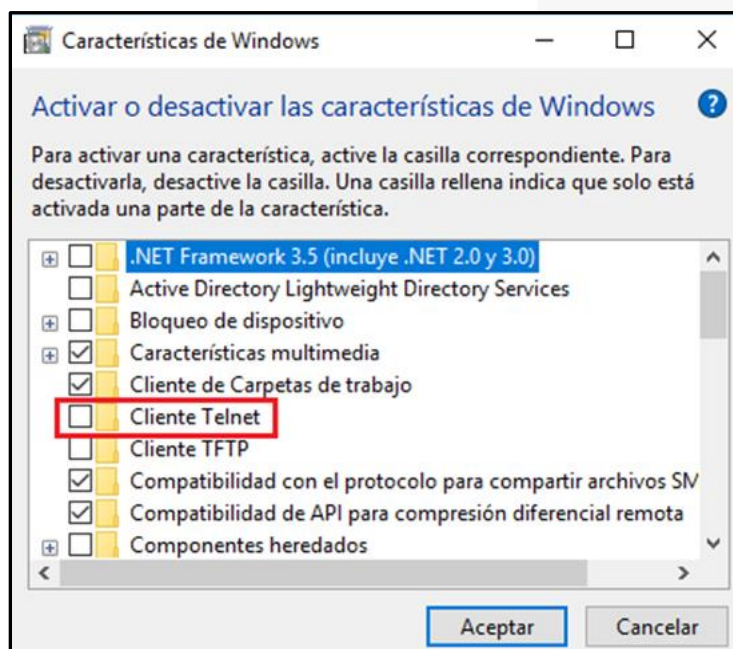
**Nota:** Para realizar estos cambios debe contar con permisos de administrador, si no cuenta con ellos contacte al administrador para que continúe con el proceso. Para realizar el proceso de verificación de disponibilidad de puertos, se deben ejecutar los siguientes pasos:

1. Habilitar o tener disponible un cliente Telnet en el equipo, para confirmarlo diríjase a “Panel de control” y seguidamente ingrese a “Programas”.

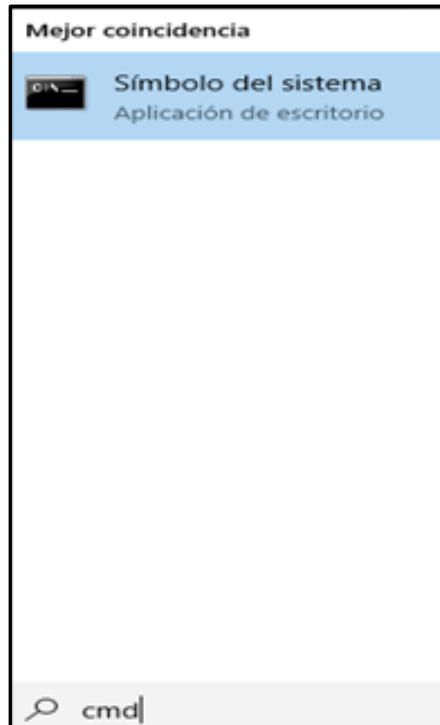




2. Abrir la opción de “Activar las características de Windows”.
3. En la ventana que se le muestra, activar la casilla de “Cliente Telnet”.



- Esperar a que se realicen los cambios, una vez terminados cierre las ventanas y presione el botón de inicio de Windows, se debe digitar “CMD” y accederá al programa de “Símbolo del sistema”.



- Desde la ventana de la consulta se puede verificar la disponibilidad de los puertos, para esto debe escribir los siguientes comandos:
  - telnet localhost 4501 (Con esto probará el puerto de acceso 4501)
  - telnet localhost 4502 (Con esto probará el puerto de acceso 4502)

```
Símbolo del sistema
Microsoft Windows [Versión 10.0.15063]
(c) 2017 Microsoft Corporation. Todos los derechos reservados.
C:\Users\juretana>telnet localhost 4501
```

- Digitar el comando y oprimir la tecla “Enter”.

