



Guía breve para el usuario de Cisco Secure Firewall de la serie 6100

Última modificación: 2026-04-08

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CISCO SYSTEMS DE MEXICO S.DE R.L. DE C.V.

Avenida (AV) Paseo de Tamarindos 400A, piso 14

Col. Bosques de las Lomas, Cuajimalpa de Morelos

Mexico, Ciudad De Mexico 05120

Tel: +52 55 5267 1000

LAS ESPECIFICACIONES E INFORMACIÓN RELATIVAS A LOS PRODUCTOS DE ESTE MANUAL ESTÁN SUJETAS A CAMBIOS SIN PREVIO AVISO. TODAS LAS DECLARACIONES, INFORMACIONES Y RECOMENDACIONES INCLUIDAS EN ESTE MANUAL SE CONSIDERAN PRECISAS; SIN EMBARGO, NO SE PRESENTAN GARANTÍAS DE NINGÚN TIPO, NI EXPRESAS NI IMPLÍCITAS. LOS USUARIOS DEBEN ASUMIR LA PLENA RESPONSABILIDAD DE SU APLICACIÓN EN TODOS LOS PRODUCTOS.

LA LICENCIA DE SOFTWARE Y LA GARANTÍA LIMITADA DEL PRODUCTO AL QUE ACOMPAÑAN SE EXPONEN EN EL PAQUETE DE INFORMACIÓN QUE SE ENVÍA CON EL PRODUCTO Y SE INCLUYEN EN EL PRESENTE DOCUMENTO A TRAVÉS DE ESTA REFERENCIA. SI NO ENCUENTRA LA LICENCIA DEL SOFTWARE O LA GARANTÍA LIMITADA, PÓNGASE EN CONTACTO CON SU REPRESENTANTE DE CISCO PARA OBTENER UNA COPIA.

La siguiente información concierne al cumplimiento de los requisitos de la FCC para los dispositivos de Clase A: este equipo ha sido probado y cumple con los límites establecidos para un dispositivo digital de Clase A, de conformidad con el apartado 15 del reglamento de la FCC. Estos límites están diseñados para proporcionar una protección razonable frente a cualquier interferencia perjudicial al utilizar el equipo en un entorno comercial. Este equipo genera, usa y puede emitir energía de radiofrecuencia y, en caso de no instalarse ni usarse de conformidad con el manual de instrucciones, podría causar interferencias perjudiciales que dificultarían las comunicaciones por radio. La conexión de este equipo en una zona residencial puede provocar interferencias perjudiciales; en tal caso, se exigirá a los usuarios que corran con los gastos de la reparación de dichos daños.

La siguiente información concierne al cumplimiento de los requisitos de la FCC para los dispositivos de Clase B: este equipo ha sido probado y cumple con los límites establecidos para un dispositivo digital de Clase B, de conformidad con el apartado 15 del reglamento de la FCC. Estos límites han sido diseñados con el objetivo de proporcionar una protección razonable frente a interferencias perjudiciales en instalaciones residenciales. Este equipo genera, usa y puede emitir energía de radiofrecuencia y, en caso de no instalarse ni usarse de conformidad con las instrucciones, podría causar interferencias perjudiciales que dificultarían las comunicaciones por radio. Sin embargo, no es posible garantizar que no vayan a producirse interferencias en una instalación determinada. Si el equipo causa interferencias en la recepción de señales de radio o televisión (lo que se puede determinar apagando y encendiendo el equipo), se recomienda a los usuarios que intenten corregir las interferencias mediante uno o varios de los métodos que se indican a continuación:

- Reoriente o reubique la antena receptora.
- Aumente la distancia entre los equipos y el receptor.
- Conecte el equipo a una toma en un circuito diferente al que se encuentra conectado el receptor.
- Solicite ayuda al distribuidor o a un técnico experto en radio y televisión.

Las modificaciones realizadas en el producto que no estén autorizadas por Cisco podrían anular la aprobación de la FCC y negarle el permiso para utilizar el producto.

La implementación por parte de Cisco de la compresión del encabezado de TCP es una adaptación de un programa desarrollado por la Universidad de California, Berkeley (UCB) como parte de la versión de dominio público del sistema operativo UNIX de la UCB. Todos los derechos reservados. Copyright © 1981, Regentes de la Universidad de California.

NO OBSTANTE CUALQUIER OTRA GARANTÍA QUE AQUÍ SE DESCRIBA, TODOS LOS ARCHIVOS DE DOCUMENTO Y SOFTWARE DE ESTOS PROVEEDORES SE PROPORCIONAN "TAL CUAL" CON TODOS LOS ERRORES QUE PUDIERAN INCLUIR. CISCO Y LOS PROVEEDORES ANTERIORMENTE MENCIONADOS NIEGAN CUALQUIER GARANTÍA, EXPRESA O IMPLÍCITA, INCLUIDAS, SIN LIMITACIÓN, AQUELLAS DE COMERCIABILIDAD, ADECUACIÓN A UN FIN DETERMINADO E INCUMPLIMIENTO O QUE PUEDAN SURGIR DE UN PROCESO DE NEGOCIACIÓN, USO O PRÁCTICA COMERCIAL.

