

<b>CABS</b> Computo TV	<b>Certificación DSI a equipos de CABS</b>	<b>Versión</b>	7.0
		<b>Fecha</b>	03/04/2018
		<b>Área</b>	CABS
		<b>Realizó</b>	Lizeth García
		<b>Revisó</b>	Arturo García
		<b>Aprobó</b>	Ernesto Espinosa

Alcance	Objetivo
Aplica a bloqueadoras y Testigos	Certificar todas las bloqueadoras y testigos del área.

## Procedimiento

1. Transferir la carpeta CERTIFICACIÓN, que debe contener los siguientes archivos:

- Carpeta GPOW7
- certificacionDSI.exe
- Front\_check\_3p.exe
- GPOBKP.bat
- lectura\_default\_password.exe
- LGPO.exe
- md5.exe

GPOW7	11/12/2017 12:11 p...	Carpeta de archivos	
img	11/12/2017 12:11 p...	Carpeta de archivos	
130717.act	26/03/2018 11:43 a...	Archivo ACT	1 KB
activar-servicios.bat	27/12/2017 03:46 p...	Archivo por lotes de...	1 KB
Certificacion_DSI.exe	23/03/2018 05:37 p...	Aplicación	562 KB
Cetificacion DSI para Bloqueadoras y Testigo...	28/02/2018 03:03 p...	Foxit Reader PDF D...	1,348 KB
Front_check_3p.exe	20/06/2017 06:24 p...	Aplicación	266 KB
GPOBKP.bat	01/12/2017 12:51 p...	Archivo por lotes de...	1 KB
ips.txt	15/03/2018 10:03 p...	Documento de texto	1 KB
lectura_default_password.exe	22/03/2018 11:06 p...	Aplicación	685 KB
LGPO.exe	20/01/2016 02:54 p...	Aplicación	372 KB
md5.exe	15/01/2008 11:19 a...	Aplicación	48 KB

2. Ejecutar como administrador la aplicación **lectura\_default\_password.exe**

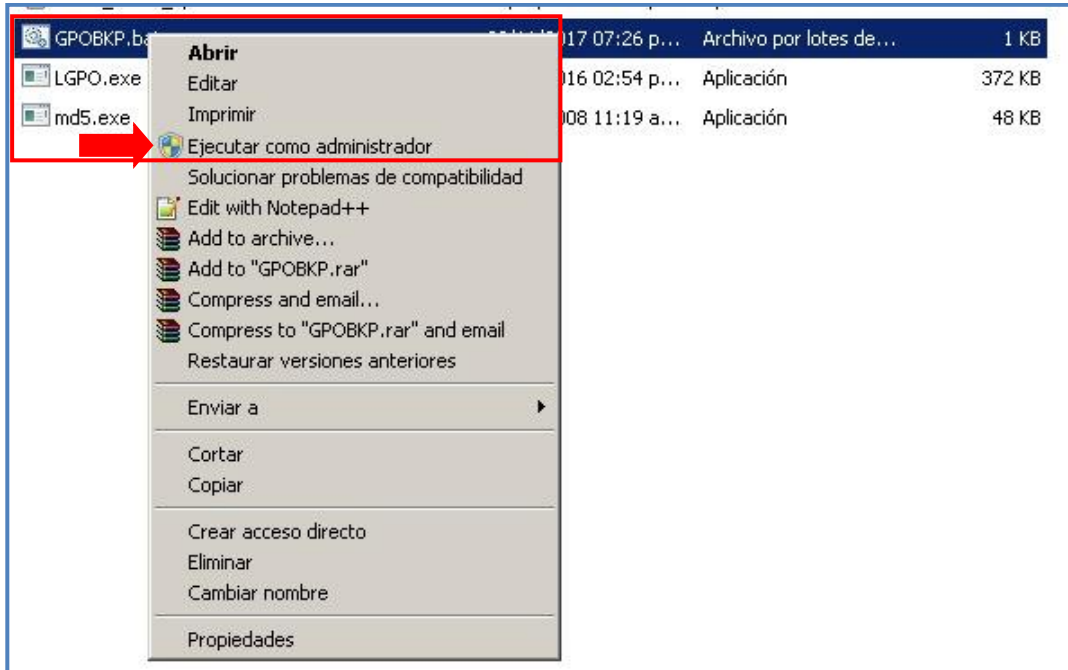
GPOW7	11/12/2017 12:11 p...	Carpeta de archivos	
img	11/12/2017 12:11 p...	Carpeta de archivos	
130717.act	26/03/2018 11:43 a...	Archivo ACT	1 KB
activar-servicios.bat	27/12/2017 03:46 p...	Archivo por lotes de...	1 KB
Certificacion_DSI.exe	23/03/2018 05:37 p...	Aplicación	562 KB
Cetificacion DSI para Bloqueadoras y Testigo...	28/02/2018 03:03 p...	Foxit Reader PDF D...	1,348 KB
Front_check_3p.exe	20/06/2017 06:24 p...	Aplicación	266 KB
GPOBKP.bat	01/12/2017 12:51 p...	Archivo por lotes de...	1 KB
ips.txt	15/03/2018 10:03 p...	Documento de texto	1 KB
lectura_default_password.exe	22/03/2018 11:06 p...	Aplicación	685 KB
LGPO.exe	20/01/2016 02:54 p...	Aplicación	372 KB
md5.exe	15/01/2008 11:19 a...	Aplicación	48 KB

2.1 La aplicación al ejecutarse mostrara un **usuario** y **password**, mismos que deben ser guardados ya que se utilizaran posteriormente.

The application window displays the following elements:

- Header:** E:\CERTIFICACION\ - 1.0.0.3.22/03/18.23:06:08
- Fields and Buttons:**
  - directorio actualizacion: D:\actualizacion\_13-07-17\
  - act 3qs -> 4s2
  - crea usuario default:
  - directorio aplicacion MB: D:\minibloq\
  - act 3qs -> 4s2 serv [40]
  - autoinicio usr default:
  - reg filtros:
  - usuario admin: desarrollo
  - password admin:
  - cambia contraseña adm:
  - autoinicio usr admin:
  - abre cons:
  - cierra cons:
  - borra usuario default:
- Status Box (indicated by a red arrow):**
  - dominio: 112395\_TB1
  - usuario admin: desarrollo
  - default password: no configurado

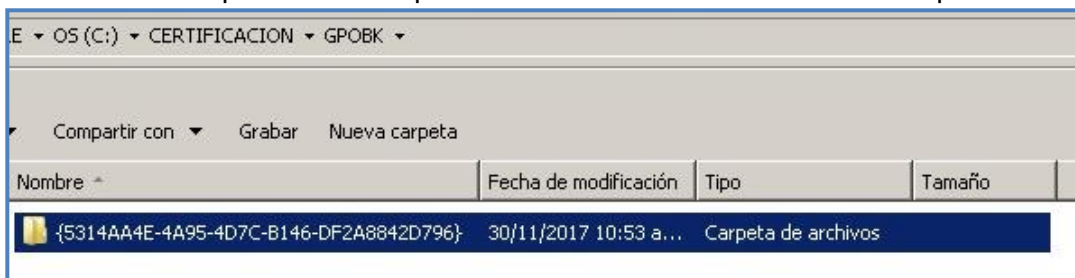
### 3. Ejecutar como administrador el archivo **GPOBK.bat**



Se generaran dos carpetas **GPOBK** y **REGBK**.

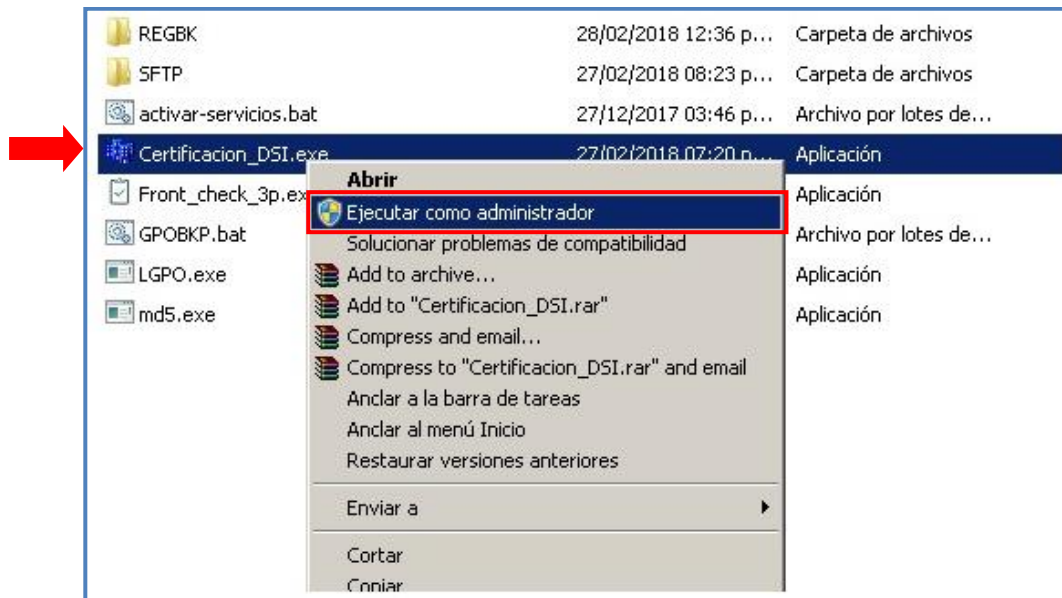
GPOBK	28/02/2018 12:36 p...	Carpeta de archivos	
GPOW7	11/12/2017 12:11 p...	Carpeta de archivos	
img	11/12/2017 12:11 p...	Carpeta de archivos	
REGBK	28/02/2018 12:36 p...	Carpeta de archivos	
SFTP	27/02/2018 08:23 p...	Carpeta de archivos	
activar-servicios.bat	27/12/2017 03:46 p...	Archivo por lotes de...	1 KB
Certificacion_DSI.exe	27/02/2018 07:20 p...	Aplicación	559 KB
Front_check_3p.exe	20/06/2017 05:24 p...	Aplicación	266 KB
GPOBK.bat	01/12/2017 12:51 p...	Archivo por lotes de...	1 KB
LGPO.exe	20/01/2016 02:54 p...	Aplicación	372 KB
md5.exe	15/01/2008 11:19 a...	Aplicación	48 KB