- Se muestra una ventana como la siguiente imagen, lo cual significa que el puerto se encuentra habilitado:

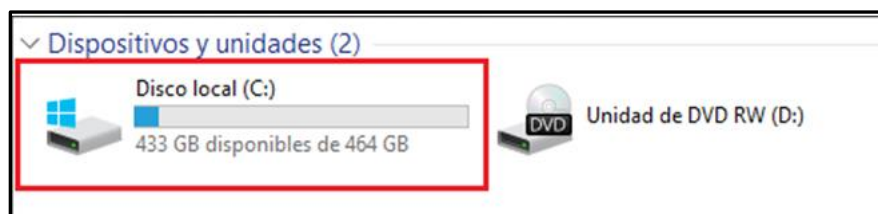


- En caso de que el puerto no esté habilitado se muestra un mensaje de error como el de la siguiente imagen:

```
C:\Users\admini>telnet localhost 4503
Conectándose a localhost...No se puede abrir la conexión al host, en puerto 4503: Error en la conexión
```

## 5. Verificar archivo host

- Ubicarse en el disco local C:



2. Luego ingresar a la carpeta “Windows”.

Archivos de programa	15/11/2017 11:57 a...	Carpeta de archivos
Archivos de programa (x86)	15/11/2017 11:57 a...	Carpeta de archivos
Firma Digital	21/7/2017 4:37 p. m.	Carpeta de archivos
Intel	20/7/2017 8:36 a. m.	Carpeta de archivos
OMNIKEY	21/7/2017 4:36 p. m.	Carpeta de archivos
PerfLogs	18/3/2017 3:03 p. m.	Carpeta de archivos
Usuarios	16/8/2017 8:24 a. m.	Carpeta de archivos
Windows	15/11/2017 8:18 a. ...	Carpeta de archivos

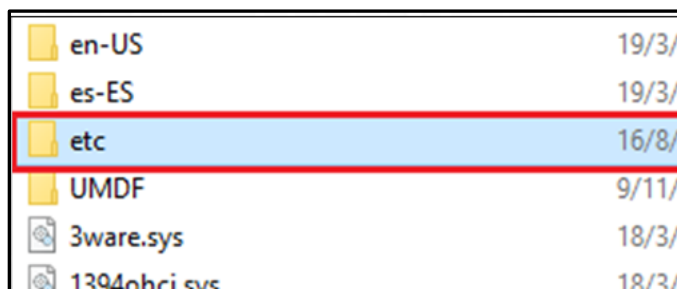
3. Buscar la carpeta “System32”.

SKB	19/3/2017 11:15 p....	
SoftwareDistribution	16/8/2017 8:33 a. m.	
Speech	18/3/2017 3:03 p. m.	
Speech_OneCore	18/3/2017 3:03 p. m.	
System	18/3/2017 3:03 p. m.	
System32	16/11/2017 9:06 a. ...	
SystemApps	19/3/2017 11:15 p....	
SystemResources	19/3/2017 11:15 p....	
SysWOW64	15/11/2017 8:13 a. ...	

4. Ingresar a la carpeta “drivers”.

de-DE	19/3/2017 11:15 p....	
DiagSvc	19/3/2017 11:13 p....	
Dism	10/7/2017 6:38 p. m.	
downlevel	18/3/2017 5:40 a. m.	
drivers	15/11/2017 7:56 a. ...	
DriverStore	15/11/2017 8:44 a. ...	
dsc	19/3/2017 11:13 p....	
el-GR	19/3/2017 11:15 p....	

