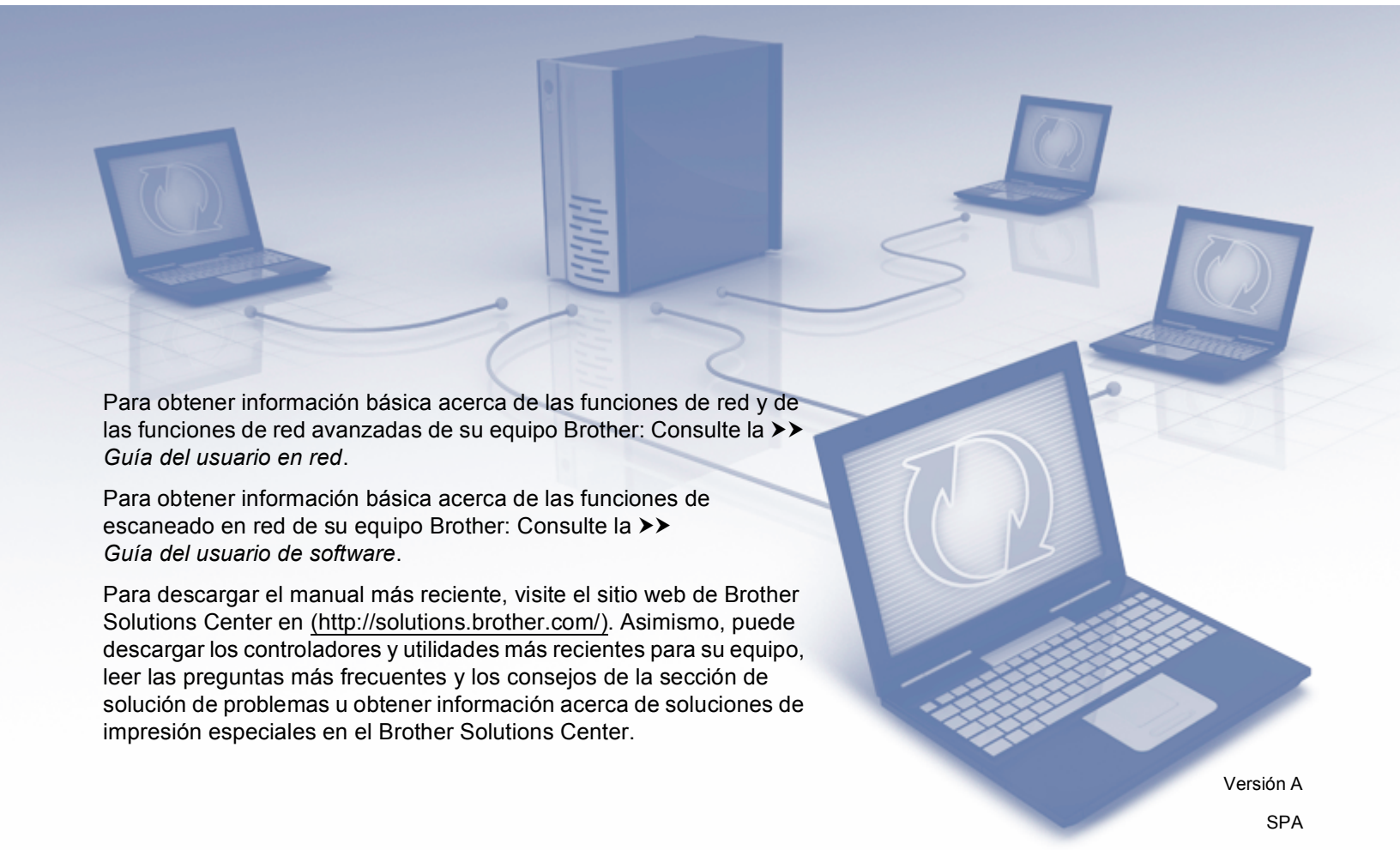
Guía para escanear a red (Windows®)



Para obtener información básica acerca de las funciones de red y de las funciones de red avanzadas de su equipo Brother: Consulte la ➤➤ *Guía del usuario en red*.

Para obtener información básica acerca de las funciones de escaneado en red de su equipo Brother: Consulte la ➤➤ *Guía del usuario de software*.

Para descargar el manual más reciente, visite el sitio web de Brother Solutions Center en (http://solutions.brother.com/). Asimismo, puede descargar los controladores y utilidades más recientes para su equipo, leer las preguntas más frecuentes y los consejos de la sección de solución de problemas u obtener información acerca de soluciones de impresión especiales en el Brother Solutions Center.

Versión A

SPA

Modelos a los que se puede aplicar

Esta Guía del usuario se aplica a los siguientes modelos.

Modelos de pantalla LCD de 5 líneas:
DCP-8110DN/8150DN/8155DN/MFC-8510DN/8520DN/8710DW/8810DW/8910DW

Modelos de pantalla táctil: DCP-8250DN/MFC-8950DW(T)

Definiciones de las notas

A lo largo de esta Guía del usuario se utilizan los siguientes iconos:

Nota	Las notas le indican cómo responder a una situación que surja o le proporcionan sugerencias sobre el funcionamiento con otras características.

Marcas comerciales

El logotipo de Brother es una marca registrada de Brother Industries, Ltd.

Microsoft, Windows, Windows Server e Internet Explorer son marcas registradas o marcas comerciales de Microsoft Corporation en Estados Unidos y/o en otros países.

Las empresas cuyos programas de software se mencionan en este manual tienen un acuerdo de licencia de software específico de los programas de los que son propietarios.

Todos los nombres comerciales y nombres de productos de empresas que aparecen en productos Brother, documentos asociados y cualquier otro material son marcas comerciales o marcas comerciales registradas de estas respectivas empresas.

NOTA IMPORTANTE

- Visite el Brother Solutions Center en http://solutions.brother.com/ y haga clic en Manuales en su página de modelos para descargar los otros manuales.
- No todos los modelos están disponibles en todos los países.