Se creara un respaldo en la carpeta **GPOBK** de las directivas de la máquina

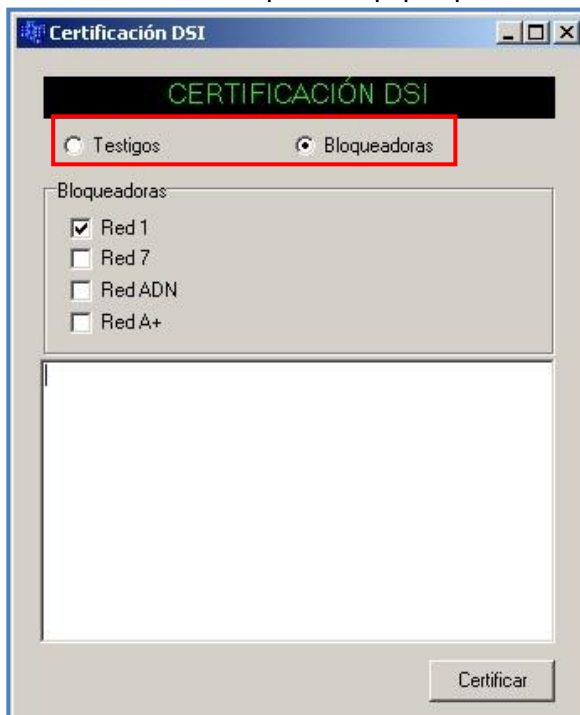


4. Ejecutar como administrador la aplicación **certificacionDSI.exe**

**Nota:** Al realizar este paso se copiarán automáticamente los archivos **Backup.XML** y **Bkupinfo.XML** en la carpeta GPOW7

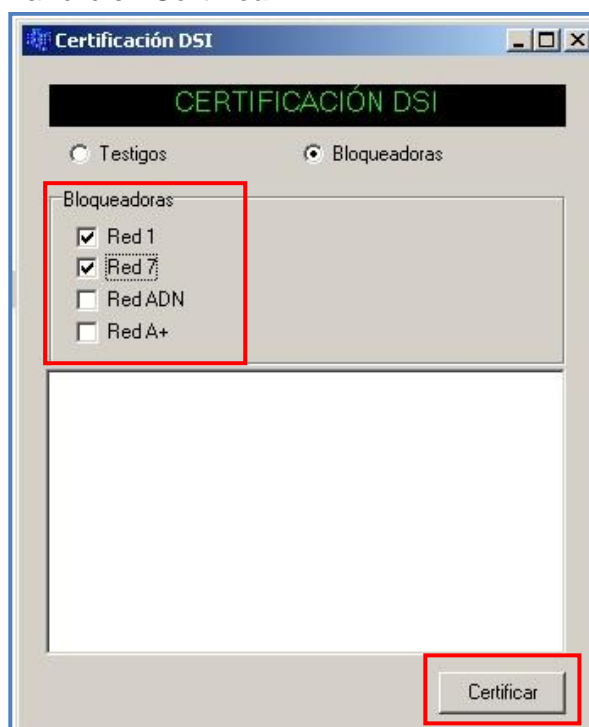


4.1 Seleccionar el tipo de equipo que se desea certificar: Testigos o Bloqueadoras.



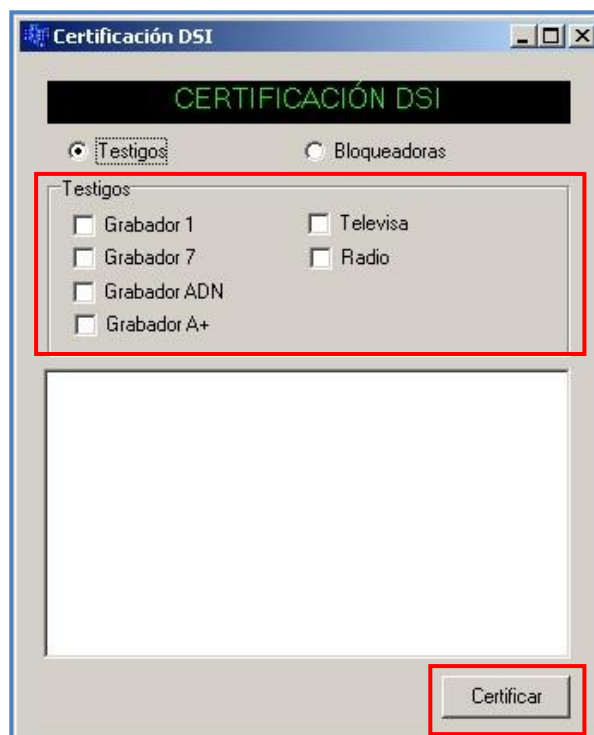
4.2 En caso de seleccionar Bloqueadoras, se procede a seleccionar la red.

**Nota:** Se puede seleccionar más de una red en el caso de que se cuente con subcanal.  
Dar clic en **Certificar**.



4.3 En caso de seleccionar Testigos, se procede a seleccionar el grabador.

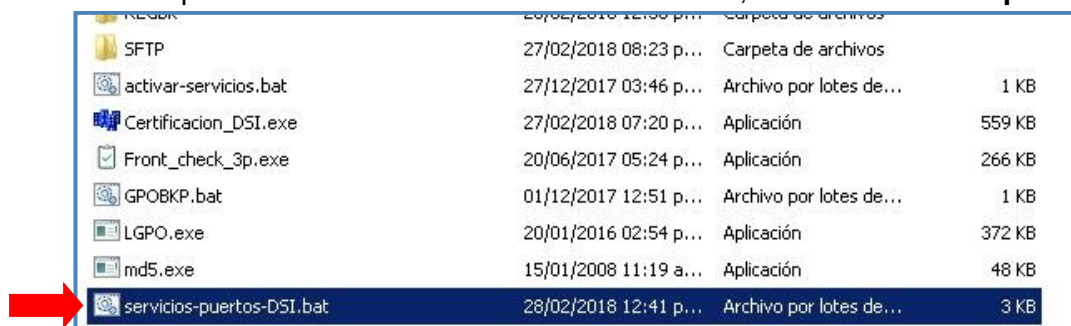
Dar clic en **Certificar**



4.4 La aplicación mostrara un mensaje de éxito cuando la certificación haya sido aplicada al equipo.



5. En la carpeta Certificación se crea un archivo .bat, llamado **servicios-puertos-DSI.bat**.



5.1 Ejecutar como administrador

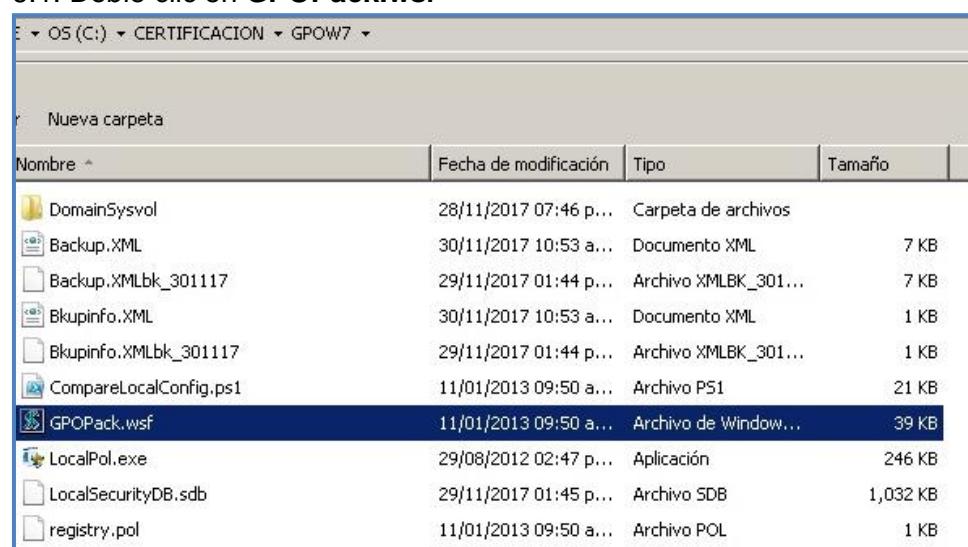


**Nota:** Todos los equipos deben tener instalado el antivirus AV, si no es así, se debe realizar el proceso de instalación.

