



# **MANUAL DE CONFIGURACION DEL FIREWALL EN WINDOWS PARA INSTALAR PRINTANISTA HUB**

Elaborado por: Ing. Ivonne Méndez  
13 de Febrero 2025

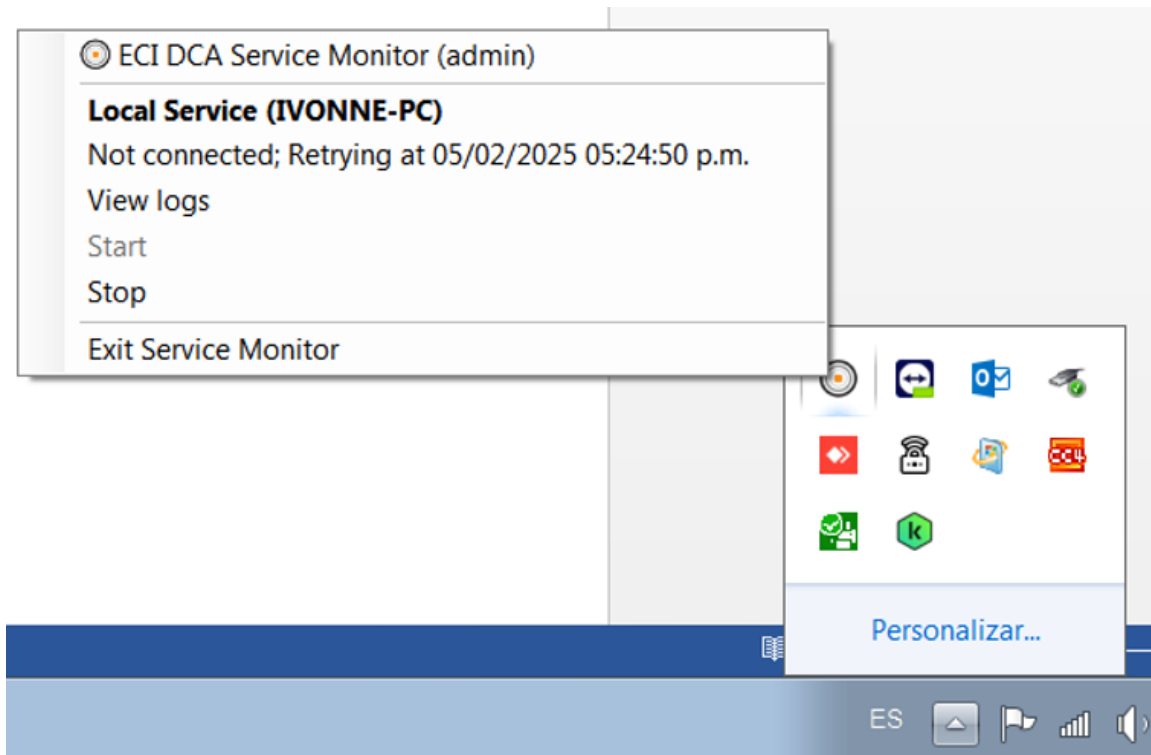
# INDICE

## Contenido

INTRODUCCION .....	3
CONFIGURACION DEL FIREWALL DE WINDOWS.....	4
REGLAS DE ENTRADA (PROGRAMA) .....	4
REGLAS DE ENTRADA (PUERTOS) .....	9
REGLAS DE SALIDA (PROGRAMA).....	12
REGLAS DE SALIDA (PUERTOS) .....	12
CONECTADO A PRINTANISTA .....	12
VERIFICACION CON EL AREA DE MONITOREO .....	13

## INTRODUCCION

Cuando instalamos Printanista Hub (ECI DCA), muchas veces aparece el mensaje de “Not connected”. Para evitar esto hay que configurar el firewall de Windows, inmediatamente después de haber realizado la instalación, tal y como se describe en los siguientes pasos.