BAJO NINGUNA CIRCUNSTANCIA CISCO O SUS PROVEEDORES SERÁN RESPONSABLES DE NINGÚN DAÑO INDIRECTO, ESPECIAL, SECUNDARIO O FORTUITO, INCLUIDOS ENTRE OTROS, LA PÉRDIDA DE GANANCIAS, O LA PÉRDIDA O EL DAÑO DE DATOS COMO CONSECUENCIA DEL USO O INCAPACIDAD DE USO DE ESTE MANUAL, INCLUSO EN EL CASO DE QUE CISCO O SUS PROVEEDORES HAYAN SIDO NOTIFICADOS SOBRE LA POSIBILIDAD DE QUE SE PRODUZCAN TALES DAÑOS.

Cualquier dirección de protocolo de Internet (IP) o número de teléfono utilizado en este documento no pretende ser una dirección o un número de teléfono real. Cualquier ejemplo, salida de visualización de comandos, diagrama de topología de red y figura incluida en el documento se muestra solo con fines ilustrativos. El uso de direcciones IP o números de teléfono reales en el material ilustrativo no es intencionado, sino mera coincidencia.

Se carece de control sobre todas las copias impresas y duplicados en formato electrónico de este documento. Consulte la versión en línea actual para obtener la versión más reciente.

Cisco tiene más de 200 oficinas en todo el mundo. Las direcciones y los números de teléfono están disponibles en el sitio web de Cisco: www.cisco.com/go/offices.

© 2026 Cisco Systems, Inc. Todos los derechos reservados.



CAPÍTULO 1

Guía breve para el usuario de Cisco Secure Firewall de la serie 6100

- Características, en la página 1
- Número de serie y código QR del portal de documentación, en la página 1
- Panel frontal, en la página 3
- LED del panel frontal, en la página 5
- Panel posterior, en la página 7
- Puertos de administración, consola y USB, en la página 8
- Botón de encendido y botón de restablecimiento, en la página 10
- Especificaciones de hardware, en la página 11
- Módulos de fuente de alimentación, en la página 11
- Módulos de ventiladores, en la página 13
- SSD, en la página 14
- Puesta a tierra del chasis, en la página 15
- Colocación, en la página 18
- Producto de clase A, en la página 18
- Almacenamiento, transporte, venta y eliminación , en la página 18
- Qué hacer si el equipo funciona mal, en la página 19
- Información adicional, en la página 20

Características

Cisco Secure Firewall de la serie 6100 es una plataforma de servicios de seguridad modular independiente que incluye las series 6160 y 6170.

En la siguiente figura, se muestran los chasis de Secure Firewall de la serie 6100.

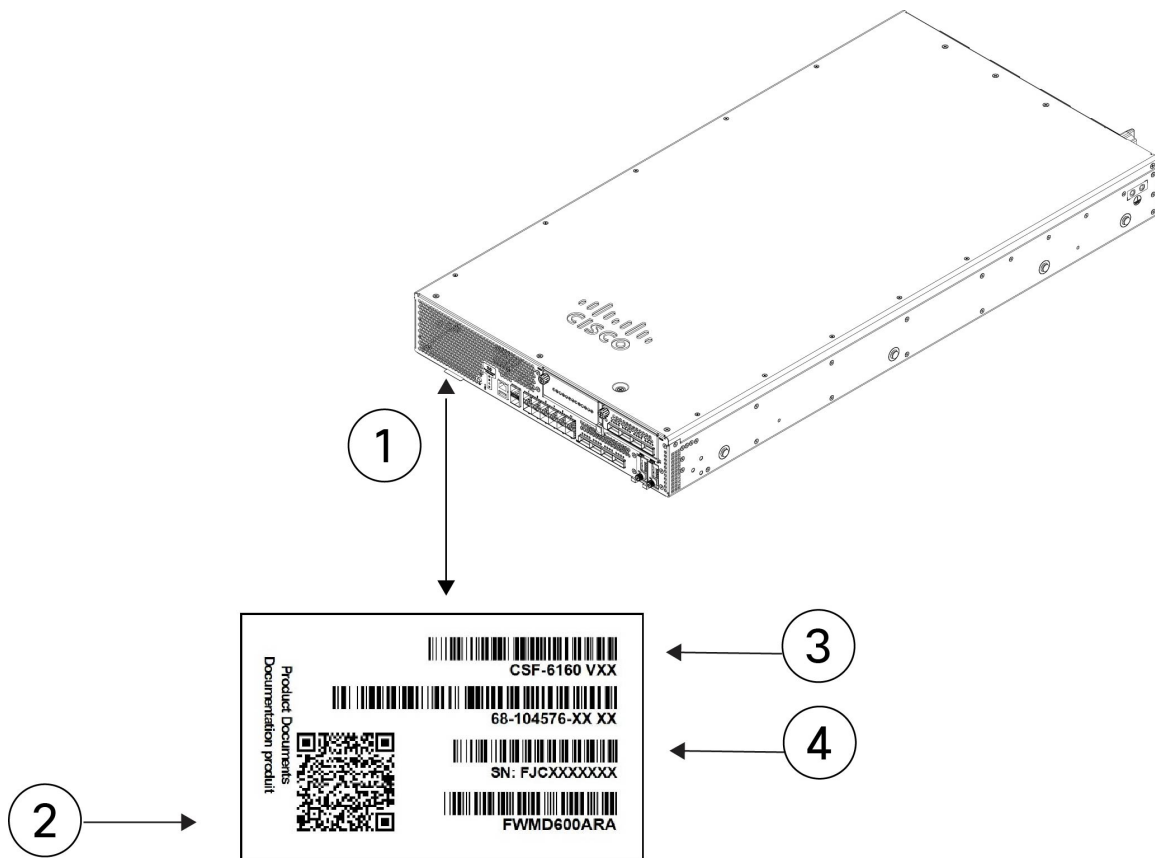
En la siguiente tabla, se enumeran las funciones de Secure Firewall de la serie 6100.