Tabla de contenido

1 Introducción 1

Visión general 1
Ventajas para el cliente 1

2 Configuración de Escanear a red con un navegador web 2

Introducción del nombre de archivo de Escanear a red 2
Configuración de ajustes predeterminados de Escanear a red 4
Sincronización con el servidor SNTP 6

3 Funcionamiento del equipo 8

Escanear a red mediante Perfiles de Escaneado a red para modelos de pantalla LCD de 5 líneas 8
Ajuste de un nuevo valor predeterminado para el tamaño de archivo 10
Uso de Escanear a red con perfiles de Escanear a red para DCP-8250DN y MFC-8950DW(T) 11
Introducción de texto 13
Introducción de texto en modelos con pantalla LCD de 5 líneas 13
Introducción de texto en DCP-8250DN y MFC-8950DW(T) 14

4 Certificado digital para PDF firmado 15

Configuración del certificado para PDF firmado 15
Certificados admitidos 16
Instalación del certificado digital 17
Creación de un certificado autofirmado 18
Creación de una solicitud de firma de certificado (Certificate Signing Request, CSR) 19
Instalación del certificado en el equipo 21
Importación y exportación del certificado y la clave privada 22
Importación del certificado autofirmado, el certificado emitido por una CA y la clave privada 22
Exportación del certificado autofirmado, el certificado emitido por una CA y la clave privada 22
Importación y exportación de un certificado de CA 23

5 Solución de problemas 24

Visión general 24
Identificación del problema 24
Terminología de red y formato de archivo PDF 26
Terminología de red 26
Formato de archivo PDF 26

1 Introducción

Visión general

Al seleccionar Escanear a red, puede escanear documentos directamente a una carpeta compartida de un servidor CIFS situado en una red local o en Internet. La función Escanear a red admite la autenticación Kerberos y NTLMv2.

La información detallada necesaria para utilizar Escanear a red se puede introducir mediante Administración basada en Web para configurar previamente los detalles y almacenarlos en un perfil de Escanear a red. Un perfil Escanear a red almacena la información del usuario y la configuración para su uso en una red o en Internet.

Ventajas para el cliente

- Puede escanear el documento directamente a un servidor CIFS.
- Puede configurar hasta 10 perfiles para la función Escanear a red. Una vez que haya configurado los perfiles de la función Escanear a red mediante Administración basada en Web, podrá utilizar la función Escanear a red desde el panel de control del equipo sin utilizar el ordenador.
- Escanear a red admite la autenticación Kerberos y la autenticación NTLMv2 para la comunicación segura.

2 Configuración de Escanear a red con un navegador web

Al seleccionar Escanear a red, puede escanear documentos directamente a una carpeta compartida de un servidor CIFS situado en una red local o en Internet. La función Escanear a red admite la autenticación Kerberos y NTLMv2.

La información detallada necesaria para utilizar Escanear a red se puede introducir mediante Administración basada en Web para configurar previamente los detalles y almacenarlos en un perfil de Escanear a red. Un perfil Escanear a red almacena la información del usuario y la configuración para su uso en una red o en Internet.

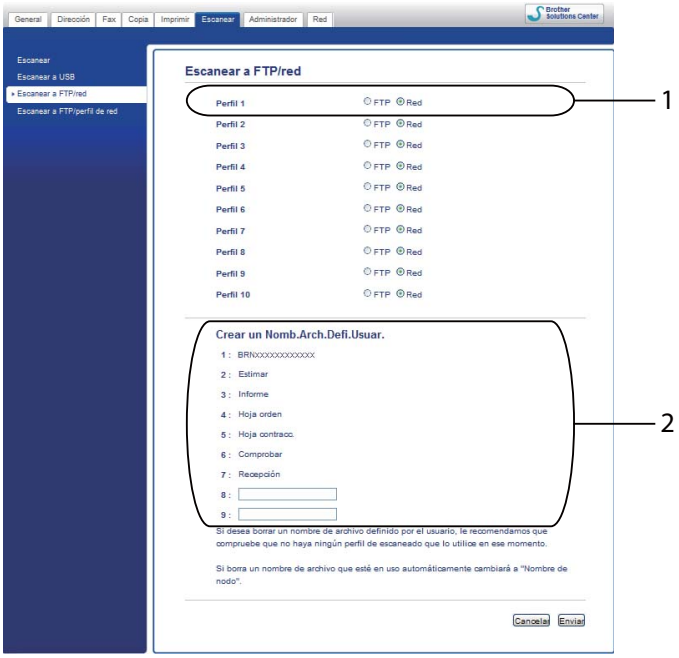
Nota

- Es necesario configurar el protocolo SNTP (servidor de hora de red), o bien, deberá ajustar correctamente la fecha, la hora y la zona horaria para la autenticación. Para obtener más información, consulte *Sincronización con el servidor SNTP* ➤➤ página 6.
- Se recomienda utilizar Windows® Internet Explorer® 7.0/8.0 o Firefox® 3.6 para Windows® y Safari 4.0/5.0 para Macintosh. Asegúrese de que JavaScript y las cookies siempre están activados en el navegador que utilice. Si utiliza un navegador web diferente, asegúrese de que sea compatible con HTTP 1.0 y HTTP 1.1.

Introducción del nombre de archivo de Escanear a red

1. Inicie su navegador web.
2. Introduzca “http://dirección IP del equipo/” en la barra de direcciones de su navegador (donde “dirección IP del equipo” es la dirección IP del equipo o el nombre del servidor de impresión).
   - Por ejemplo: http://192.168.1.2/
3. No se necesita una contraseña de manera predeterminada. Si ha establecido anteriormente una contraseña, introdúzcala y pulse  .
4. Haga clic en **Escanear**.
5. Haga clic en **Escanear a FTP/red**.

6 Seleccione **Red** (1) en los números de perfil (del 1 al 10) que desee utilizar para los ajustes de Escanear a red.
También es posible almacenar dos nombres de archivo definidos por el usuario, que pueden utilizarse para crear un perfil de Escanear a red, además de los siete nombres de archivo predefinidos en **Crear un Nomb.Arch.Defi.Usuar.** (2). Es posible introducir un máximo de 15 caracteres en cada uno de los dos campos.