# CONFIGURACION DEL FIREWALL DE WINDOWS

## REGLAS DE ENTRADA (PROGRAMA)

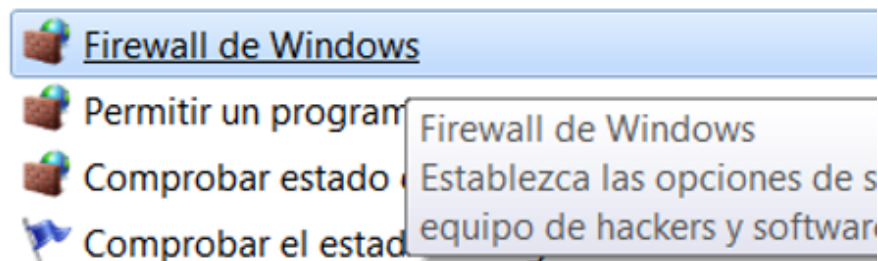
Debemos llevar a cabo los siguientes pasos:

1. En el buscador del sistema operativo escribimos la palabra “firewall de windows” y le damos clic a la opción que aparece

Programas (1)

 Firewall de Windows con seguridad avanzada

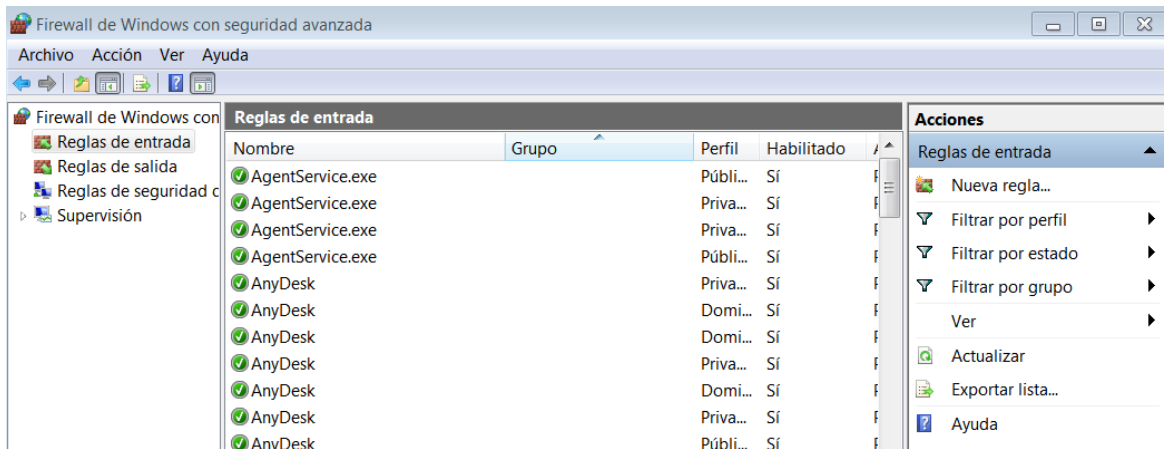
Panel de control (4)



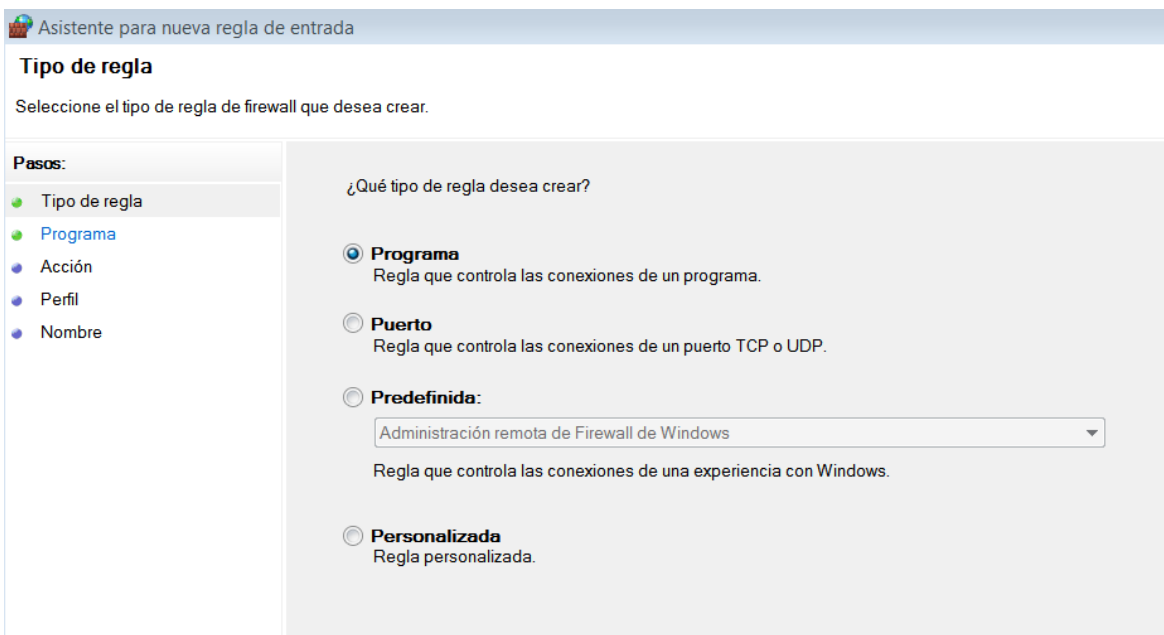
2. Se abrirá una ventana en la cual hay que darle clic en la opción de la izquierda que dice “Configuración avanzada”