Número de serie y código QR del portal de documentación

La tarjeta de recursos extraíble en el panel frontal del chasis de Secure Firewall de la serie 6100 contiene el número de serie del chasis y el código QR del portal de documentación, que le permite acceder a la información

del producto, la guía de primeros pasos, la guía de reglamentaciones y cumplimiento, la guía de instalación de hardware y la guía de aprovisionamiento automatizado.

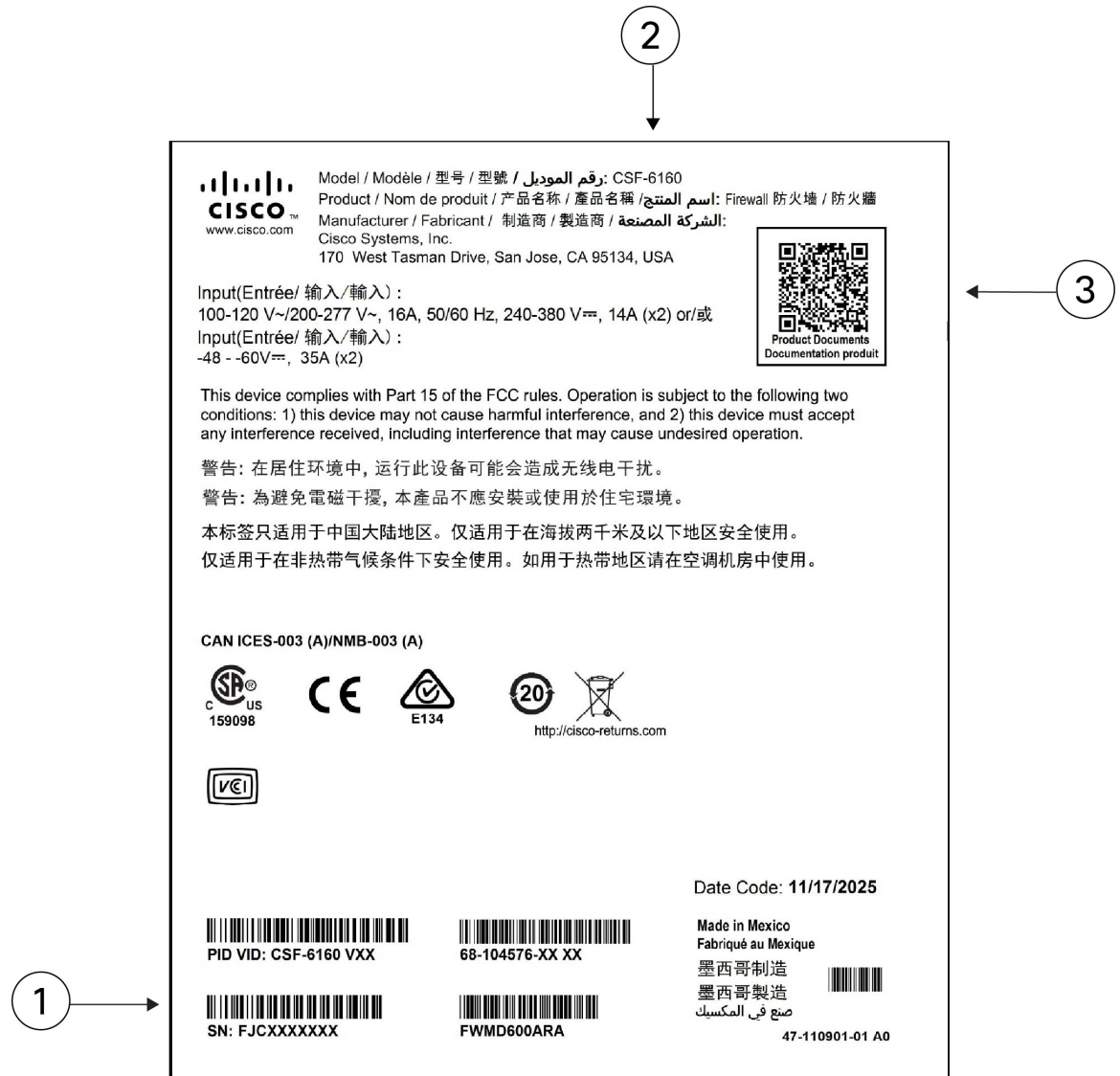
Figura 1: Tarjeta de recursos extraíble



1	Etiqueta de identificación de recursos extraíble	2	Código QR del portal de documentación
3	Número de modelo del chasis	4	Número de serie del chasis

La etiqueta de cumplimiento en la parte inferior del chasis contiene el número de serie del chasis, las marcas de cumplimiento normativo y también el código QR del portal de documentación que dirige a las guías enumeradas anteriormente. La siguiente figura muestra un ejemplo de etiqueta de cumplimiento que se encuentra en la parte inferior del chasis.