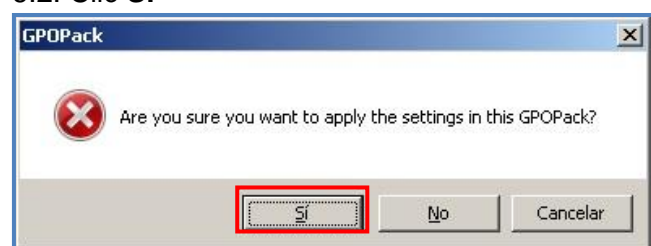
## 6. Ir a la carpeta GPOW7



### 6.1. Doble clic en GPOPack.wsf



### 6.2. Clic Si

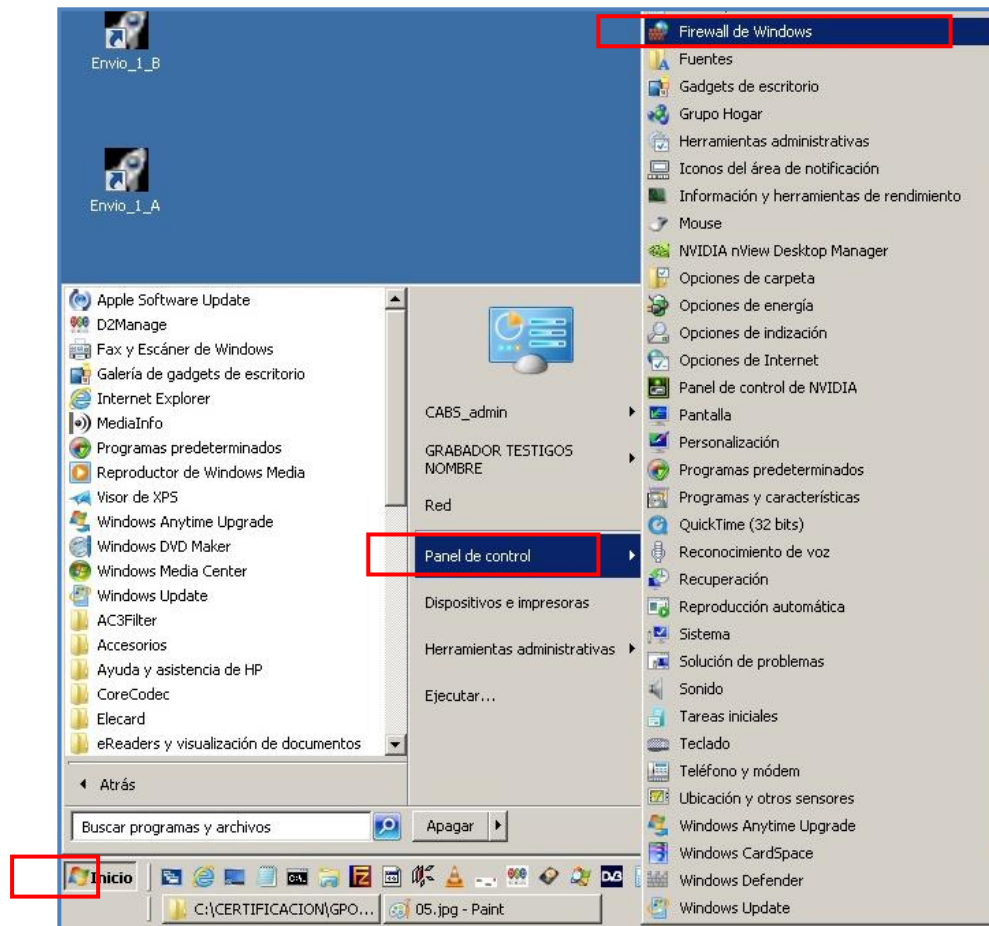


### 6.3. Clic Aceptar





## 7. Ir a Inicio → Panel de control → Firewall de Windows



### 7.1 Dar clic en Configuración Avanzada

Ventana principal del Panel de control

Permitir un programa o una característica a través de Firewall de Windows

- Cambiar la configuración de notificaciones
- Activar o desactivar Firewall de Windows
- Restaurar valores predeterminados
- Configuración avanzada

Solución de problemas de red

**Vea también**

- [Centro de actividades](#)
- [Centro de redes y recursos compartidos](#)

Firewall de Windows ayuda a impedir que hackers o software malintencionado obtengan acceso al equipo a través de Internet o de una red.

¿Cómo me ayuda un firewall a proteger mi equipo?

¿Qué son las ubicaciones de red?

	<b>Redes domésticas o de trabajo (privadas)</b>	<b>Conectado</b>
Redes domésticas o del trabajo en cuyos usuarios y dispositivos confíe		
Estado de Firewall de Windows:	Activado	
Conexiones entrantes:	Bloquear todas las conexiones a los programas que no estén en la lista de programas permitidos	
Redes domésticas o del trabajo (privadas) activas:	Red 2	
Estado de notificación:	Notificarme cuando Firewall de Windows bloquee un nuevo programa	

	<b>Redes públicas</b>	<b>Conectado</b>
Redes en lugares públicos como aeropuertos o cafeterías		
Estado de Firewall de Windows:	Activado	
Conexiones entrantes:	Bloquear todas las conexiones a los programas que no estén en la lista de programas permitidos	
Redes públicas activas:	Red no identificada	
Estado de notificación:	Notificarme cuando Firewall de Windows bloquee un nuevo programa	

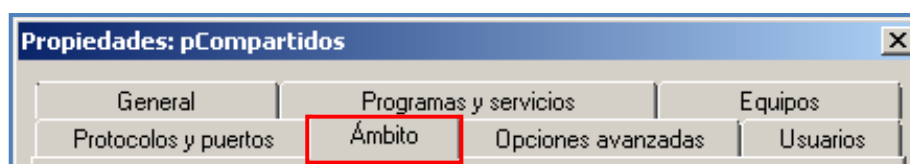
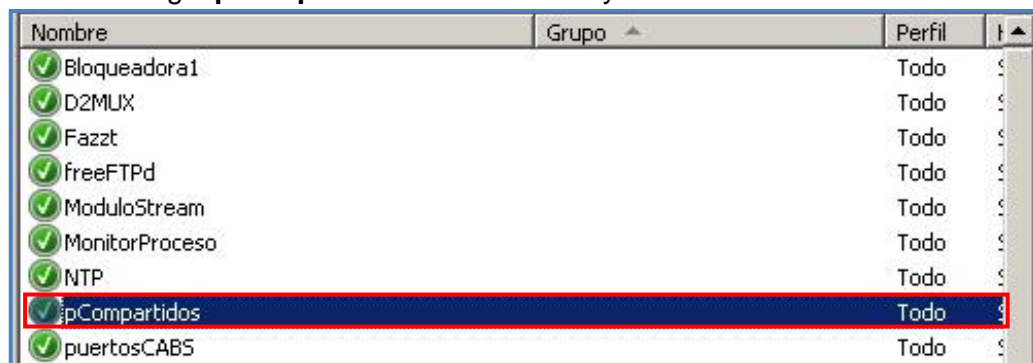


## 7.2 Clic en **Reglas de entrada**.

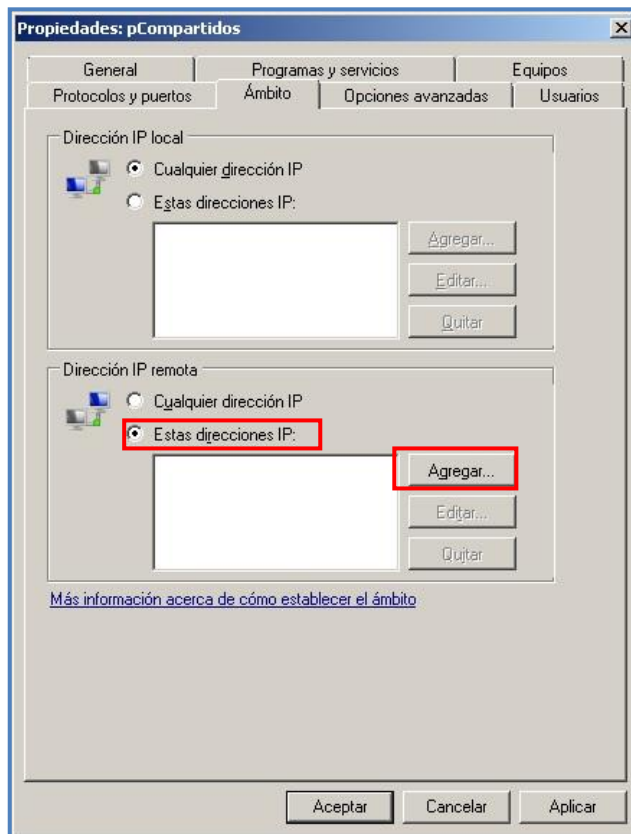
Verificar que las reglas de entrada: **VNC5800**, **VNC5900**, **VNCviewer.exe**, **winvnc.exe** se encuentren activas y publicas.