3. En “Reglas de entrada” seleccionamos la opción “Nueva regla”



4. Damos clic en “Programa” y en “siguiente”



5. Clic en examinar y buscamos la consola del ECI DCA que se encuentra en la siguiente ruta en el disco local C: %ProgramFiles% (x86)\ECI DCA\DCA.Edge.Console.exe y luego clic en siguiente

 Asistente para nueva regla de entrada

### Programa

Especifique la ruta completa y el nombre del archivo ejecutable del programa con el que coincide esta regla.

**Pasos:**

- Tipo de regla
- Programa
- Acción
- Perfil
- Nombre


¿Se aplica esta regla a todos los programas o a uno específico?

☐ **Todos los programas**  
La regla se aplica a todas las conexiones en el equipo que coinciden con otras propiedades de reglas.

☒ **Esta ruta de acceso del programa:**

Ejemplo: c:\path\program.exe  
          %ProgramFiles%\browser\browser.exe

6. Clic en “Permitir la conexión” y “siguiente”

 Asistente para nueva regla de entrada

### Acción

Especifique la acción que debe llevarse a cabo cuando una conexión coincide con las condiciones especificadas en la regla.

**Pasos:**

- Tipo de regla
- Programa
- Acción
- Perfil
- Nombre

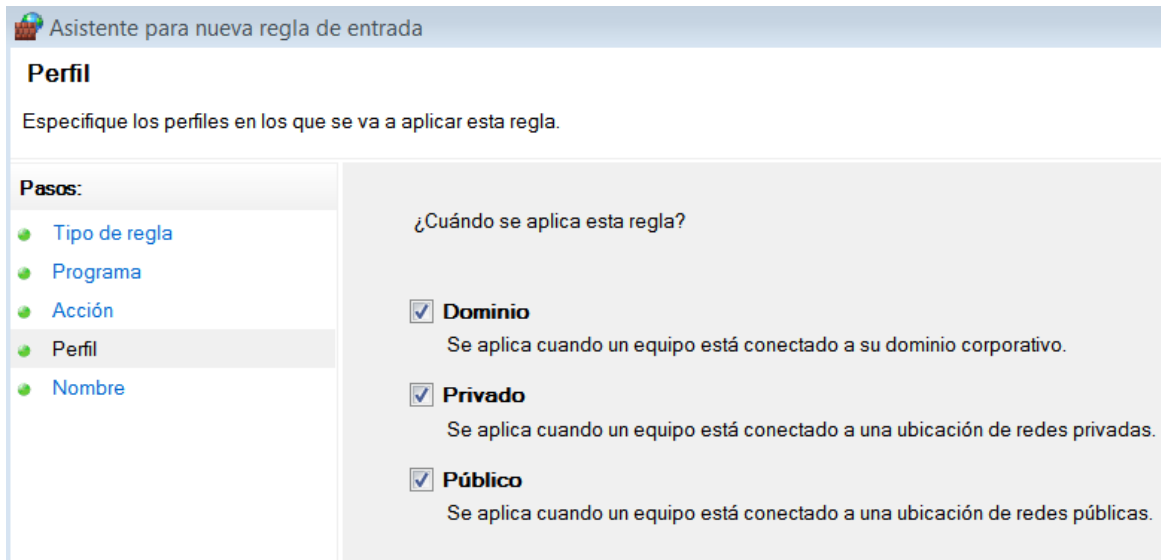
¿Qué medida debe tomarse si una conexión coincide con las condiciones especificadas?