Figura 2: Ejemplo de etiqueta de cumplimiento

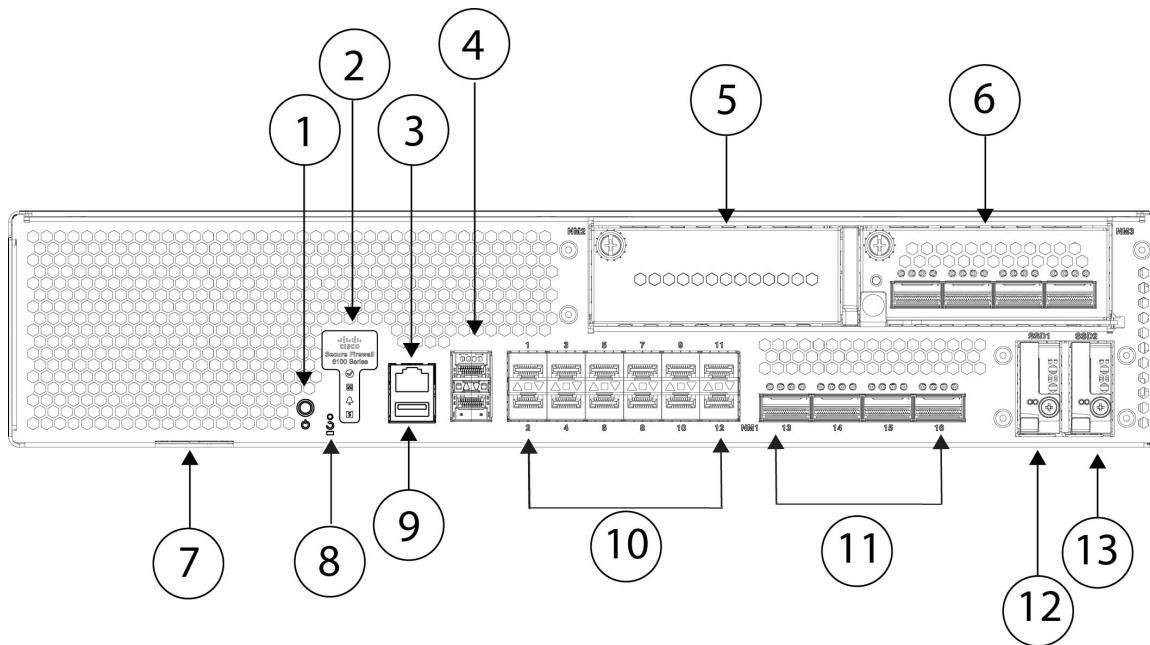


1	Número de serie	2	Número de modelo del chasis
3	Código QR del portal de documentación		—

Panel frontal

En la siguiente figura, se muestra el panel frontal de Secure Firewall de la serie 6100. Consulte [LED del panel frontal, en la página 5](#) para obtener una descripción de los LED.

Figura 3: Panel frontal de CSF-6160 y CSF-6170



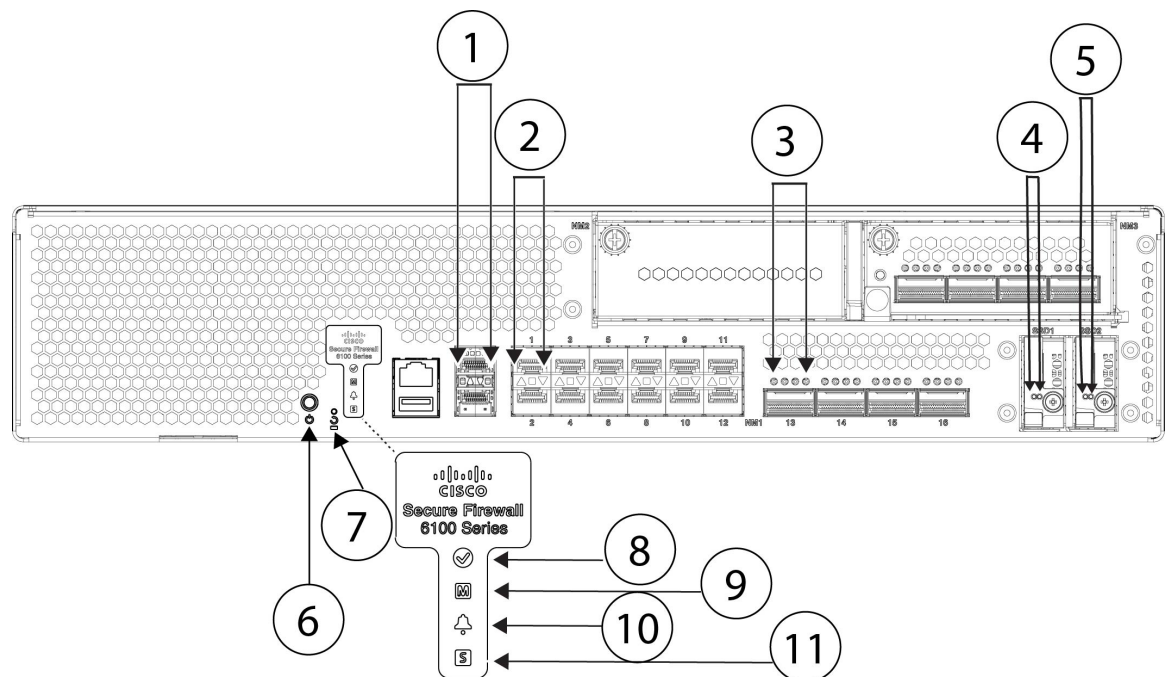
<p>1 Botón de encendido/apagado</p> <p>Botón pulsador multifunción que controla el reinicio, el apagado y el encendido.</p>	<p>2 LED del sistema</p>
<p>3 Puerto de consola RJ-45 (8P8C)</p>	<p>4 Puertos de administración apilados dobles (compatibles con 1/10/25 Gbps)</p> <p>Puerto superior:</p> <ul style="list-style-type: none"> • Cisco Secure Firewall Threat Defense: administración 0 (también denominada administración 1/1) • ASA: Administración 1/1 <p>Puerto inferior:</p> <ul style="list-style-type: none"> • Cisco Secure Firewall Threat Defense: Administración 1 (también denominada Administración 1/2) • ASA: Administración 1/2
<p>5 Ranuras para módulos de red (NM-2)</p>	<p>6 Ranuras para módulos de red (NM-3)</p>
<p>7 Tarjeta de recursos extraíble con número de serie del chasis y código QR al portal de documentación digital que tiene enlaces a la guía de primeros pasos, la guía de hardware y la guía de reglamentaciones y cumplimiento.</p>	<p>8 Botón de restablecimiento de fábrica empotrado</p>