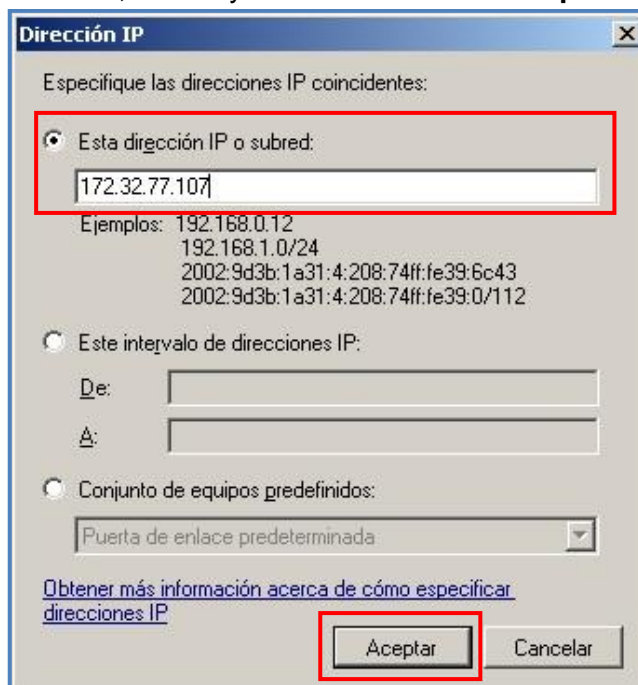
## 7.3 En la regla **pCompartidos** dar doble clic y en el menú seleccionar **Ámbito**



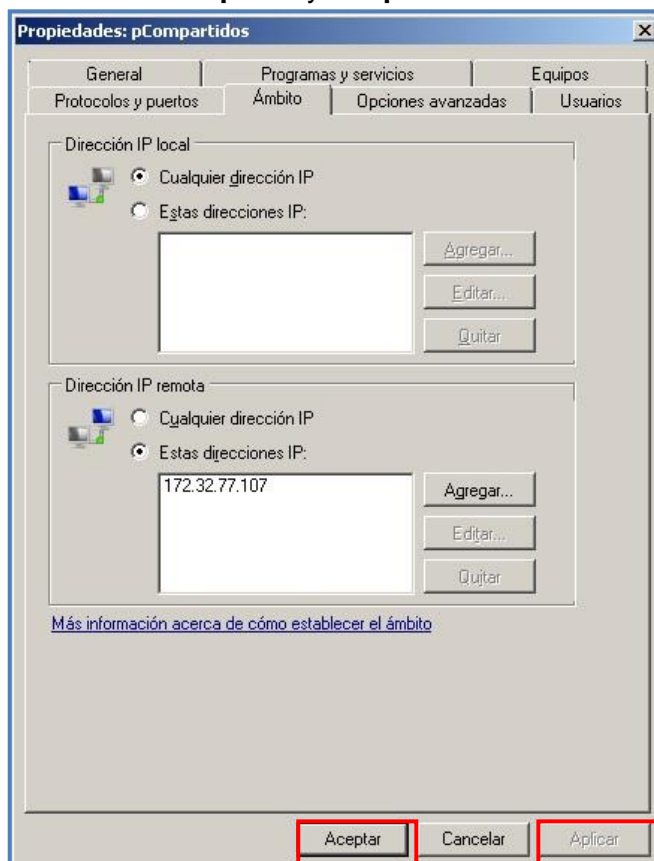
7.4 En **Dirección IP remota** , dar check en **Estas direcciones IP** y dar clic en **Agregar**



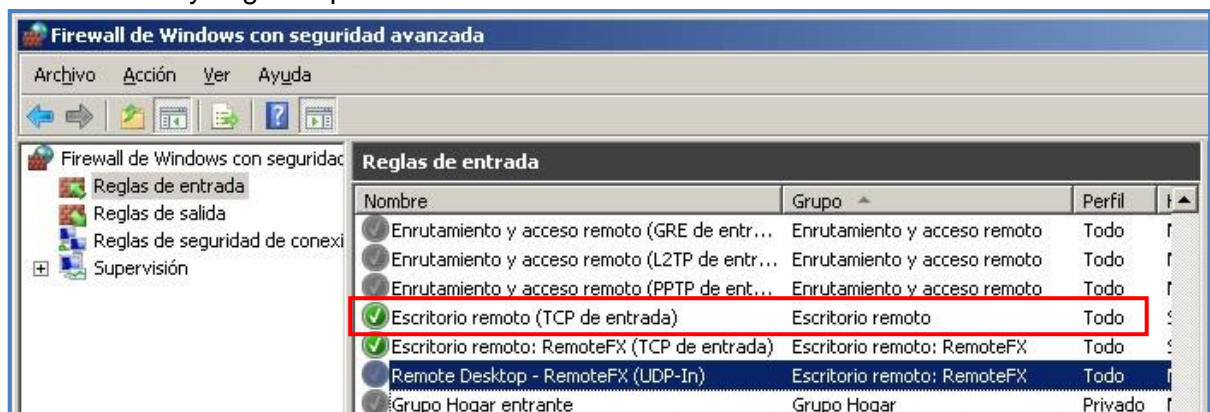
7.5 Se deben agregar las direcciones IP de todas las redes restantes, de la red que se está configurando. Es decir, si se configura la Red1, se deben agregar las direcciones IP de Red7, Red40 y RedA+. Dar clic en **Aceptar**.



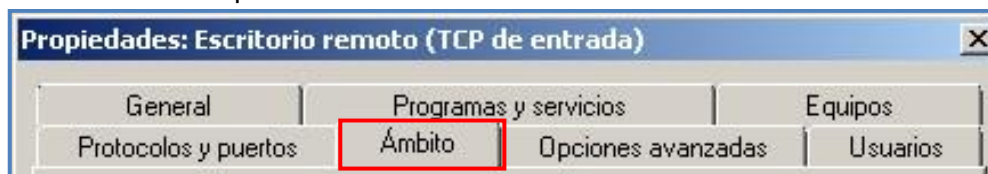
## 7.6 Dar clic en **Aplicar** y **Aceptar**



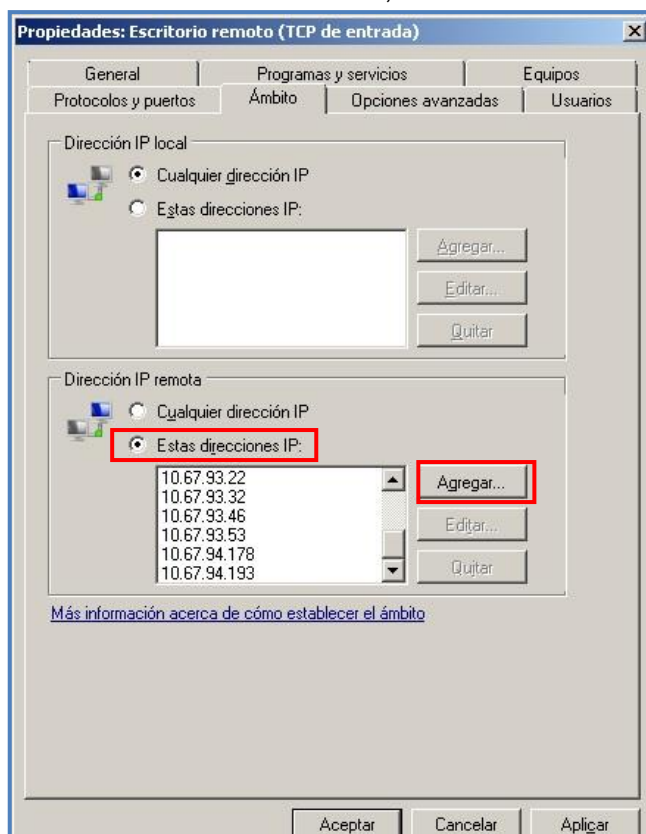
7.7 La regla **Escritorio remoto (TCP de entrada)** debe encontrarse activa si no es así, dar doble clic y seguir al paso 7.8



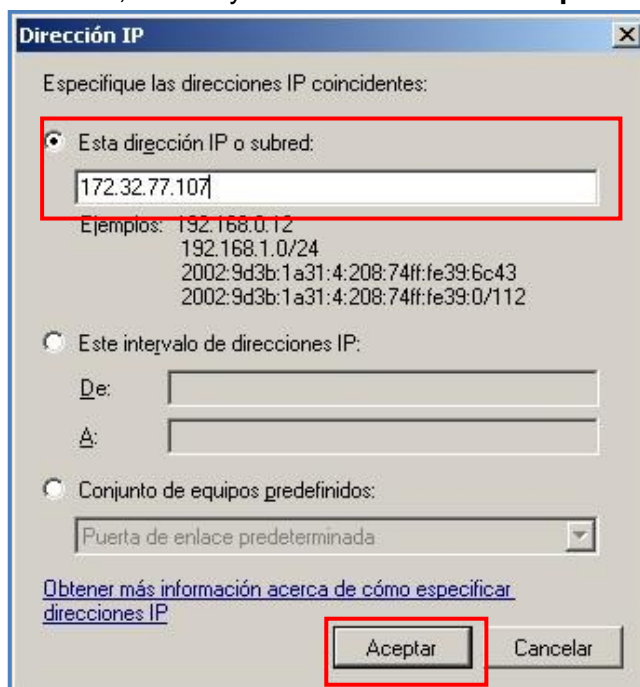
## 7.8 Dar clic en la pestaña **Ámbito**



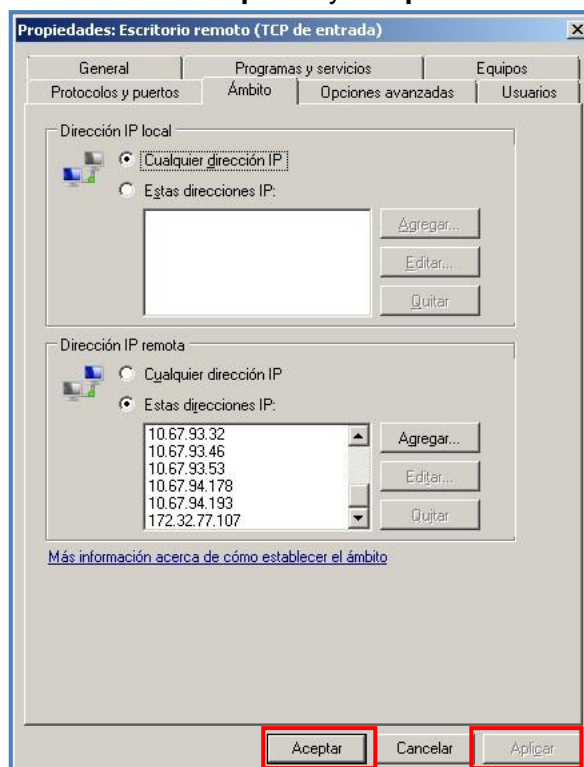
7.9 En **Dirección IP remota** , dar check en **Estas direcciones IP** y dar clic en **Agregar**