☒ **Permitir la conexión**  
Esto incluye las conexiones protegidas mediante IPsec y las que no lo están.

☐ **Permitir la conexión si es segura**  
Esto incluye solamente las conexiones autenticadas mediante IPsec. Éstas se protegerán mediante la configuración de reglas y propiedades de IPsec del nodo Regla de seguridad de conexión.

☐ **Bloquear la conexión**

7. Seleccionamos las 3 opciones que se muestran y damos clic en “siguiente”



**Asistente para nueva regla de entrada**

### Perfil

Especifique los perfiles en los que se va a aplicar esta regla.

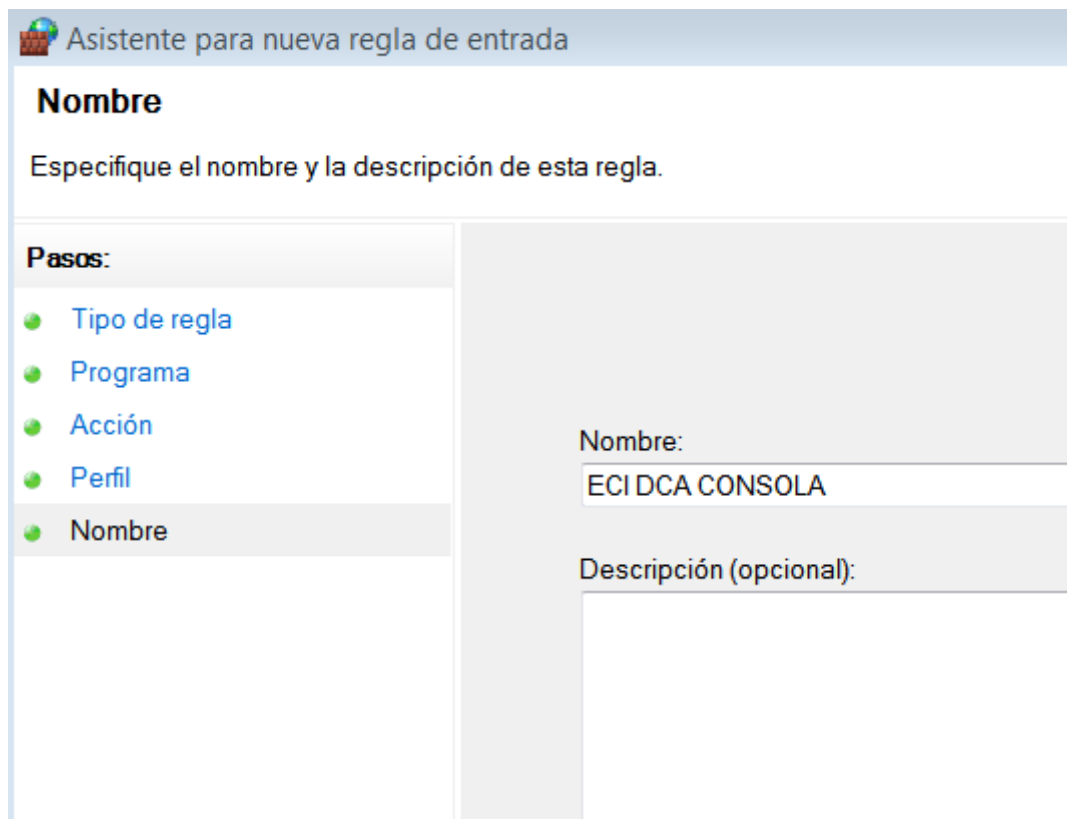
**Pasos:**

- Tipo de regla
- Programa
- Acción
- Perfil**
- Nombre

¿Cuándo se aplica esta regla?

- ☒ **Dominio**  
Se aplica cuando un equipo está conectado a su dominio corporativo.
- ☒ **Privado**  
Se aplica cuando un equipo está conectado a una ubicación de redes privadas.
- ☒ **Público**  
Se aplica cuando un equipo está conectado a una ubicación de redes públicas.

8. Le asignamos el nombre de ECI DCA Consola y clic en “Finalizar”



**Asistente para nueva regla de entrada**

### Nombre

Especifique el nombre y la descripción de esta regla.