9	Puerto USB 3.0 tipo A	10	Doce puertos de fibra fijos SFP56 de 1/10/25/50 Gbps (NM-1) Puertos de fibra denominados del 1/1 al 1/12 de izquierda a derecha
11	Cuatro puertos de fibra fija QSFP56 de 40/100/200 Gbps (NM-1) Puertos de fibra denominados de 1/13 a 1/16 de izquierda a derecha	12	Ranura para SSD (SSD-1)
13	Ranura para SSD (SSD-2)	—	—

LED del panel frontal

En la siguiente figura, se muestran los LED del panel frontal de Secure Firewall de la serie 6100.

Figura 4: LED del panel frontal de CSF-6160 y CSF-6170



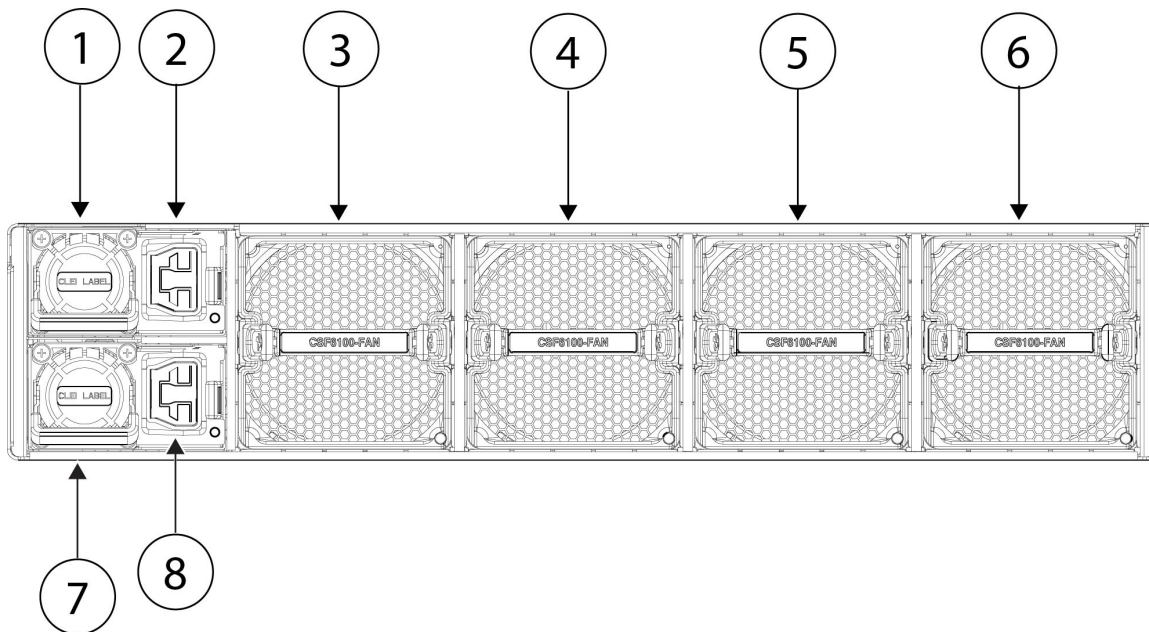
<p>1 Puerto de administración</p> <p>El puerto de administración de fibra de 1/10/25 Gbps tiene un LED bicolor debajo de la caja de SFP que indica enlace/actividad/falla:</p> <ul style="list-style-type: none"> • Desactivado: sin SFP. • Verde: el enlace está activo. • Verde intermitente: actividad de la red. • Ámbar: SFP presente, pero sin enlace. 	<p>2 Estado de actividad/enlace del puerto de fibra</p> <p>Cada puerto de fibra tiene un LED de dos colores debajo de la caja de SFP.</p> <ul style="list-style-type: none"> • Desactivado: sin SFP. • Verde: el enlace está activo. • Verde intermitente: actividad de la red. • Ámbar: sin enlace o falla de red.
<p>3 Enlace/actividad de puerto fijo de QSFP</p> <p>Cada puerto de fibra tiene un LED bicolor debajo de la caja de QSFP.</p> <ul style="list-style-type: none"> • Desactivado: sin SFP. • Verde: el enlace está activo. • Verde intermitente: actividad de la red. • Ámbar: sin enlace o falla de red. <p>Nota Hay cuatro LED para cada zócalo QSFP.</p> <p>Cuando se ejecutan 40/100/200 Gbps nativos, solo el LED izquierdo está activo (de 4 LED por puerto). Sin embargo, en el modo de división 4 x 10/25 G/50 G, los cuatro LED de un puerto están activos y se activan según la actividad del canal respectivo.</p>	<p>4 SSD-1</p> <p>Nota El LED izquierdo está activo. El LED derecho siempre está apagado.</p> <ul style="list-style-type: none"> • Apagado: la SSD no está presente. • Verde: la SSD está presente; sin actividad. • Verde intermitente: la SSD está activa. • Ámbar: la SSD tiene un problema o una falla.
<p>5 SSD-2</p> <p>Nota El LED izquierdo está activo. El LED derecho siempre está apagado.</p> <ul style="list-style-type: none"> • Apagado: la SSD no está presente. • Verde: la SSD está presente; sin actividad. • Verde intermitente: la SSD está activa. • Ámbar: la SSD tiene un problema o una falla. 	<p>6 Alimentación</p> <ul style="list-style-type: none"> • Apagado: el sistema está apagado. Si el cable de alimentación de CA está enchufado y el LED de la fuente de alimentación parpadea en verde, la alimentación en espera aún está encendida. • Verde intermitente: el sistema detectó un evento en el botón de encendido e inició la secuencia de apagado. No quite la fuente de alimentación de CA o CC mientras este LED esté parpadeando para que el sistema tenga tiempo de realizar un apagado correcto. • Verde: el sistema está totalmente encendido. • Ámbar: se completó un apagado correcto o se detectaron fallas de alimentación en el sistema.