Nota

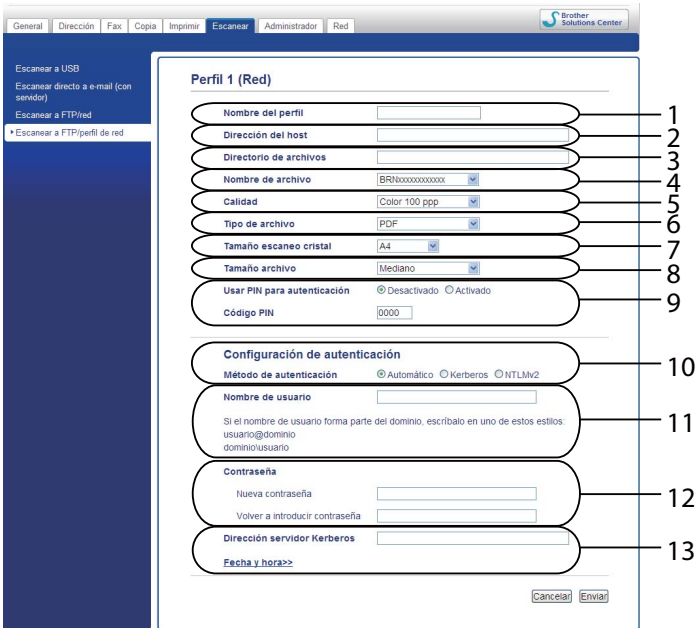
El uso de determinados caracteres o símbolos en el nombre de un archivo puede causar problemas a la hora de acceder al archivo. Es recomendable que utilice únicamente combinaciones de los siguientes caracteres en un nombre de archivo:

1234567890
ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
! # $ % & ‘ ( ) - , @ ^ _ ’ { } ~

7 Haga clic en **Enviar**.

Configuración de ajustes predeterminados de Escanear a red

1. Inicie su navegador web.
2. Introduzca “http://dirección IP del equipo/” en la barra de direcciones de su navegador (donde “dirección IP del equipo” es la dirección IP del equipo o el nombre del servidor de impresión).
   - Por ejemplo: http://192.168.1.2/
3. No se necesita una contraseña de manera predeterminada. Si ha establecido anteriormente una contraseña, introdúzcala y pulse .
4. Haga clic en **Escanear**.
5. Haga clic en **Escanear a FTP/perfil de red**.
6. Elija el Perfil que desea configurar en **Escanear a FTP/perfil de red**.
   Puede configurar y modificar los siguientes ajustes de la función Escanear a red mediante un navegador web.



1 Introduzca el nombre que desea utilizar para el perfil de escaneado a red. Este nombre aparecerá en la pantalla LCD del equipo y puede tener un máximo de 15 caracteres.

2 La **Dirección del host** es el nombre del dominio del servidor CIFS. Introduzca la **Dirección del host** (por ejemplo, mipc.ejemplo.com) (hasta 64 caracteres) o la dirección IP (por ejemplo, 192.23.56.189).

3 Especifique la carpeta de destino donde se guardará el documento en el servidor CIFS (por ejemplo, brother\abc) (hasta 60 caracteres).

4 Escriba el nombre de archivo que desea utilizar para el documento escaneado. Puede seleccionar siete nombres de archivo predeterminados y dos nombres de archivo definidos por el usuario. El nombre de archivo que se utilizará para el documento será el nombre de archivo seleccionado, más los últimos 6 dígitos del contador de escáner de superficie plana o del alimentador automático de documentos, más la extensión del archivo (por ejemplo, Estimate_098765.pdf). También puede introducir manualmente un nombre de archivo de hasta 15 caracteres.

5 Seleccione la calidad de escaneado en la lista desplegable. Puede elegir **Color 100 ppp**, **Color 200 ppp**, **Color 300 ppp**, **Color 600 ppp**, **Color automático**, **Gris 100 ppp**, **Gris 200 ppp**, **Gris 300 ppp**, **Gris automático**, **ByN 300 ppp**, **ByN 200 ppp**, **ByN 200 x 100 ppp** o **Selección de usuario**.

6 Elija el tipo de archivo para el documento en la lista desplegable. Puede elegir **PDF**, **PDF/A**, **PDF seguro**, **PDF firmado**, **JPEG**, **XPS** o **Selección de usuario** para documentos en color o en escala de grises y **PDF**, **PDF/A**, **PDF seguro**, **PDF firmado**, **TIFF** o **Selección de usuario** para documentos en blanco y negro.

7 (Para modelos de pantalla táctil) Si utiliza el cristal de escaneado, seleccione **A4**, **Carta** o **Legal/Folio** para **Tamaño escaneo cristal**.

8 Si elige color o gris en la calidad del escaneado, elija el tamaño de archivo para el documento desde la lista desplegable. Puede elegir **Grande**, **Mediano**, **Pequeño** o **Selección de usuario**.

9 Si desea proteger el perfil, marque la casilla **Usar PIN para autenticación** e introduzca un número PIN de 4 dígitos en **Código PIN**.

10 Seleccione el método de autenticación. Puede elegir **Automático**, **Kerberos** o **NTLMv2**. Si selecciona **Automático**, el método de autenticación se detectará automáticamente.

11 Introduzca el **Nombre de usuario** que haya registrado en el servidor CIFS para el equipo (hasta 96 caracteres).

12 Introduzca la **Contraseña** de acceso al servidor CIFS (hasta 32 caracteres).

13 Si desea establecer manualmente la **Dirección servidor Kerberos**, especifique la **Dirección servidor Kerberos** (por ejemplo, mipc.ejemplo.com) (hasta 64 caracteres).

Nota

- Si selecciona **Selección de usuario** en la calidad de escaneado, el tipo de archivo o el tamaño de archivo, deberá seleccionar dichos ajustes desde el panel de control del equipo.
- Si ha seleccionado **PDF seguro**, el equipo le pedirá que introduzca una contraseña de 4 dígitos mediante los números del 0 al 9 antes de iniciar el escaneado.
- Si elige **PDF firmado**, deberá instalar un certificado en su equipo mediante Administración basada en Web. Elija **PDF firmado** desde **Administrador** en Administración basada en Web. (Consulte *Certificado digital para PDF firmado* ➤➤ página 15).
- Para obtener información acerca de PDF/A, PDF seguro y PDF firmado, consulte *Formato de archivo PDF* ➤➤ página 26.