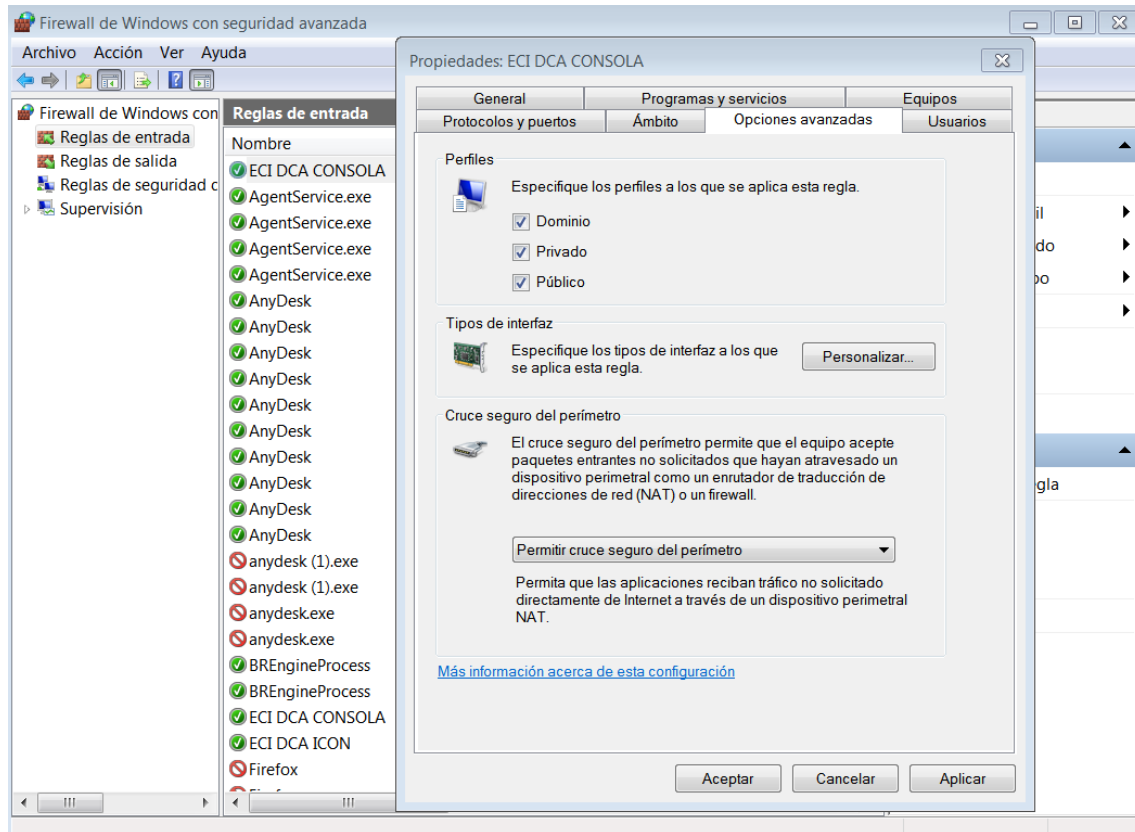
**Pasos:**

- Tipo de regla
- Programa
- Acción
- Perfil
- Nombre**

Nombre:  
ECI DCA CONSOLA

Descripción (opcional):

9. Damos doble clic en la regla creada, y en la ventana que se abrirá seleccionamos la pestaña “Opciones avanzadas”, después abajo en “Cruce seguro del perímetro” seleccionamos “Permitir cruce seguro del perímetro”.



10. Creamos una nueva regla de entrada pero ahora con la ruta %ProgramFiles% (x86)\ECI DCA\DCA.Edge.TrayIcon.exe y seguimos todos los pasos anteriores



Asistente para nueva regla de entrada

### Programa

Especifique la ruta completa y el nombre del archivo ejecutable del programa con el que coincide esta regla.

**Pasos:**

- Tipo de regla
- Programa
- Acción
- Perfil
- Nombre

¿Se aplica esta regla a todos los programas o a uno específico?

☐ **Todos los programas**  
La regla se aplica a todas las conexiones en el equipo que coinciden con otras propiedades de reglas.

☒ **Esta ruta de acceso del programa:**

Ejemplo: c:\path\program.exe  
%ProgramFiles%\browser\browser.exe

## REGLAS DE ENTRADA (PUERTOS)

1. Crearemos 2 reglas de entrada, 1 para el puerto 443 y otra para el 53. Debemos seleccionar la palabra “Puerto” y damos clic en siguiente.