<p>7</p>	<p>Botón de restablecimiento de fábrica</p> <ul style="list-style-type: none"> • Verde intermitente: parpadea 5 segundos después de presionar el botón. • Desactivado: el restablecimiento se ha completado. <p>Nota El botón de restablecimiento de fábrica comienza a parpadear después de haber estado presionado durante al menos 5 segundos y persiste hasta que el software haya aplicado completamente todas las configuraciones predeterminadas de fábrica o se interrumpa con un ciclo de encendido.</p>	<p>8</p>	<p>Activo (rol de un par de alta disponibilidad)</p> <ul style="list-style-type: none"> • Apagado: la unidad no está configurada o habilitada en un par de alta disponibilidad. • Verde: la unidad está en modo activo. • Amarillo: la unidad está en modo de espera.
<p>9</p>	<p>Administrado</p> <p>Reservado para uso futuro.</p>	<p>10</p>	<p>Alarma</p> <ul style="list-style-type: none"> • Apagado: mientras el sistema se está encendiendo y arrancando. • Amarillo: fuente de alimentación, temperatura demasiado alta o fallas del ventilador. • Verde: sin alarmas.
<p>11</p>	<p>Sistema</p> <ul style="list-style-type: none"> • Apagado: mientras el sistema está arrancando. • Parpadeo rápido de color verde: el sistema se está iniciando. • Verde: función normal del sistema. • Amarillo: el arranque del sistema falló. • Amarillo, intermitente: condición de alarma, el sistema necesita servicio o atención y es posible que no arranque correctamente. 	<p>—</p>	<p>—</p>

Panel posterior

La siguiente figura muestra el panel posterior de Secure Firewall de la serie 6100. Consulte [Módulos de fuente de alimentación, en la página 11](#) y [Módulos de ventiladores, en la página 13](#) para obtener una descripción de los LED de la fuente de alimentación y del ventilador.

Figura 5: Panel posterior de CSF-6160 y CSF-6170



1	Módulo de fuente de alimentación (PSU-1)	2	Conector del módulo de fuente de alimentación (PSU-1)
3	Módulo de ventilador doble (FAN-1)	4	Módulo de ventilador doble (FAN-2)
5	Módulo de ventilador doble (FAN-3)	6	Módulo de ventilador doble (FAN-4)
7	Módulo de fuente de alimentación (PSU-2)	8	Conector del módulo de fuente de alimentación (PSU-2)

Puertos de administración, consola y USB

Puerto de administración

El chasis de Secure Firewall de la serie 6100 tiene dos puertos de administración. Son puertos SFP28 de 1/10/25 Gbps que admiten fibra, así como DAC o GLC-TE.

Puerto de consola RJ-45

El chasis de Secure Firewall de la serie 6100 no se envía con un cable de serie RJ-45, a menos que lo solicite con el chasis. Por ejemplo, puede obtener un cable de serie de USB a RJ-45. Puede utilizar la CLI para configurar su Secure Firewall de la serie 6100 a través del puerto de consola serial RJ-45 mediante un servidor de terminal o un programa de emulación de terminales en una computadora.

El puerto RJ-45 (8P8C) admite la señalización RS-232 a un controlador UART interno. El puerto de la consola no tiene ningún control de flujo de hardware y no admite un módem de marcación remota. La configuración predeterminada del puerto de la consola se muestra de la siguiente manera:

- 9600 baudios de velocidad

- 8 bits de datos
- Sin paridad
- 1 bit de parada
- Sin control del flujo

Puerto USB 3.0 tipo A

Puede utilizar el puerto USB tipo A externo para conectar un dispositivo de almacenamiento de datos. El identificador de la unidad USB externa es `usb:`. El puerto USB tipo A admite lo siguiente:

- Intercambio con el sistema activo.
- Unidad USB formateada con FAT32.
- Imagen de arranque kickstart de ROMMON para fines de recuperación de detección.
- Copia de archivos en el espacio de trabajo:/ y datos volátiles:/ dentro de local-mgmt. Los archivos más relevantes son:
 - Archivos principales.
 - Capturas de paquetes de EthAnalyzer.
 - Archivos de soporte técnico.
 - Archivos de registro del módulo de seguridad.
- Carga de imagen del paquete de la plataforma con la **imagen de descarga USB A:**

El puerto USB tipo A *no* admite la carga de imágenes de Cisco Secure Package (CSP).