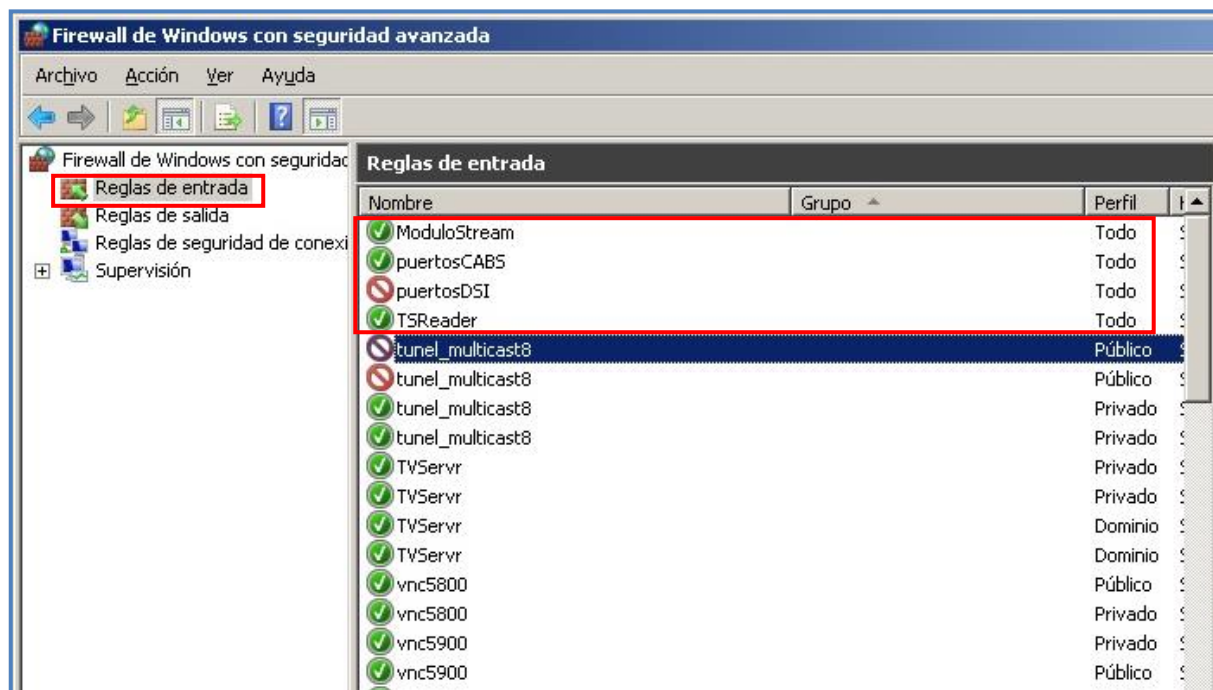
7.10 Se deben agregar las direcciones IP de todas las redes restantes, de la red que se está configurando. Es decir, si se configura la Red1, se deben agregar las direcciones IP de Red7, Red40 y RedA+. Dar clic en **Aceptar**.




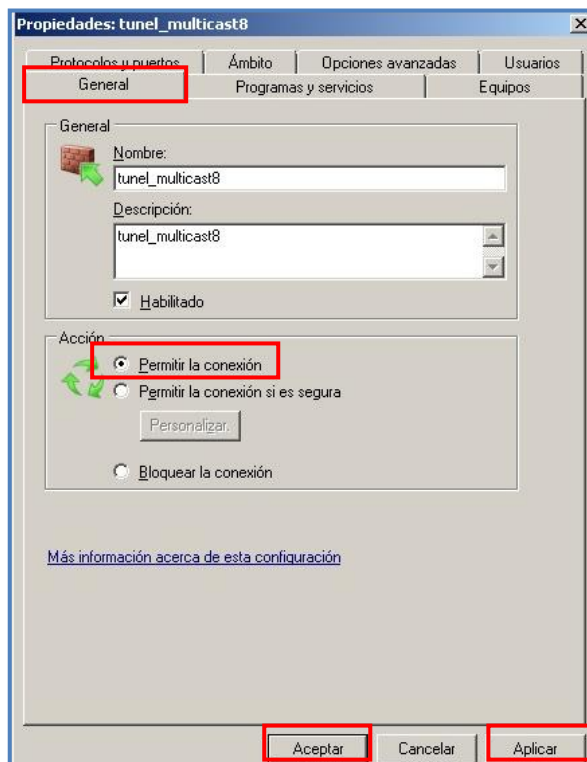
## 7.11 Dar clic en **Aplicar** y **Aceptar**



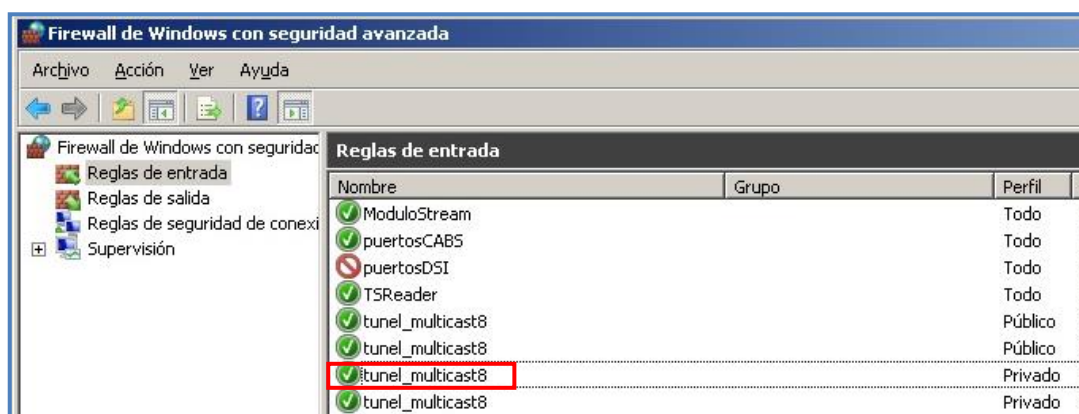
7.12 Las reglas **ModuloStream**, **puertosCABS** y **TSReader** deben aparecer en check verde. La regla **puertosDSI** deben aparecer con el símbolo  en rojo. Como se muestra a continuación:



**Nota:** En caso de que en las **Reglas de entrada** aparezca una aplicación de CABS con el símbolo  **tunel\_multicast8** en rojo, dar doble clic y en Propiedades → General. Y dar check en **Permitir la conexión**. Posteriormente clic en **Aplicar** y **Aceptar**.

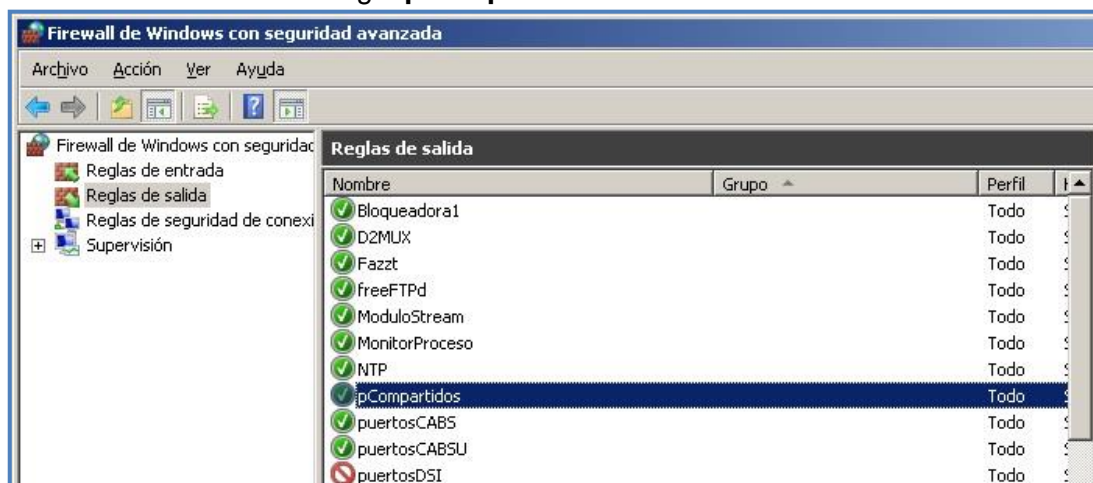


Después de realizar esa configuración debe de aparecer la aplicación en check verde.



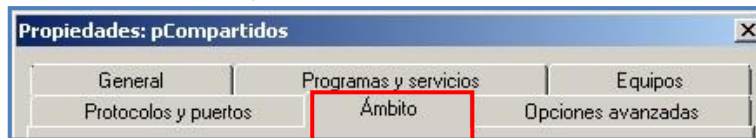
### 7.13 Clic en **Reglas de Salida**.