7 Una vez configurados los ajustes de Escanear a red, haga clic en **Enviar**.

Sincronización con el servidor SNTP

Es necesario configurar el protocolo SNTP (servidor de hora de red), o bien, deberá ajustar correctamente la fecha, la hora y la zona horaria en el panel de control para la autenticación Kerberos. La hora debe coincidir con la hora utilizada por el servidor Kerberos.

SNTP es el protocolo que se utiliza para sincronizar la hora utilizada por el equipo para la autenticación con el servidor de hora SNTP (esta hora no es la que se visualiza en la pantalla LCD del equipo). Es posible sincronizar la hora utilizada por el equipo de manera regular con el tiempo universal coordinado (UTC) ofrecido por el servidor de tiempo SNTP.

Nota

Esta función no se encuentra disponible en algunos países.

1. Inicie su navegador web.
2. Introduzca “http://dirección IP del equipo/” en la barra de direcciones de su navegador (donde “dirección IP del equipo” es la dirección IP del equipo o el nombre del servidor de impresión).
   - Por ejemplo: http://192.168.1.2/
3. No se necesita una contraseña de manera predeterminada. Si ha establecido anteriormente una contraseña, introdúzcala y pulse →.
4. Haga clic en **Red** y, a continuación, haga clic en **Protocolo**.
5. Marque la casilla de verificación **SNTP** para activar el ajuste.
6. Haga clic en **Configuración avanzada**.
   - **Estado**

     Permite visualizar si los ajustes del servidor SNTP están activados o desactivados.
   - **Método del servidor SNTP**

     Seleccione **AUTOMÁTICO** o **ESTÁTICO**.
     - **AUTOMÁTICO**

       Si dispone de un servidor DHCP en su red, el servidor SNTP obtendrá automáticamente la dirección de dicho servidor.
     - **ESTÁTICO**

       Introduzca la dirección que desee utilizar.
   - **Dirección del servidor SNTP primario**, **Dirección del servidor SNTP secundario**

     Introduzca la dirección del servidor (hasta 64 caracteres).

     La dirección del servidor SNTP secundario se utiliza como una copia de seguridad en la dirección del servidor SNTP principal. Si el servidor primario no está disponible, el equipo se pondrá en contacto con el servidor SNTP secundario. Si dispone de servidor SNTP primario pero no de un servidor SNTP secundario, simplemente deje este campo en blanco.

■ **Puerto del servidor SNTP primario**, **Puerto del servidor SNTP secundario**

Introduzca el número de puerto (entre 1 y 65535).

El puerto del servidor SNTP secundario se utiliza como una copia de seguridad en el puerto del servidor SNTP principal. Si el puerto primario no está disponible, el equipo se podrá en contacto con el puerto SNTP secundario. Si dispone de puerto SNTP primario pero no de un puerto SNTP secundario, simplemente deje este campo en blanco.

■ **Intervalo de sincronización**

Introduzca el número de horas entre los intentos de sincronización del servidor (de 1 a 168 horas).

Nota

- Es necesario configurar **Fecha y hora** para sincronizar la hora utilizada por el equipo con el servidor de hora. Haga clic en **Fecha y hora** y, a continuación, configure **Fecha y hora** en la pantalla **General**. También puede configurar la Fecha y hora desde el panel de control del equipo.

- Marque la casilla de verificación **Sincronizar con servidor SNTP**. También es necesario verificar la configuración de zona horaria correctamente. Seleccione la diferencia horaria entre su ubicación y UTC en la lista desplegable **Zona horaria**. Por ejemplo, la zona horaria oriental en EE.UU. y Canadá es UTC-05:00.

■ **Estado de la sincronización**

Puede confirmar el último estado de sincronización.

7 Haga clic en **Enviar** para aplicar los ajustes.

3 Funcionamiento del equipo

Una vez que haya configurado los ajustes de Escanear a red, ya puede utilizar la función Escanear a red.

Escanear a red mediante Perfiles de Escaneado a red para modelos de pantalla LCD de 5 líneas

1. Cargue el documento.
2. Pulse (**DIGITALIZAR (SCAN) (ESCÁNER)**).
3. Pulse ▲ o ▼ para seleccionar `Escanear a red`. Pulse **OK**.
   (Para DCP-8155DN, MFC-8520DN, MFC-8810DW y MFC-8910DW) Vaya al paso ❹.
   (Para DCP-8110DN, DCP-8150DN, MFC-8510DN y MFC-8710DW) Vaya al paso ❺.
4. Pulse ▲ o ▼ para seleccionar `1 cara`, `2caraBordeLarg` o `2caraBordeCort`.
   Pulse **OK**.
5. Pulse ▲ o ▼ para seleccionar uno de los perfiles que aparecen en la lista.
   Pulse **OK**.
6. Si marca la casilla **Usar PIN para autenticación** en **Escanear a FTP/perfil de red** de Administración basada en Web, en la pantalla LCD aparecerá un mensaje que le solicitará que introduzca un número PIN. Introduzca el número PIN de 4 dígitos y, a continuación, pulse **OK**.
   - Si se ha completado el perfil, irá automáticamente al paso ⓫.
   - Si se ha configurado **Selección de usuario** mediante Administración basada en Web, se le solicitará que seleccione en el panel de control la calidad del escaneado, el tipo de archivo y el tamaño de archivo.
   - Si no se ha completado el perfil, por ejemplo, no se ha seleccionado la calidad o tipo de archivo, se le pedirá que especifique cualquier información que falte en los pasos siguientes.
7. Seleccione una de las siguientes opciones:
   - Pulse ▲ o ▼ para seleccionar `Color 100 ppp`, `Color 200 ppp`, `Color 300 ppp`, `Color 600 ppp`, `Color automát.`, `Gris 100 ppp`, `Gris 200 ppp`, `Gris 300 ppp` o `Gris automático`. Pulse **OK** y vaya al paso ❽.
   - Pulse ▲ o ▼ para seleccionar `ByN 300 ppp`, `ByN 200 ppp` o `ByN 200x100 PPP`. Pulse **OK** y vaya al paso ❾.
8. Pulse ▲ o ▼ para seleccionar `PDF`, `PDF/A`, `PDF seguro`, `PDF firmado`, `JPEG` o `XPS`. Pulse **OK** y vaya al paso ❿.