Puertos de red

El chasis de Cisco Secure Firewall 6100 tiene dos ranuras para módulos de red que admiten los siguientes módulos de red:

- SFP+ de 8 puertos de 1/10 Gbps (CSF6K-XNM-8X10G)
- SFP+ de 8 puertos de 1/10/25 Gbps (CSF6K-XNM-8X25G)
- QSFP/QSFP+ de 4 puertos de 40 Gbps (CSF6K-XNM-4X40G)
- QSFP56/QSFP de 4 puertos de 40/100/200 Gbps (CSF6K-XNM-4X200G)
- QSFP56/QSFP28/QSFP de 2 puertos de 100 Gbps (CSF6K-XNM-2X100G)
- SFP de 6 puertos de 1 Gbps con desvío de hardware, multimodo SX (CSF6K-XNM-6X1SXF)
- SFP de 6 puertos de 10 Gbps con desvío de hardware, multimodo SR (CSF6K-XNM-6X10SRF)
- SFP de 6 puertos de 10 Gbps con desvío de hardware, monomodo LR (CSF6K-XNM-6X10LRF)
- SFP de 6 puertos de 25 Gbps con desvío de hardware, multimodo SR (CSF6K-XNM-6X25SRF)
- SFP de 6 puertos de 25 Gbps con desvío de hardware, monomodo LR (CSF6K-XNM-6X25LRF)
- 1000Base-T de 8 puertos de cobre de 1 Gbps con desvío de hardware (CSF6K-XNM-8X1GF)
- QSFP-DD de 2 puertos de 400 Gbps (CSF6K-XNM-2X400G)

Botón de encendido y botón de restablecimiento

Secure Firewall de la serie 6100 tiene un botón de encendido en el panel frontal que controla la alimentación del sistema. El sistema se enciende automáticamente cuando se aplica alimentación de CA. El botón está en la posición de encendido cuando se presiona y en posición de apagado cuando sobresale. Para reiniciar, mantenga presionado durante 5 segundos; para un apagado correcto, manténgalo presionado durante 15 segundos. Espere siempre a que los LED se apaguen antes de desconectar los cables de alimentación para evitar daños en el disco.

También hay un botón de restablecimiento de fábrica empotrado. Si se mantiene presionado durante 5 segundos, se restablece el sistema a los valores predeterminados de fábrica y se borran las configuraciones y los archivos de usuario. Use esto si se pierden las credenciales y el acceso a la consola no está disponible. Si se produce un corte de corriente durante el restablecimiento, el proceso deberá reiniciarse una vez restituido el suministro.

Botón de encendido

El botón de encendido es un botón pulsador sin bloqueo para el control de alimentación del sistema. Se encuentra en el lado izquierdo del panel frontal. Cuando se enciende la alimentación de CA por primera vez, no es necesario presionar el botón porque el sistema se activa de manera predeterminada. Durante el proceso de apagado, el LED de alimentación parpadea en verde, lo que indica que el proceso se ha iniciado. Una vez que se completa el apagado, el sistema se apaga. Espere a que los LED de alimentación del sistema se vuelvan de color ámbar fijo antes de desconectar los cables de alimentación de CA. Consulte [LED del panel frontal, en la página 5](#) para obtener una descripción detallada del LED de estado de alimentación.

En el indicador ROMMON o FX-OS:

- Presione el botón de encendido durante 5 segundos y suéltelo para reiniciar el sistema. El LED de alimentación parpadea en verde a una velocidad de 2 Hz.
- Presione el botón de encendido durante 15 segundos y suéltelo para iniciar un apagado correcto. El LED de alimentación parpadea en verde a una velocidad de 10 Hz.



Nota Threat Defense requiere un apagado correcto. Consulte la Guía de primeros pasos para el procedimiento.



Nota Después de desconectar la alimentación del chasis desenchufando el cable de alimentación, espere al menos 10 segundos antes de volver a conectar la alimentación. Es necesario mantener apagado el sistema, incluida la alimentación en espera, durante 10 segundos.



Precaución Si quita los cables de alimentación del sistema antes de que se complete el apagado correcto, el disco puede dañarse.

Botón de restablecimiento de fábrica

El chasis tiene un botón de restablecimiento empotrado que restablece el sistema a los valores predeterminados de fábrica. Al presionar el botón durante cinco segundos, se eliminan la configuración actual y los archivos actuales.



Nota Utilice el botón de restablecimiento si se pierden las credenciales actuales y desea inicializar la casilla sin tener acceso a la consola.

Ocurre lo siguiente:

- La NVRAM ROMMON se borra y vuelve a los valores predeterminados.
- Se eliminaron todas las imágenes adicionales; permanece la imagen en ejecución actual.
- Se eliminan los registros de FXOS, los archivos de núcleo, las claves SSH, los certificados, la configuración de FXOS y la configuración de Apache.



Nota Si se pierde la alimentación entre el momento en que presionó el botón de restablecimiento y el momento en que se completa el proceso de restablecimiento, el proceso se detiene y debe presionar el botón nuevamente después de que el sistema se vuelve a encender.

Especificaciones de hardware

Módulos de fuente de alimentación

Secure Firewall de la serie 6100 admite dos módulos de fuente de alimentación para que esté disponible la protección de redundancia de la fuente de alimentación doble. Si se orientan hacia la parte posterior del chasis, los módulos de fuente de alimentación están numerados de arriba abajo: PSU-1 y PSU-2.