Asistente para nueva regla de entrada

### Tipo de regla

Seleccione el tipo de regla de firewall que desea crear.

**Pasos:**

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

¿Qué tipo de regla desea crear?

☐ **Programa**  
Regla que controla las conexiones de un programa.

☒ **Puerto**  
Regla que controla las conexiones de un puerto TCP o UDP.


☐ **Predefinida:**

▼

Regla que controla las conexiones de una experiencia con Windows.

☐ **Personalizada**  
Regla personalizada.

2. Seleccionamos la opción “TCP” y “Puertos locales específicos”, en donde escribiremos el puerto que queremos abrir, en este caso el 443 y damos clic en siguiente.

 Asistente para nueva regla de entrada

### Protocolo y puertos

Especifique los puertos y protocolos a los que se aplica esta regla.

**Pasos:**

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

¿Se aplica esta regla a TCP o UDP?


☒ TCP  
☐ UDP

¿Se aplica esta regla a todos los puertos locales o a unos puertos locales específicos?

☐ Todos los puertos locales  
☒ Puertos locales específicos:

443  
Ejemplo: 80, 443, 5000-5010

3. Seleccionamos “Permitir la conexión” y clic en siguiente.

 Asistente para nueva regla de entrada

### Acción

Especifique la acción que debe llevarse a cabo cuando una conexión coincide con las condiciones especificadas en la regla.

**Pasos:**

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre


¿Qué medida debe tomarse si una conexión coincide con las condiciones especificadas?

☒ **Permitir la conexión**  
 Esto incluye las conexiones protegidas mediante IPsec y las que no lo están.

☐ **Permitir la conexión si es segura**  
 Esto incluye solamente las conexiones autenticadas mediante IPsec. Éstas se protegerán mediante la configuración de reglas y propiedades de IPsec del nodo Regla de seguridad de conexión.

Personalizar...

4. Elegimos las 3 opciones y clic en siguiente:

 Asistente para nueva regla de entrada

### Perfil

Especifique los perfiles en los que se va a aplicar esta regla.

**Pasos:**

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil**
- Nombre

¿Cuándo se aplica esta regla?

- ☒ **Dominio**  
Se aplica cuando un equipo está conectado a su dominio corporativo.
- ☒ **Privado**  
Se aplica cuando un equipo está conectado a una ubicación de redes privadas.
- ☒ **Público**  
Se aplica cuando un equipo está conectado a una ubicación de redes públicas.

5. Le damos un nombre al puerto y clic en finalizar.

 Asistente para nueva regla de entrada

### Nombre

Especifique el nombre y la descripción de esta regla.

**Pasos:**

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre**

Nombre:

Descripción (opcional):

## REGLAS DE SALIDA (PROGRAMA)

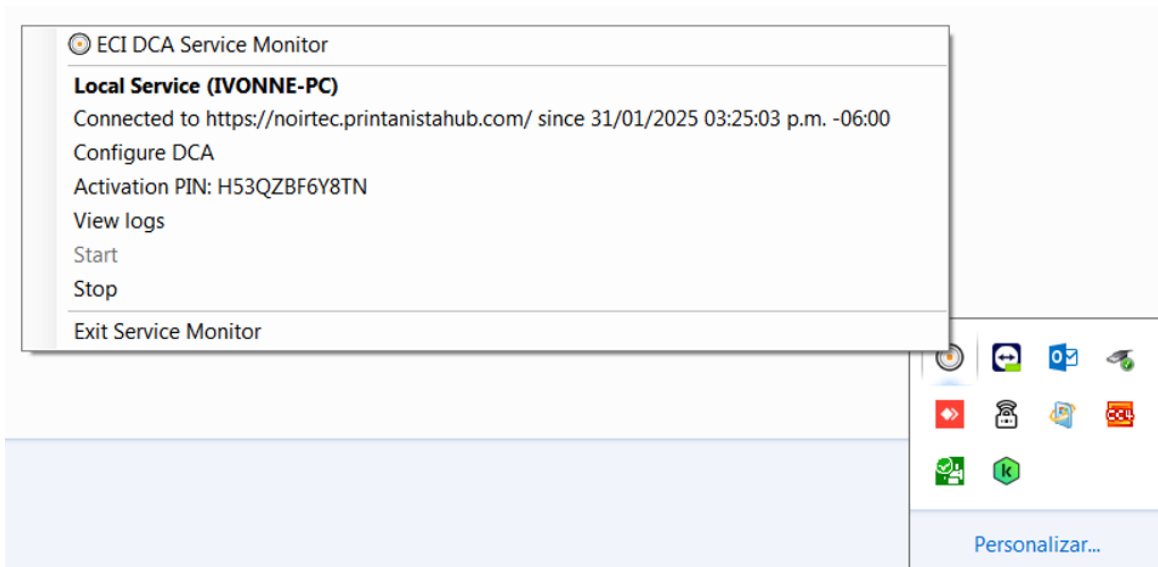
En reglas de salida crearemos 2 nuevas reglas, usando los mismos pasos que en la creación de REGLAS DE ENTRADA (PROGRAMA), con las mismas rutas de la Consola y TrayIcon del ECI DCA