Dar doble clic en la regla **pCompartidos**

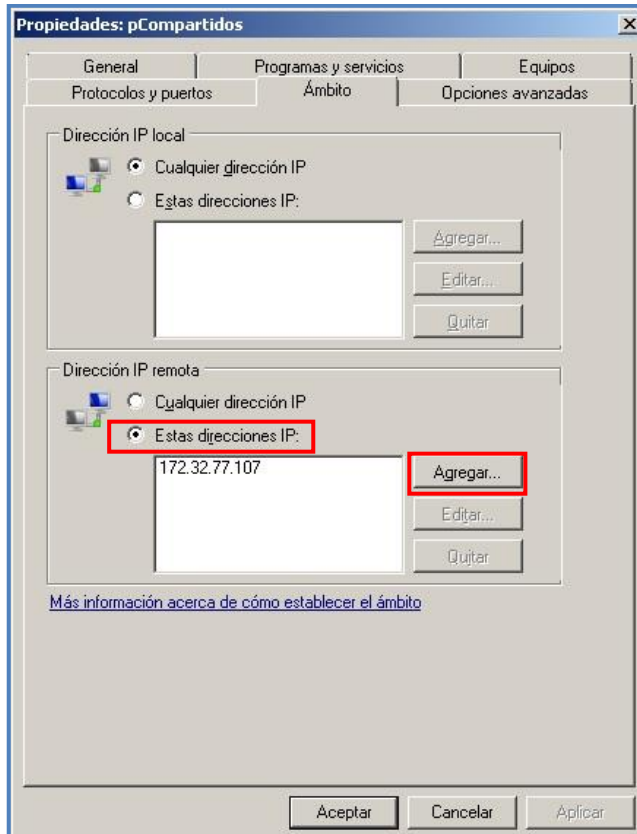




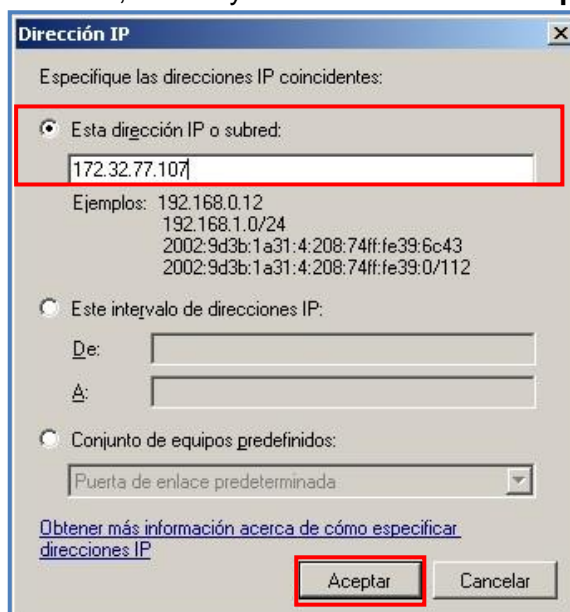
#### 7.14 Dar clic en la pestaña **Ámbito**



#### 7.15 En **Dirección IP remota** , dar check en **Estas direcciones IP** y dar clic en **Agregar**



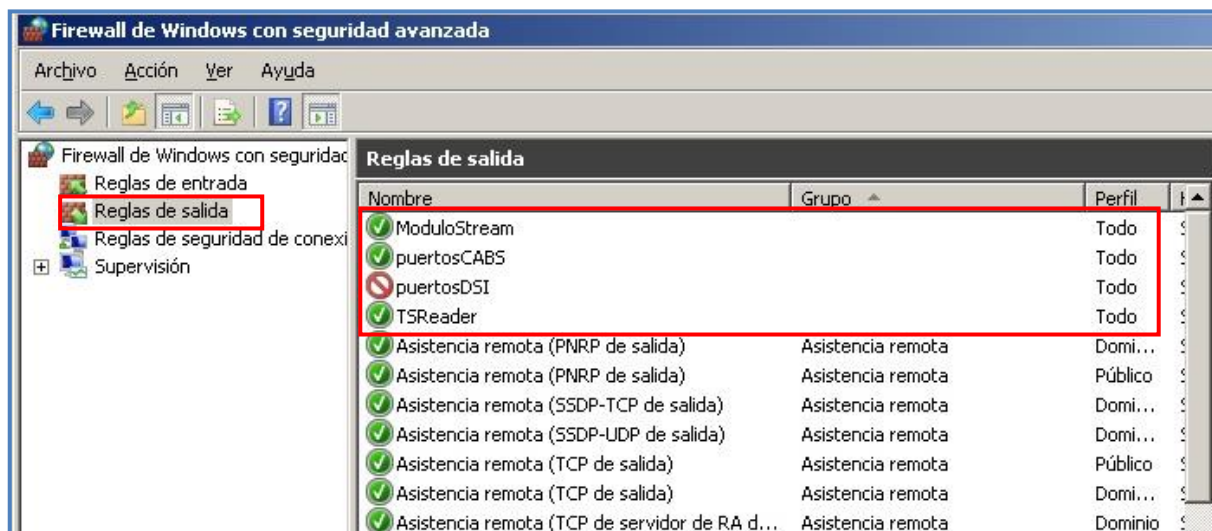
7.16 Se deben agregar las direcciones IP de todas las redes restantes, de la red que se está configurando. Es decir, si se configura la Red1, se deben agregar las direcciones IP de Red7, Red40 y RedA+. Dar clic en **Aceptar**.



### 7.17 Dar clic en **Aplicar** y **Aceptar**



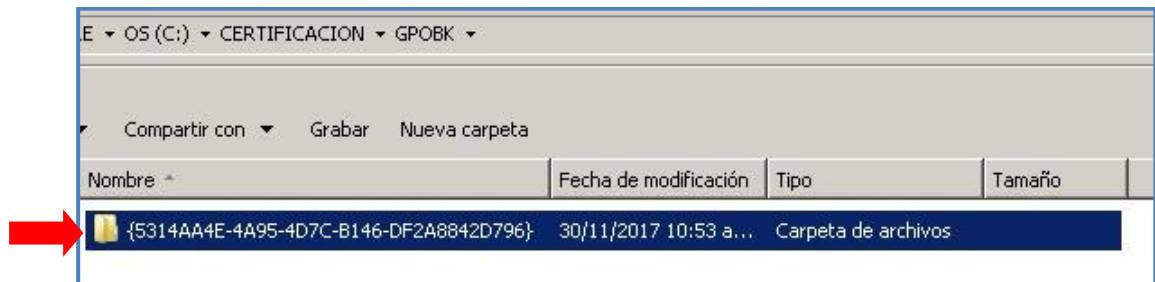
### 7.18 Las reglas de salida se deben encontrar de la misma manera que las reglas de entrada.



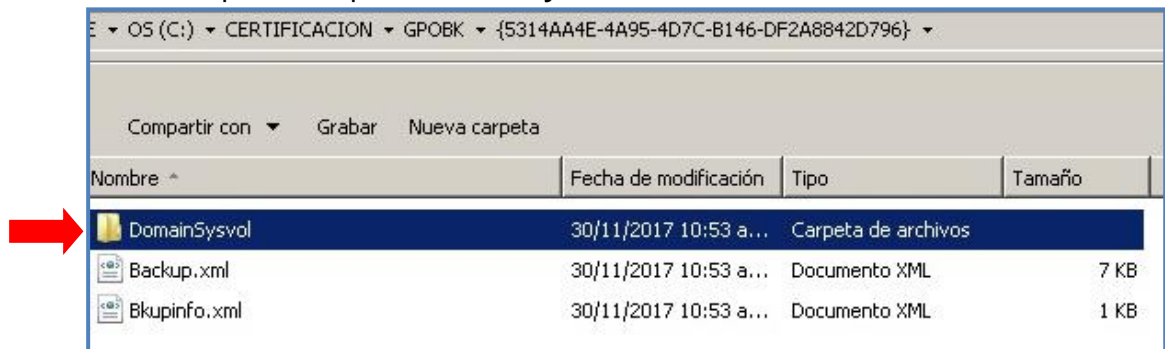
### 7.19 Reiniciar el equipo, en bloque de programa y posteriormente validar que se encuentre un icono azul y una palomita verde, que aparece en la barra de inicio.