5. Seguidamente ingresar a la carpeta “etc.”.

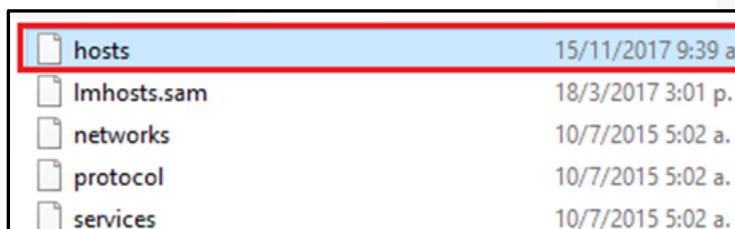


6. Una vez en la carpeta tendrá, entre los archivos existentes seleccionar el denominado “hosts”.

**Nota:** Para realizarle cambios al documento deberá tener permisos de administrador.

7. El archivo cuenta con protección por tanto para editarlo debe primero moverlo al escritorio.

8. Una vez en el escritorio presionar clic derecho, “abrir con” y utilizar “bloc de notas”.



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10      x.acme.com             # x client host
#
# localhost name resolution is handled within DNS itself.
#   127.0.0.1      localhost
#   ::1            localhost

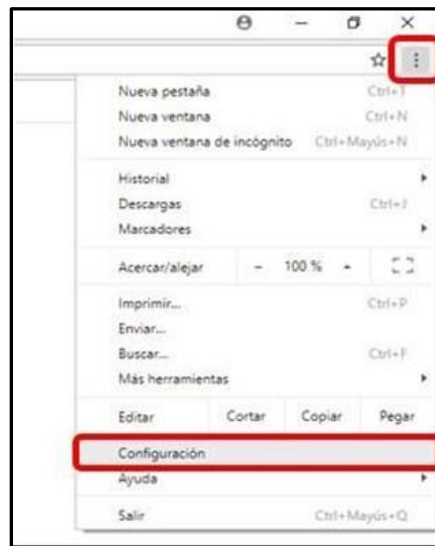
#Componente de Autenticacion y Firma Digital
127.0.0.1 service.componentefirmacr.go.cr
```