9 Pulse ▲ o ▼ para seleccionar PDF, PDF/A, PDF seguro, PDF firmado o TIFF. Pulse **OK** y vaya al paso ⓫.

Nota

- Si ha seleccionado PDF seguro, el equipo le pedirá que introduzca una contraseña de 4 dígitos mediante los números del 0 al 9 antes de iniciar el escaneado.
- Si elige PDF firmado, deberá instalar y, a continuación, configurar un certificado en su equipo mediante Administración basada en Web.
- No es posible seleccionar el tamaño de archivo al escanear un documento en blanco y negro. Los documentos en blanco y negro se almacenarán en formato de archivo TIFF y los datos no se comprimirán.

10 Pulse ▲ o ▼ para seleccionar el tamaño de archivo.
Pulse **OK** y vaya al paso ⓫.

11 Efectúe una de las acciones siguientes:

- Para iniciar el escaneado, pulse **Iniciar (Start) (Inicio)**.
- Para cambiar el nombre de archivo, vaya al paso ⓬.

12 Pulse ▲ o ▼ para seleccionar el nombre de archivo que desee utilizar y, a continuación, pulse **OK**. Pulse **Iniciar (Start) (Inicio)**.

Nota

Para cambiar manualmente el nombre de archivo, vaya al paso ⓭.

13 Pulse ▲ o ▼ para seleccionar <Manual>. Pulse **OK**.
Introduzca el nombre de archivo que desee utilizar (hasta 64 caracteres) y pulse **OK**. (Para obtener información sobre cómo introducir texto, consulte *Introducción de texto en modelos con pantalla LCD de 5 líneas* ➤➤ página 13).
Pulse **Iniciar (Start) (Inicio)**.

Ajuste de un nuevo valor predeterminado para el tamaño de archivo

Puede configurar sus propios ajustes predeterminados para el tamaño de archivo. Si desea obtener un escaneado de calidad superior, elija un tamaño de archivo más grande. Si desea obtener un tamaño de archivo más pequeño, elija un tamaño de archivo más pequeño.

1. Pulse **Menu (Menú)**.
2. Pulse ▲ o ▼ para seleccionar `Config. gral.`. Pulse **OK**.
3. Pulse ▲ o ▼ para seleccionar `Escan. docume.`. Pulse **OK**.
4. Pulse ▲ o ▼ para seleccionar `Tamaño archivo`. Pulse **OK**.
5. Pulse ▲ o ▼ para seleccionar `Color` o `Gris`. Pulse **OK**.
6. Pulse ▲ o ▼ para seleccionar `Pequeño`, `Mediano` o `Grande`. Pulse **OK**.
7. Pulse **Parar (Stop/Exit) (Detener/Salir)**.

Nota

No es posible seleccionar el tamaño de archivo al escanear un documento en blanco y negro. Los documentos en blanco y negro se almacenarán en formato de archivo TIFF y los datos no se comprimirán.

Uso de Escanear a red con perfiles de Escanear a red para DCP-8250DN y MFC-8950DW(T)

1. Cargue el documento.
2. Pulse `Escanear`.
3. Pulse `Escanear a red`.
4. Pulse ▲ o ▼ para seleccionar uno de los perfiles que aparecen en la lista.
5. Si marca la casilla **Usar PIN para autenticación** en **Escanear a FTP/perfil de red** de Administración basada en Web, en la pantalla LCD aparecerá un mensaje que le solicitará que introduzca un número PIN. Introduzca el número PIN de 4 dígitos y, a continuación, pulse `OK`.
   - Si se ha completado el perfil, irá automáticamente al paso ⓫.
   - Si se ha configurado **Selección de usuario** mediante Administración basada en Web, se le solicitará que seleccione en el panel de control la calidad del escaneado, el tipo de archivo y el tamaño de archivo.
   - Si no se ha completado el perfil, por ejemplo, no se ha seleccionado la calidad o tipo de archivo, se le pedirá que especifique cualquier información que falte en los pasos siguientes.
6. Pulse `Calidad` y, a continuación, elija una de las opciones siguientes:
   - Pulse ◀ o ▶ para seleccionar `Color 100 ppp`, `Color 200 ppp`, `Color 300 ppp`, `Color 600 ppp`, `Color automát.`, `Gris 100 ppp`, `Gris 200 ppp`, `Gris 300 ppp` o `Gris automático`. Vaya al paso ❼.
   - Pulse ◀ o ▶ para seleccionar `ByN 300 ppp`, `ByN 200 ppp` o `ByN 200x100 ppp`. Vaya al paso ❽.
7. Pulse `Tipo archivo` y, a continuación, seleccione `PDF`, `PDF/A`, `PDF seguro`, `PDF firmado`, `JPEG` o `XPS`.
   Vaya al paso ❾.
8. Pulse `Tipo archivo` y, a continuación, seleccione `PDF`, `PDF/A`, `PDF seguro`, `PDF firmado`, o `TIFF`. Vaya al paso ❾.

Nota

- Si ha seleccionado `PDF seguro`, el equipo le pedirá que introduzca una contraseña de 4 dígitos mediante los números del 0 al 9 antes de iniciar el escaneado.
- Si elige `PDF firmado`, deberá instalar y, a continuación, configurar un certificado en su equipo mediante Administración basada en Web.

9 Si utiliza el cristal de escaneado, pulse `Tamaño área escaneado`.
Pulse para seleccionar `A4`, `Carta` o `Legal/Folio` para la configuración del cristal de escaneado y, a continuación, seleccione una de las siguientes opciones:

- Si ha seleccionado color o gris en el ajuste de calidad del paso 6, vaya al paso 10.
- Si ha seleccionado blanco y negro en el ajuste de calidad del paso 6, vaya al paso 11.

10 Pulse `Tamño archvo` y, a continuación, seleccione el tamaño del archivo.
Vaya al paso 11.

11 Efectúe una de las acciones siguientes:

- Para iniciar el escaneado, pulse **Iniciar (Start) (Inicio)**.
- Para cambiar el nombre de archivo, vaya al paso 12.