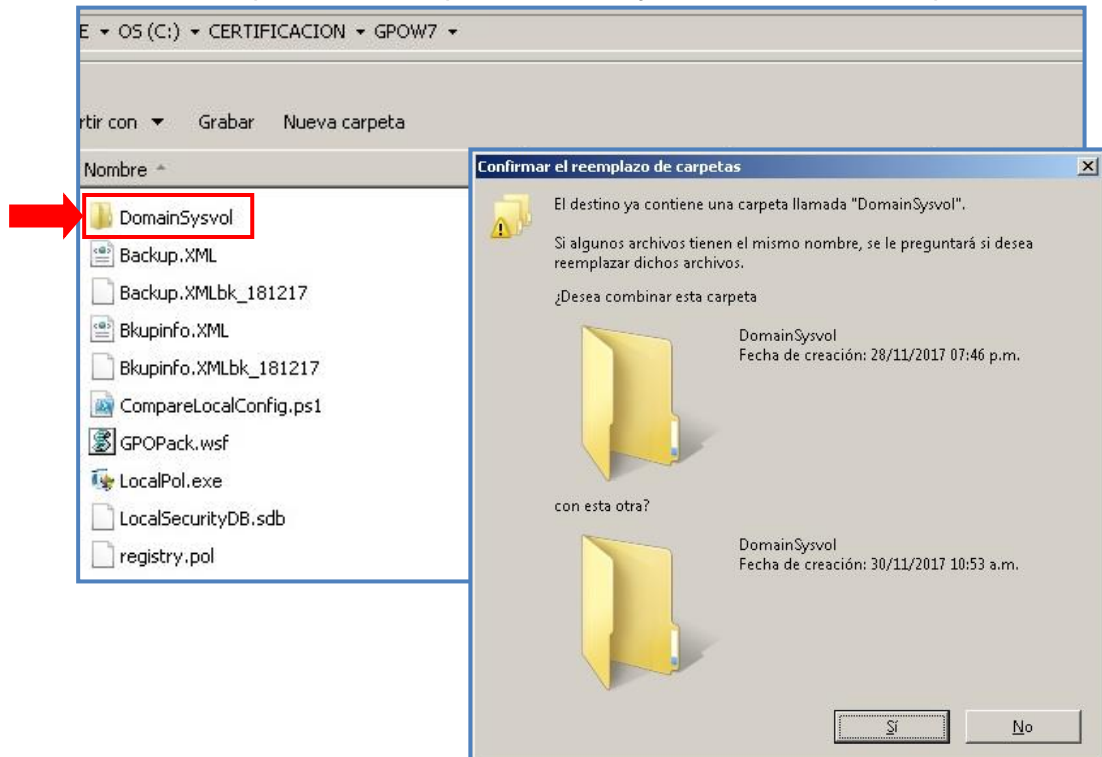
7.19.1. En caso de que no se haya tenido un **reinicio exitoso** del equipo (ej. que no hayan iniciado las aplicaciones automáticamente). Ir a la carpeta **GPOBK** e ingresar a la única carpeta que se encuentra dentro.



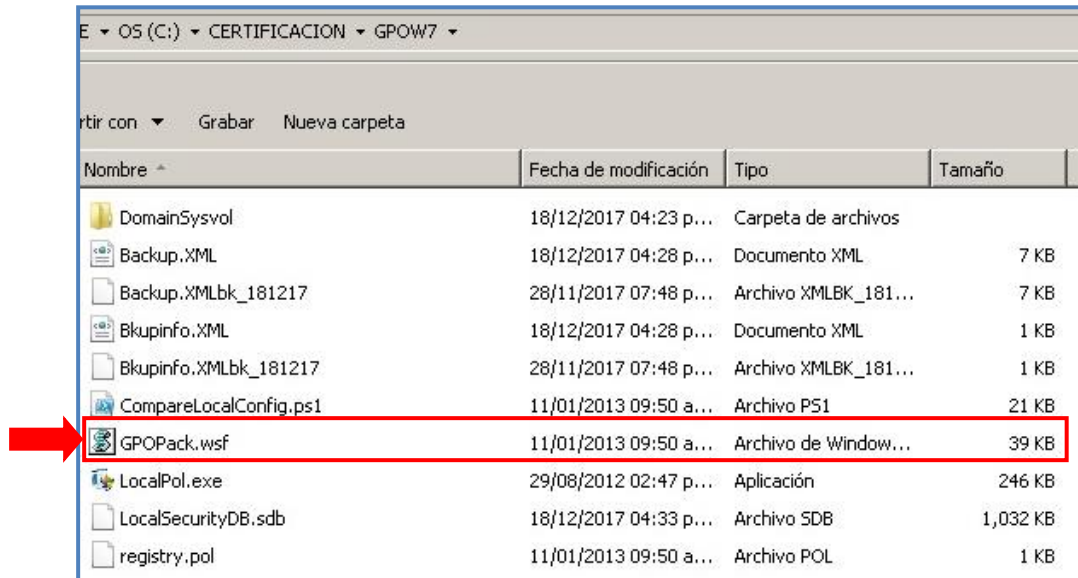
### 7.19.2. Copiar la carpeta **DomainSysvol**



### 7.19.3. Reemplazar esta carpeta **DomainSysvol** dentro de la carpeta **GPOW7**



#### 7.19.4. Dar doble clic en **GPOPack.wsf** y repetir los pasos **6.1**, **6.2** y **6.3**

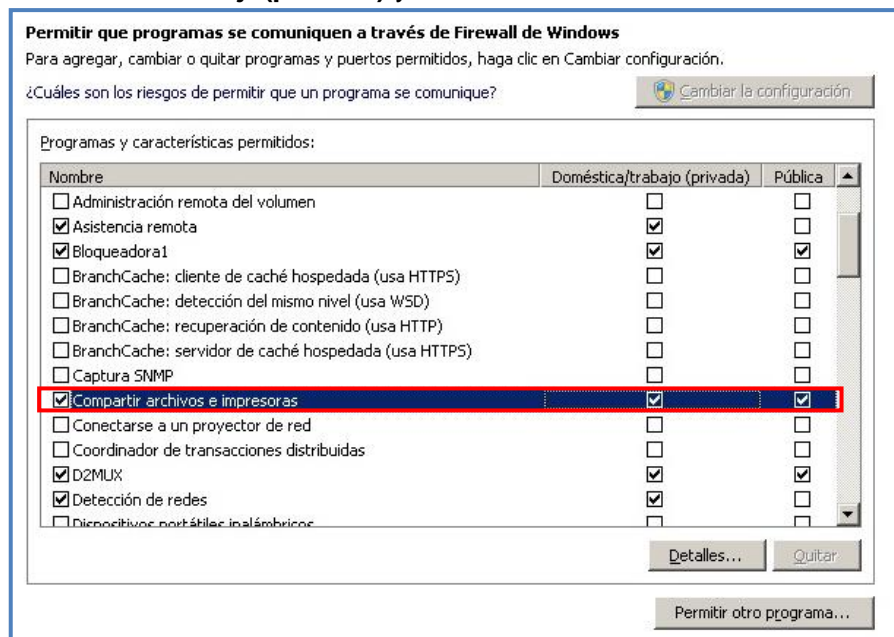


#### 7.19.5. **Se reinicia nuevamente** el equipo para que los cambios sean aplicados.

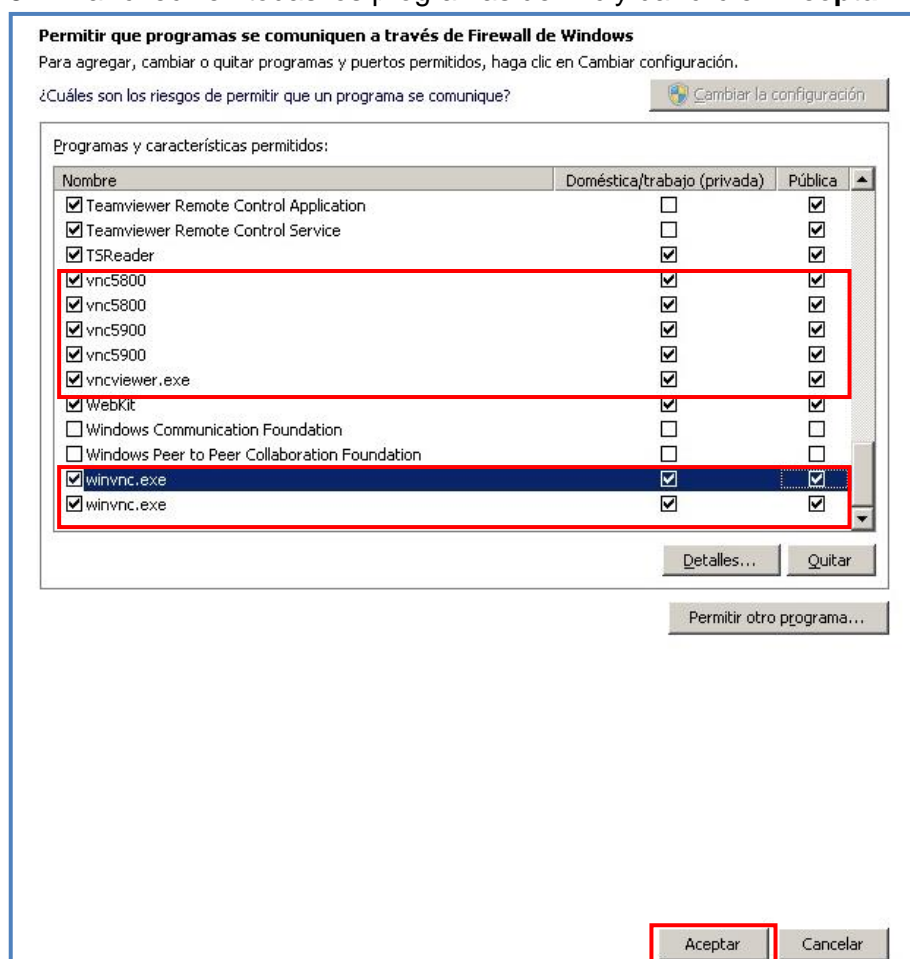
8. Dar clic en **Permitir un programa o una característica a través de Firewall de Windows.**



## 8.1 Dar check en **Compartir archivos e impresoras** y seleccionar el check de **Doméstica/trabajo(privada)** y **Pública**.