9. Puede ser que el equipo que tenga configurada una sola dirección o varias, como se muestra en el ejemplo, en caso de que la dirección 127.0.0.1 [service.componentefirmacr.go.cr](http://service.componentefirmacr.go.cr) no se encuentre registrada en el archivo, se deberá agregarle de forma manual por el usuario.

**Nota:** Esta dirección es indispensable para que el equipo funcione correctamente si no se está utilizando el navegador Google Chrome.

## 6. Habilitar las ventanas emergentes

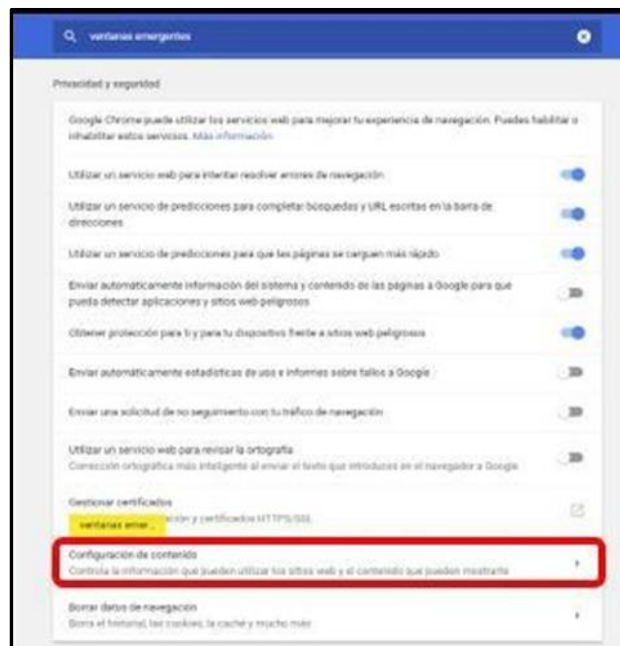
1. Presionar el botón localizado en la esquina superior derecha para desplegar una lista de opciones; luego hacer clic “Configuración”.



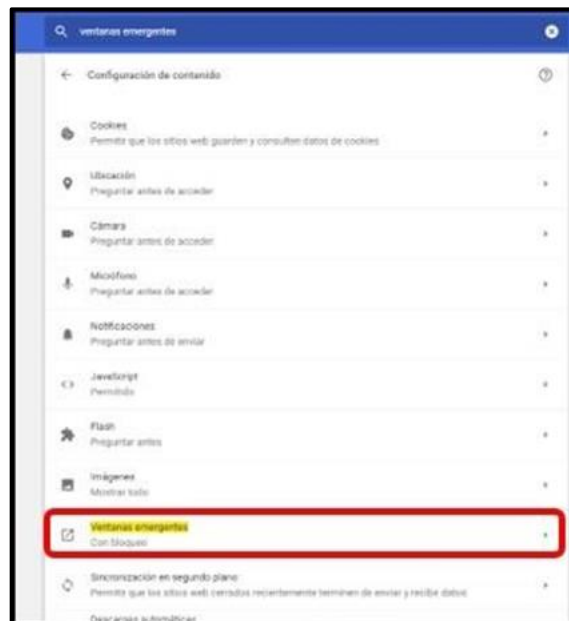
2. Escribir “ventanas emergentes” en la barra de búsqueda.



3. Hacer clic sobre la opción “Configuración de contenido” para ir a la siguiente ventana.



#### 4. Hacer clic sobre “ventanas emergentes.”



#### 5. Presionar “Añadir” en la sección llamada “Permitir”.



#### 6. En la ventana que se despliegue escribir las siguientes direcciones:

- [“https://vpj.sicop.go.cr/index.jsp”](https://vpj.sicop.go.cr/index.jsp)