## REGLAS DE SALIDA (PUERTOS)

Creamos 2 reglas de salida, 1 para el puerto 443 y otra para el 53, igual que en el apartado de REGLAS DE ENTRADA (PUERTOS)

## CONECTADO A PRINTANISTA

Una vez aplicadas las reglas del firewall, revisamos que en la barra de tareas haya aparecido el icono del ECI DCA (Printanista hub) con la palabra “Connected”



## VERIFICACION CON EL AREA DE MONITOREO

Luego de haber terminado todos los pasos de instalación, hay que verificar con el área de monitoreo como paso final, si le aparece correctamente instalado el software del cliente en la cuenta de Printanista Hub.

**ECI DCA** Overview Host Info Stats Discovery Devices Configuration Logs

### Status

- **Connection:** Connected to <https://noirtec.printanistahub.com/> since 18/02/2025 03:17:36 a. m. -06:00
- **Server:** Printanista Hub 5.8.20.11437
- **Activation:** Activated
- **Discovery:** Idle. Last scan at 18/02/2025 10:15:23 a. m. -06:00 found 7 devices on 256 IPs in 0:01:38.5895671
- **Devices Monitored:** 7

Dicha área ingresará al escritorio remoto de Printanista y le debe aparecer la cantidad total de dispositivos monitoreados en la opción “Overview”, y en “Devices” deberá aparecer la ip y modelo de cada dispositivo monitoreado. De no ser así, el área de monitoreo proporcionará los nuevos pasos a seguir o el manual correspondiente, para concluir con la instalación.

**ECI DCA** Overview Host Info Stats Discovery Devices Configuration Logs

All Devices

Collection Engine	Endpoint	Thumbprint	Detail
Onsite	10.9.14.121:161	13QU...9QEF	EnterpriseNumbers=1347/2699;HrDeviceDescr=ECOSYS M4125idn;HrDeviceID=1.3.6.1.4.1.1347.43.1.2.1
Pulse	10.9.14.140:161	5L4A...5NGA	EnterpriseNumbers=1536/2385/2699;HrDeviceDescr=SHARP MX-M363N;HrDeviceID=1.3.6.1.4.1.2385.3.1.71.1.2
Pulse	10.9.14.141:161	47PG...QKHP	EnterpriseNumbers=1536/2385/2699;HrDeviceDescr=SHARP MX-M283N;HrDeviceID=1.3.6.1.4.1.2385.3.1.71.1.1
Pulse	10.9.14.161:161	4B6C...4V8X	EnterpriseNumbers=641/2699;HrDeviceDescr=Lexmark MS811 406347990P92D LW40.DN2.P439;HrDeviceID=0.0
Pulse	10.9.14.170:161	55E7...W1NQ	EnterpriseNumbers=11/1240/2435/2699;HrDeviceDescr=Brother DCP-L5650DN series;HrDeviceID=0.0
Onsite	10.9.14.57:161	49HF...GR69	EnterpriseNumbers=1347/2699;HrDeviceDescr=TASKalfa MZ3200i;HrDeviceID=1.3.6.1.4.1.1347.43.1.2.1
Pulse	10.9.14.72:161	3PZP...61J1	EnterpriseNumbers=641/2699;HrDeviceDescr=Lexmark MS811 40636C6604P2K LW50.DN2.P544;HrDeviceID=0.0