12 Pulse ◄ o ► para visualizar `Nombre de archivo`. Pulse `Nombre de archivo`.
Pulse ▲ o ▼ para seleccionar el nombre de archivo que desee utilizar y, a continuación, pulse `OK`. Pulse **Iniciar (Start) (Inicio)**.

Nota

Para cambiar manualmente el nombre de archivo, vaya al paso 13.

13 Pulse ▲ o ▼ para seleccionar `<Manual>`. Pulse `OK`. (Para obtener información sobre cómo introducir texto, consulte *Introducción de texto en DCP-8250DN y MFC-8950DW(T)* ➤➤ página 14).
Introduzca el nombre de archivo que desee utilizar (hasta 64 caracteres) y pulse `OK`.
Pulse **Iniciar (Start) (Inicio)**. Vaya al paso 14.

14 En la pantalla LCD aparece `Conexión`. Una vez que se ha realizado correctamente la conexión con el servidor de red, el equipo iniciará el proceso de escaneado.
Si utiliza el cristal de escaneado, la pantalla LCD mostrará `Siguient página?`. Pulse `Sí` o `No` dependiendo de si desea escanear las páginas posteriores o no.

Introducción de texto

Introducción de texto en modelos con pantalla LCD de 5 líneas

Para configurar algunas selecciones de menú necesitará introducir caracteres de texto. Para ello, las teclas del teclado de marcación tienen letras impresas. Las teclas: **0**, **#** y ✳ no tienen letras impresas, ya que se utilizan como caracteres especiales.

Pulse la tecla adecuada del teclado de marcación tantas veces como se indica en esta tabla de referencia para acceder el carácter que desee.

Pulse la tecla	una vez	dos veces	tres veces	cuatro veces	cinco veces	seis veces	siete veces	ocho veces	nueve veces
1	@	.	/	1	@	.	/	1	@
2	a	b	c	A	B	C	2	a	b
3	d	e	f	D	E	F	3	d	e
4	g	h	i	G	H	I	4	g	h
5	j	k	l	J	K	L	5	j	k
6	m	n	o	M	N	O	6	m	n
7	p	q	r	s	P	Q	R	S	7
8	t	u	v	T	U	V	8	t	u
9	w	x	y	z	W	X	Y	Z	9

Inserción de espacios

Para introducir un espacio, pulse ▶ dos veces entre los números. Para introducir un espacio en un nombre, pulse ▶ dos veces entre los caracteres.

Corrección de errores

Si ha introducido una letra incorrecta y desea cambiarla, pulse ◀ o ▶ para desplazar el cursor al carácter incorrecto y, a continuación, pulse **Eliminar (Clear) (Borrar)**.

Repetición de letras

Para introducir un carácter de la misma tecla que el carácter anterior, pulse ▶ para desplazar el cursor a la derecha antes de volver a pulsar la tecla.

Caracteres y símbolos especiales

Pulse ✳, **#** o **0** y, a continuación, pulse ◀ o ▶ para desplazar el cursor al símbolo o al carácter que desee. Pulse **OK** para seleccionarlo. Aparecerán los símbolos y caracteres correspondientes a su selección de menú.

Introducción de texto en DCP-8250DN y MFC-8950DW(T)

Para configurar algunas selecciones de menús es posible que necesite introducir texto en el equipo.

Pulse varias veces para seleccionar entre letras, números o caracteres especiales. Pulse para cambiar entre mayúsculas y minúsculas.

Inserción de espacios

Para introducir un espacio, pulse la tecla de espacio o ▶.

Corrección de errores

Si ha introducido un carácter incorrecto y desea cambiarlo, utilice los botones de flecha para situar el cursor bajo el carácter incorrecto. A continuación, pulse . Introduzca el carácter correcto. También puede insertar letras desplazando el cursor e introduciendo un carácter.

Nota

- Los caracteres disponibles pueden variar en función del país.
- El diseño del teclado puede variar según la función que esté ajustando.

4 Certificado digital para PDF firmado

Configuración del certificado para PDF firmado

Si elige PDF firmado, deberá configurar un certificado en su equipo mediante Administración basada en Web.

Para utilizar PDF firmado deberá instalar un certificado en su equipo y en su ordenador.

1. Inicie su navegador web.
2. Introduzca “http://dirección IP del equipo/” en la barra de direcciones de su navegador (donde “dirección IP del equipo” es la dirección IP del equipo o el nombre del servidor de impresión).
   - Por ejemplo: http://192.168.1.2/
3. No se necesita una contraseña de manera predeterminada. Si ha establecido anteriormente una contraseña, introdúzcala y pulse .
4. Haga clic en **Administrador**.
5. Elija **PDF firmado** para realizar una configuración.
6. Seleccione el certificado de la lista desplegable **Seleccionar el certificado**.

7. Haga clic en **Enviar**.

Certificados admitidos

El equipo Brother admite los siguientes certificados.

- Certificado autofirmado

  El servidor de impresión emite su propio certificado. Mediante este certificado, es posible utilizar la comunicación SSL/TLS fácilmente sin disponer de un certificado de una CA. (Consulte *Creación de un certificado autofirmado* ➤➤ página 18).

- Certificados de una CA

  Existen dos métodos para instalar certificados de una CA. Si ya dispone de una CA o si desea utilizar un certificado de una CA externa fiable:

  - Si se utiliza una CSR (Certificate Signing Request, solicitud de firma de certificado) de este servidor de impresión. (Consulte *Creación de una solicitud de firma de certificado (Certificate Signing Request, CSR)* ➤➤ página 19).
  - Si se importa un certificado y una clave privada. (Consulte *Importación y exportación del certificado y la clave privada* ➤➤ página 22).

- Certificados de CA

  Si utiliza un certificado de CA que identifique a la propia autoridad de certificación y posea su clave privada, deberá importar un certificado de CA de la CA antes de efectuar la configuración. (Consulte *Importación y exportación de un certificado de CA* ➤➤ página 23).

Instalación del certificado digital

Para usar PDF firmado es necesario instalar un certificado digital en el equipo y en el dispositivo que envía datos al equipo, por ejemplo un ordenador. Para configurar el certificado, el usuario debe iniciar sesión de forma remota en el equipo mediante un navegador web utilizando su dirección IP.