- [“https://www.sicop.go.cr”](https://www.sicop.go.cr).



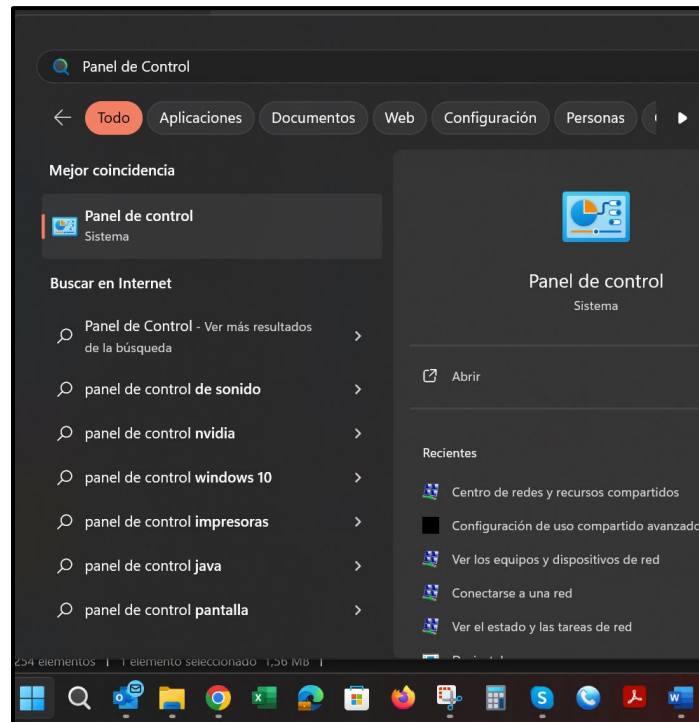
## 7. Presionar “Añadir” para terminar.



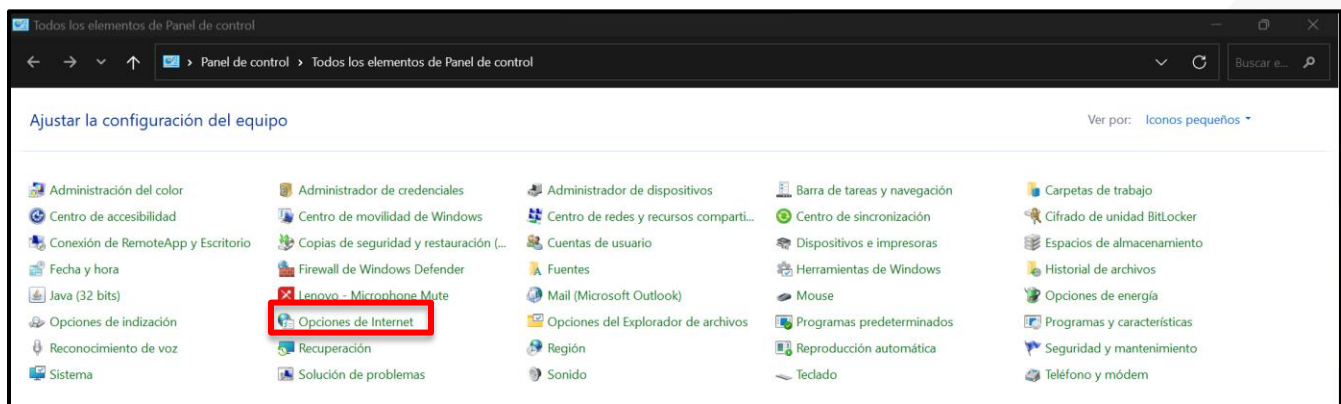
## 7. Manejo con servidores proxy

Un proxy es un servidor (un programa o sistema informático) que funciona como intermediario en las peticiones de recursos de red que realiza un cliente a otro servidor. Para saber si su computadora tiene un proxy configurado, favor realizar los siguientes pasos:

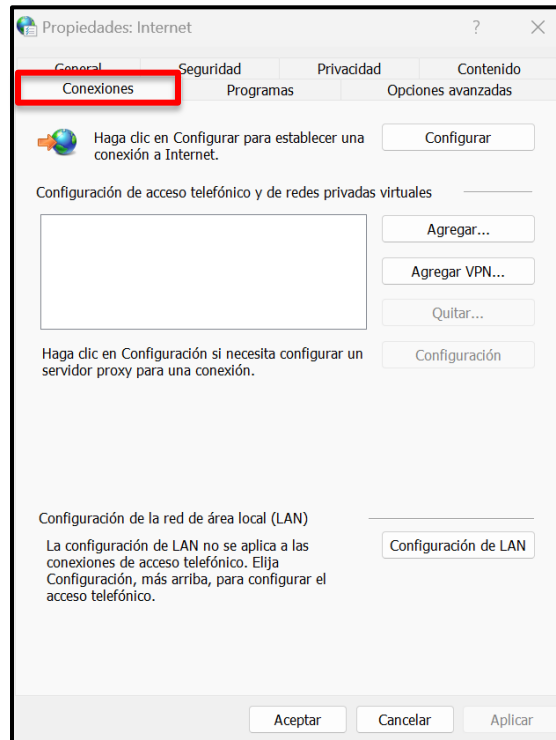
1. Dar clic sobre el botón “Inicio” opción “Panel de Control”.



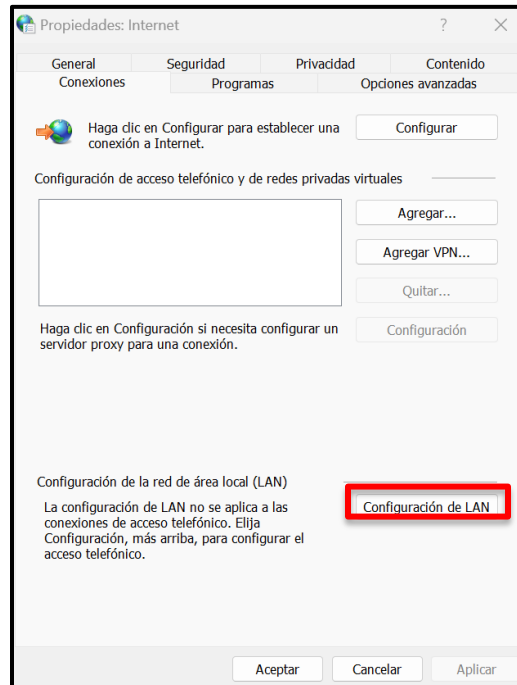
2. En la pantalla desplegada de Panel de Control, seleccionar la opción “Opciones de Internet”.



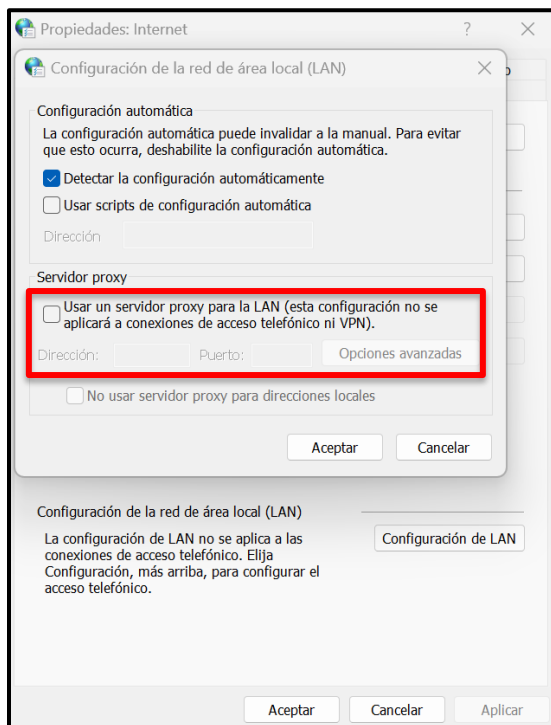
3. En la pantalla “Propiedades de Internet”, debe seleccionar la opción “Conexiones”.