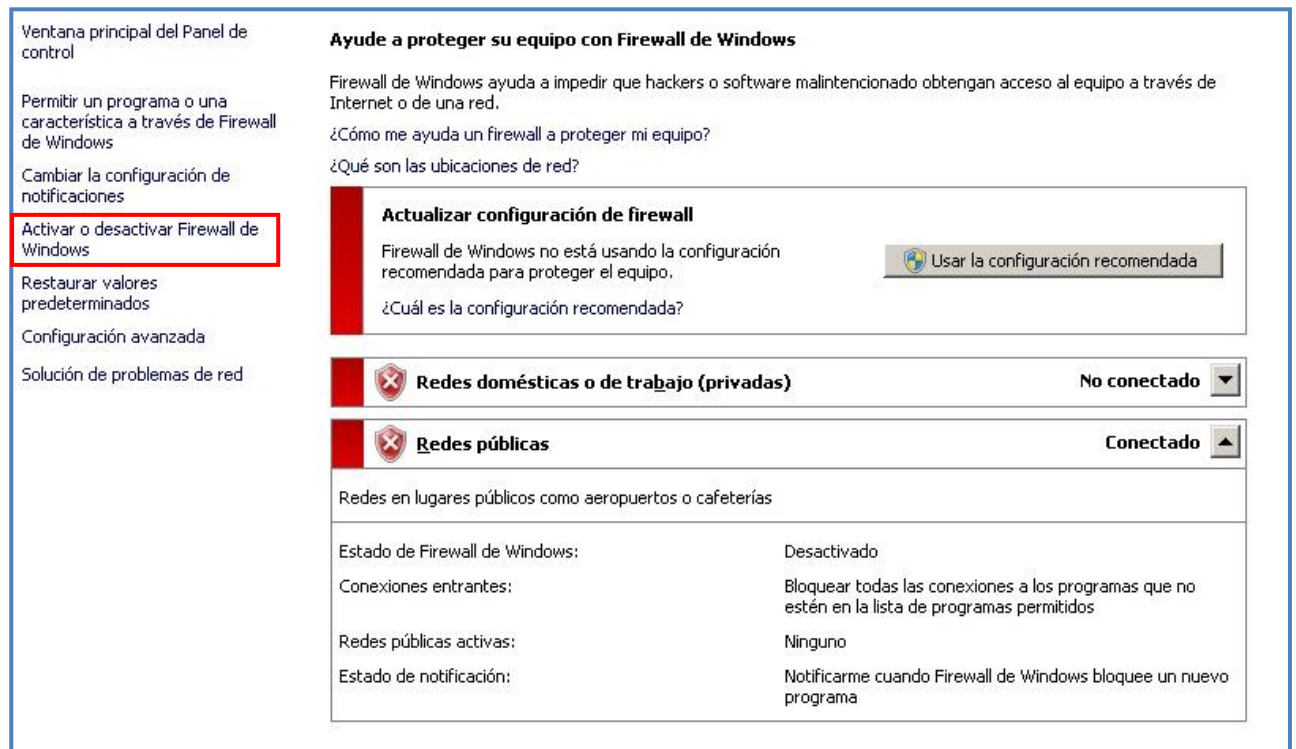


## 8.2 Dar check en todas los programas de vnc y dar clic en **Aceptar**.

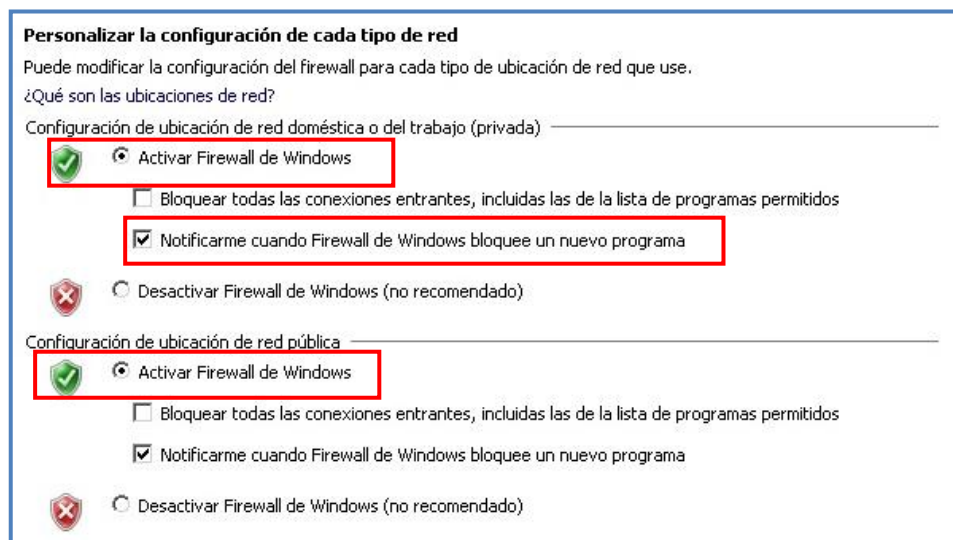




## 9. Clic en **Activar o desactivar Firewall de Windows**



9.2 En Configuración de ubicación de red doméstica o del trabajo (privada) dar check en **Activar Firewall de Windows** y dar check en **Notificarme cuando Firewall de Windows bloquee un nuevo programa**. En configuración de ubicación de red pública dar check en **Activar Firewall de Windows**. Después dar clic en **Aceptar**



9.3 Cerrar sesión del equipo e ingresar nuevamente.



## 10. Ejecutar la aplicación **Front-check-3p.exe**

AV	18/12/2017 04:23 p...	Carpeta de archivos	
bitacoras	18/12/2017 04:30 p...	Carpeta de archivos	
GPOBK	18/12/2017 04:28 p...	Carpeta de archivos	
GPOW7	18/12/2017 04:30 p...	Carpeta de archivos	
img	18/12/2017 04:23 p...	Carpeta de archivos	
REGBK	18/12/2017 04:28 p...	Carpeta de archivos	
certificacionDSI.exe	29/11/2017 08:33 p...	Aplicación	526 KB
Front_check_3p.exe	20/06/2017 06:24 p...	Aplicación	266 KB
GPOBKP.bat	01/12/2017 12:51 p...	Archivo por lotes de...	1 KB
LGPO.exe	20/01/2016 02:54 p...	Aplicación	372 KB
md5.exe	15/01/2008 11:19 a...	Aplicación	48 KB
servicios-puertos-DSI.bat	08/12/2017 07:19 p...	Archivo por lotes de...	2 KB

### 10.1. Esperar

```
C:\CERTIFICACION\Front_check_3p.exe
Creando carpeta resultados...
Este script requiere permisos administrador...
Ejecutando Script...
Este proceso puede demorar algunos minutos...
```

### 10.2. Una vez que haya concluido, mostrara la siguiente pantalla:

Checklist de seguridad equipos Windows - Salida Script de certificacion - Internet Explorer

C:\CERTIFICACION\Resultados\CSA\_30\_11\_2017\_BV3 Pendientes.html

Checklist de seguridad equip...

Archivo Edición Ver Favoritos Herramientas Ayuda

Sitios sugeridos Opinión: "Votar por M..."

### Checklist de Seguridad 2016 Ver 3.5 - Equipos Windows

Equipo: BV3  
Ip: 10.74.240.49 Interface: Tarjeta LAN inalámbrica 802.11 USB  
Dominio: BV3  
Usuario: CABS\_admin  
Arquitectura: 64 bits  
Sistema operativo: Microsoft Windows 7 Professional  
Version: 6.1.7601  
Service Pack: 1  
Fecha y hora de ejecucion: 30/11/2017 11:01:13 a.m.

La ejecucion de las remediaciones de seguridad son responsabilidad de la persona que ejecuta este programa, la ejecucion del script para ENUMERACION de puntos pendientes del checklist no afecta la operacion del servidor sin embargo los puntos de REMEDIACION mismos que se indican que se configuren y se proporciona este medio para agilizar y facilitar la configuracion es responsabilidad de la persona que configura los equipos o que ejecutan los scripts para configuracion automatica (no enumeracion)  
Los scripts para remediacion solo funcionan con Internet Explorer debido a la integracion con el sistema operativo.

#### Resultado del escaneo

❌	Pendiente	Id 1366 Para usuarios personalizados obliga el cambio de contraseña al menos cada 90 días
✅	Cumple	Id 1368 Las cuentas de usuario de default, genéricas y de pruebas han sido eliminadas o deshabilitadas.
✅	Cumple	Id 1369 Las contraseñas son de 15 caracteres mínimo, alfanuméricos y no son iguales al usuario.

10.3. Dentro de la carpeta **CERTIFICACION** se creara una carpeta nombrada "Resultados" misma que se debe enviar al Ing. Vladimir con la IP del equipo que se certifico, así como el **usuario** y **password** que se obtuvieron al inicio de la instalación, para que sea proporcionada al equipo de DSI.



bitacoras	30/11/2017 10:55 a...	Carpeta de archivos	
GPOBK	30/11/2017 10:53 a...	Carpeta de archivos	
GPOW7	30/11/2017 10:57 a...	Carpeta de archivos	
img	30/11/2017 10:51 a...	Carpeta de archivos	
<b>Resultados</b>	<b>30/11/2017 11:02 a...</b>	<b>Carpeta de archivos</b>	
certificacionDSI.exe	29/11/2017 08:33 p...	Aplicación	526 KB
certificacionDSI.exebk	28/11/2017 07:33 p...	Archivo EXEBK	521 KB
desactivar-servicios-DSI.bat	06/11/2017 06:10 p...	Archivo por lotes de...	1 KB
Front_check_3p.exe	20/06/2017 06:24 p...	Aplicación	266 KB
GPOBKP.bat	28/11/2017 07:26 p...	Archivo por lotes de...	1 KB
LGPO.exe	20/01/2016 02:54 p...	Aplicación	372 KB
md5.exe	15/01/2008 11:19 a...	Aplicación	48 KB
Resultados.zip	30/11/2017 11:03 a...	WinRAR ZIP archive	66 KB

11. Una vez concluido este proceso se debe continuar con la **Instalación de Servidor SFTP**.