1. Inicie su navegador web.
2. Introduzca “http://dirección IP del equipo/” en la barra de direcciones de su navegador (donde “dirección IP del equipo” es la dirección IP del equipo o el nombre del servidor de impresión).
   - Por ejemplo: http://192.168.1.2/
3. No se necesita una contraseña de manera predeterminada. Si ha establecido anteriormente una contraseña, introdúzcala y pulse .
4. Haga clic en **Red**.
5. Haga clic en **Seguridad**.
6. Haga clic en **Certificado**.
7. Es posible configurar los ajustes del certificado.
   Para crear un certificado autofirmado mediante Administración basada en web, vaya a *Creación de un certificado autofirmado* ➤➤ página 18.
   Para crear una solicitud de firma de certificado (Certificate Signing Request, CSR), vaya a *Creación de una solicitud de firma de certificado (Certificate Signing Request, CSR)* ➤➤ página 19.

1 Creación e instalación de un certificado autofirmado

2 Utilización de un certificado de una autoridad de certificación (CA)

Nota

- Las funciones que aparecen atenuadas y no vinculadas no se encuentran disponibles.
- Si desea obtener más información acerca de la configuración, consulte el texto de Ayuda en Administración basada en web.

Creación de un certificado autofirmado

1. Haga clic en **Crear certificado autofirmado**.
2. Introduzca un **Nombre común** y una **Fecha válida**.

Nota

- La longitud del **Nombre común** puede ser de hasta 64 caracteres. El nombre de nodo se visualiza de manera predeterminada.
- Si se utiliza el protocolo IPPS o HTTPS, se mostrará una advertencia, y deberá introducir un nombre en la URL diferente al **Nombre común** utilizado con el certificado autofirmado.

3. Puede seleccionar los ajustes **Algoritmo de clave pública** y **Algoritmo implícito** de la lista desplegable. Las configuraciones predeterminadas son **RSA (2048 bits)** para **Algoritmo de clave pública** y **SHA256** para **Algoritmo implícito**.
4. Haga clic en **Enviar**.
5. El certificado autofirmado se creará y se guardará correctamente en la memoria del equipo.

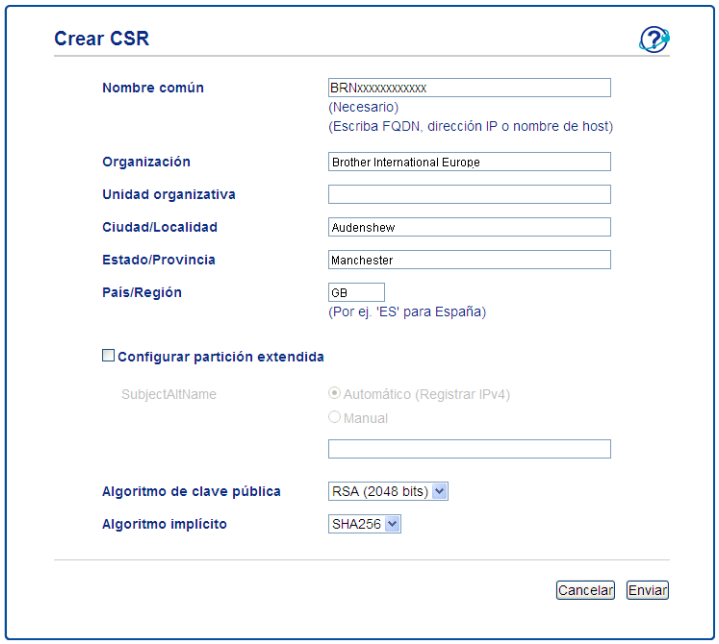
Creación de una solicitud de firma de certificado (Certificate Signing Request, CSR)

Una solicitud de firma de certificado (CSR) es una solicitud que se envía a una CA para autenticar las credenciales que se incluyen en el certificado.

Nota

Es recomendable instalar el certificado raíz de la CA en el ordenador antes de crear la CSR.

1. Haga clic en **Crear CSR**.
2. Introduzca un **Nombre común** y su información, por ejemplo, la **Organización**.
   Los datos de la empresa son necesarios para que una CA pueda confirmar su identidad y atestiguarla ante el mundo exterior.



Nota

- La longitud del **Nombre común** puede ser de hasta 64 caracteres. Es necesario introducir un **Nombre común**.
- Se mostrará una advertencia si se introduce un nombre diferente en la URL al nombre común utilizado para el certificado.
- La longitud de la **Organización**, la **Unidad organizativa**, la **Ciudad/Localidad** y el **Estado/Provincia** puede ser de hasta 64 caracteres.
- El **País/Región** debe ser un código de país ISO 3166 compuesto por dos caracteres.
- Si está configurando la extensión del certificado X.509v3, elija la casilla de verificación **Configurar partición extendida** y, a continuación, elija **Automático (Registrar IPv4)** o **Manual**.

3 Puede seleccionar los ajustes **Algoritmo de clave pública** y **Algoritmo implícito** de la lista desplegable. Las configuraciones predeterminadas son **RSA (2048 bits)** para **Algoritmo de clave pública** y **SHA256** para **Algoritmo implícito**.

4 Haga clic en **Enviar**. Aparecerá la pantalla siguiente.

5 Después de unos instantes se le presentará el certificado, que podrá guardar en un pequeño archivo o copiar y pegarlo directamente en un formulario CSR en línea ofrecido por una autoridad de certificación. Haga clic en **Guardar** para guardar el archivo CSR en su ordenador.

Nota

Siga la política de la CA relacionada con el método de envío de una CSR a la CA.

6 Se ha creado la CSR. Para obtener instrucciones sobre cómo instalar el certificado en su equipo, vaya a *Instalación del certificado en el equipo* ➤➤ página 21.

Instalación del certificado en el equipo

Cuando reciba el certificado de una CA, siga los pasos indicados a continuación para instalarlo en el servidor de impresión.

Nota

Únicamente es posible instalar un certificado emitido con la CSR de este equipo. Si desea crear otra CSR, asegúrese de que el certificado se encuentre instalado antes de crear otra CSR. Cree otra CSR después de instalar el certificado en el equipo. De lo contrario, la CSR creada antes de la instalación no será válida.