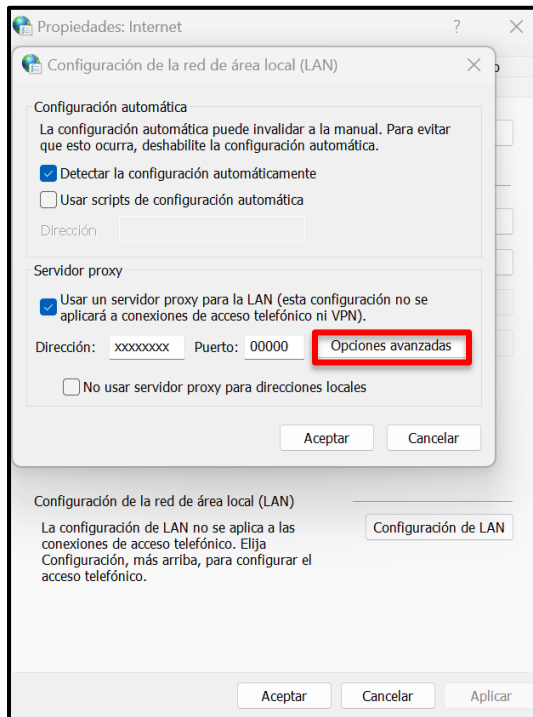
4. Luego debe presionar sobre el botón “Configuración de LAN”.



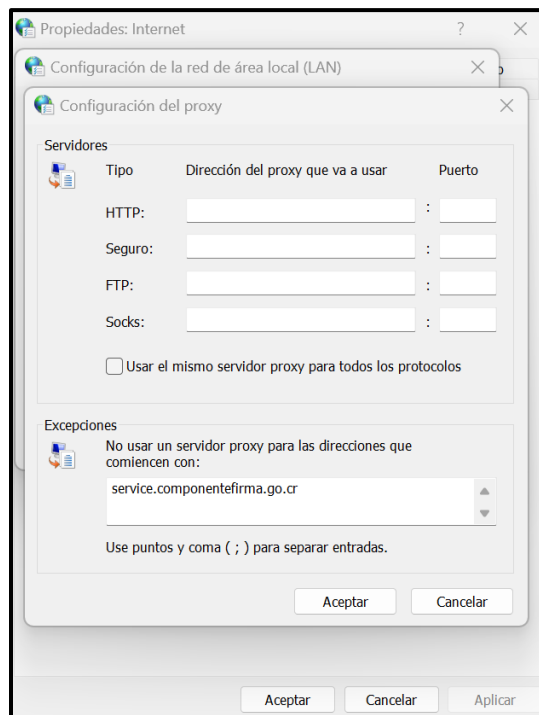
5. Si la opción que dice “Usar un servidor proxy para la LAN” no está marcada, dar clic sobre el botón “Cancelar”; con esto finalizaría el proceso.



- De lo contrario, si está marcada (seleccionada), presionar el botón "Opciones Avanzadas".



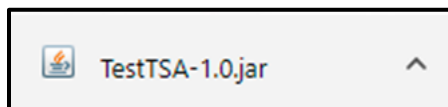
- En la pantalla que se muestra "Configuración del Proxy", en la sección "Excepciones" favor incluir los siguientes dominio [service.componentefirmacr.go.cr](http://service.componentefirmacr.go.cr) y 127.0.0.1. Luego presionar el botón "Aceptar".



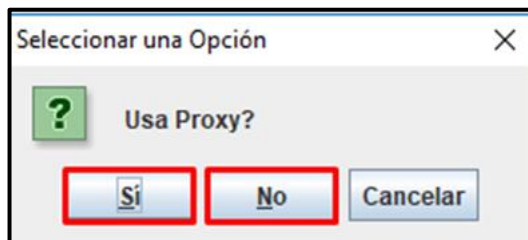
## 8. Verificar el servicio web TSA

El TSA es un servicio web de sellado de tiempo que ofrece el Banco Central de Costa Rica, su objetivo es obtener la hora y la fecha exacta en el que se realizó cierto proceso. Para verificar que este servicio está funcionando, favor seguir los siguientes pasos:

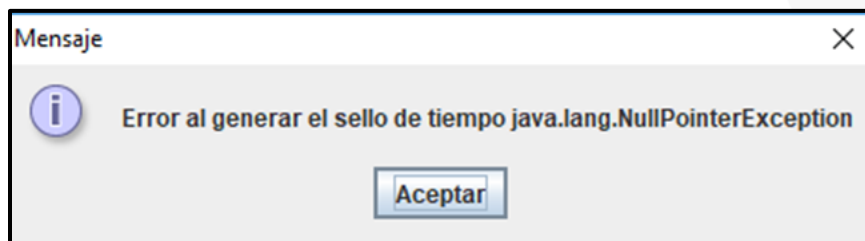
1. Ejecutar el programa descargado llamado "TestTSA-1.0".



- Una vez abierto, se debe elegir entre dos opciones, si se cuenta con un servidor proxy presione el botón “Sí”, en caso contrario hacer click sobre el botón “No”.



- Si el servicio web TSA no está siendo bloqueado debe generar la hora y la fecha exacta (Como se muestra en la siguiente imagen) cuando se presionó alguno de los dos botones anteriormente mencionados. A continuación, puede darle “Aceptar” para terminar y el programa se cerrará automáticamente.
- En caso contrario, si se despliega una ventana como se muestra en este punto, se debe agregar como excepción en el sistema de seguridad que se esté utilizando la dirección: <http://tsa.sinpe.fi.cr/tsaHttp/>.





 **SICOP**

Sistema Integrado de Compras Públicas



Hagamos el  
**futuro juntos**