1. Haga clic en **Instalar certificado** en la página **Certificado**.

2. Especifique el archivo del certificado emitido por una CA y, a continuación, haga clic en **Enviar**.
3. El certificado se ha creado y guardado correctamente en la memoria del equipo.

Importación y exportación del certificado y la clave privada

Es posible almacenar el certificado y la clave privada en el equipo y administrarlos mediante importación y exportación.

Importación del certificado autofirmado, el certificado emitido por una CA y la clave privada

1. Haga clic en **Importar certificado y clave secreta** en la página **Certificado**.
2. Especifique el archivo que desee importar.
3. Introduzca la contraseña si el archivo se encuentra cifrado y, a continuación, haga clic en **Enviar**.
4. El certificado y la clave privada se importarán al equipo correctamente.

Exportación del certificado autofirmado, el certificado emitido por una CA y la clave privada

1. Haga clic en **Exportar** que se muestra con la **Lista de certificados** en la página **Certificado**.
2. Introduzca una contraseña si desea cifrar el archivo.

Nota

Si se utiliza una contraseña en blanco, la salida no se cifrará.

3. Introduzca la contraseña de nuevo para confirmarla y, a continuación, haga clic en **Enviar**.
4. Especifique la ubicación en la que desee guardar el archivo.
5. El certificado y la clave privada se exportarán al ordenador.

Importación y exportación de un certificado de CA

Es posible almacenar un certificado de CA en el equipo mediante importación y exportación.

Cómo importar un certificado de CA

1. Haga clic en **Certificado CA** en la página **Seguridad**.
2. Haga clic en **Importar certificado CA** y seleccione el certificado. Haga clic en **Enviar**.

Cómo exportar un certificado de CA

1. Haga clic en **Certificado CA** en la página **Seguridad**.
2. Seleccione el certificado que desee exportar y haga clic en **Exportar**. Haga clic en **Enviar**.
3. Haga clic en **Guardar** para seleccionar la carpeta de destino.
4. Seleccione el destino en el que desee guardar el certificado exportado y, a continuación, guárdelo.

5 Solución de problemas

Visión general

Este capítulo explica cómo resolver los problemas de red comunes que pueden presentarse al utilizar el equipo Brother. Si después de leer este capítulo no puede solucionar su problema, visite el Brother Solutions Center en: (http://solutions.brother.com/).

Visite el Brother Solutions Center en (http://solutions.brother.com/) y haga clic en Manuales en la página de su modelo para descargar los otros manuales.

Identificación del problema

Asegúrese de que los siguientes elementos se encuentran configurados antes de leer este capítulo.

Primero compruebe los siguientes puntos:
El cable de alimentación está correctamente conectado y el equipo Brother está encendido.
Todo el embalaje protector se ha retirado del equipo.
Los cartuchos de tóner y la unidad de tambor están correctamente instalados.
Las cubiertas delantera y posterior están completamente cerradas.
El papel se introduce correctamente en la bandeja de papel.

Diríjase a la página correspondiente a la solución adecuada para usted en las listas facilitadas a continuación

- Mensajes de error al utilizar la función de Escanear a red

  Consulte *Mensajes de error al utilizar la función de Escanear a red* ➤➤ página 25

Mensajes de error al utilizar la función de Escanear a red

Mensaje de error	Causa	Acción
`Servidor desact.`	Dirección de host incorrecta	■ Si ha utilizado la dirección IP de su servidor CIFS como dirección de host, confirme la dirección IP. ■ Si ha especificado el tipo de DNS como dirección de host, confirme la dirección de host. Para configurar la dirección de tipo DNS, póngase en contacto con su administrador de red. ■ Si ha utilizado el nombre de su ordenador como dirección de host, confirme el nombre del ordenador. Para configurar el servidor WINS, póngase en contacto con su administrador de red.
`Error Autentic.` `Error enviando`	Nombre de usuario incorrecto	■ Confirme su nombre de usuario para el servidor CIFS. Para configurar su nombre de usuario, consulte *Configuración de ajustes predeterminados de Escanear a red* ➤➤ página 4. ■ Si el nombre de usuario forma parte del dominio, asegúrese de que ha introducido el nombre de dominio incluido en el nombre de usuario. Por ejemplo: • usuario@dominio • dominio\usuario
	Contraseña incorrecta	Confirme su contraseña para el servidor CIFS. Para configurar su contraseña, consulte *Configuración de ajustes predeterminados de Escanear a red* ➤➤ página 4.
`Error Autentic.` `Fech/hora incor.`	La configuración de fecha y hora de su equipo no es correcta.	Asegúrese de que los ajustes de fecha y hora y de zona horaria estén correctamente configurados mediante el panel de control, de modo que la hora del equipo coincida con la hora utilizada por el servidor que proporciona la autenticación.

Terminología de red y formato de archivo PDF

Terminología de red

- CIFS

  El sistema Common Internet File System es el modo estándar mediante el cual los usuarios de los ordenadores comparten archivos e impresoras en Windows®.

- SNTP

  El protocolo Simple Network Time Protocol se utiliza para sincronizar los relojes del ordenador en una red TCP/IP. Puede realizar la configuración de SNTP mediante el uso de Administración basada en Web (navegador web).

- Kerberos

  Kerberos es un protocolo de autenticación que permite a los dispositivos o individuos demostrar de manera segura su identidad en los servidores de red mediante un inicio de sesión único.

- NTLMv2

  NTLMv2 es el método de autenticación utilizado por Windows para registrarse en los servidores.

Formato de archivo PDF

- PDF/A

  PDF/A es un formato de archivo PDF diseñado para archivar durante un largo período de tiempo. Este formato contiene toda la información necesaria para reproducir el documento después de un largo período de almacenamiento.

- PDF seguro

  PDF seguro es un formato de documento PDF que ha sido protegido con una contraseña.

- PDF firmado

  Un Signed PDF es un formato de archivo PDF que ayuda a impedir la falsificación de datos y la suplantación de identidad, ya que incluye un certificado digital dentro del documento.

  Si elige PDF firmado, deberá instalar y después configurar un certificado en su equipo mediante Administración basada en Web.