El módulo de la fuente de alimentación tiene capacidad de intercambio con el sistema activo.



Nota Después de desconectar la alimentación del chasis desenchufando el cable de alimentación, espere al menos 10 segundos antes de volver a conectar la alimentación. Es necesario mantener apagado el sistema, incluida la alimentación en espera, durante 10 segundos.



Atención Asegúrese de que una fuente de alimentación esté siempre activa.

La fuente de alimentación CSF6100-PWR-AC es de entrada triple, CA (línea baja), HVAC (línea alta) y HVDC. Los módulos de fuente de alimentación doble pueden proporcionar hasta 3000 W cada uno en todo

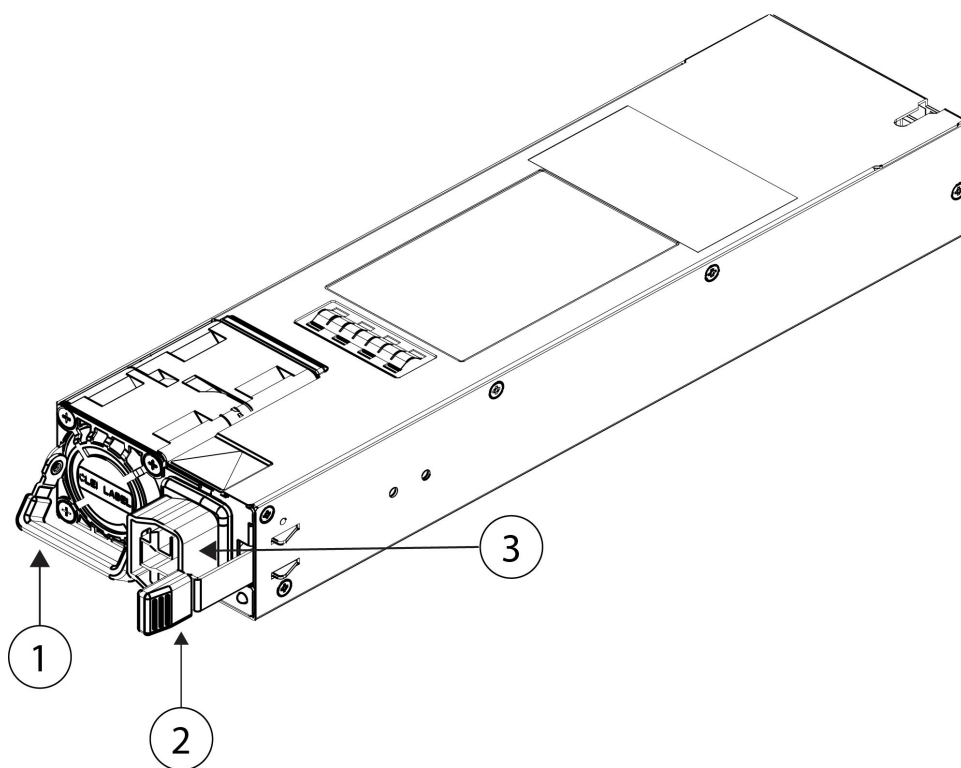
el rango de tensión de entrada (220 V CA). La carga se comparte cuando ambos módulos de fuente de alimentación están enchufados y funcionando al mismo tiempo.

El módulo de fuente de alimentación de HVAC/HVDC puede funcionar con una entrada de 110 V CA (línea baja), pero la potencia de salida se reduce a la mitad (1500 W cada una). Con dos módulos de fuente de alimentación instalados, el sistema tiene una capacidad de consumo de 3000 W, pero la redundancia no está disponible.



Nota El sistema no consume más de la capacidad de un módulo de fuente de alimentación, por lo que siempre funciona en modo de redundancia completa cuando están instalados dos módulos de fuente de alimentación.

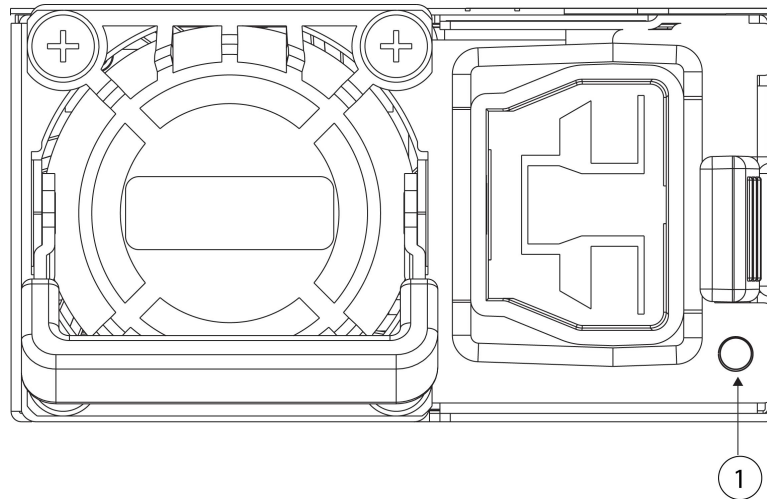
Figura 6: Módulo de fuente de alimentación



1	Manija	2	Ficha de lanzamiento
3	Conector del cable de alimentación		—

En la siguiente figura, se muestra el LED de fuente de alimentación bicolor en el módulo de fuente de alimentación.

Figura 7: LED de los módulos de la fuente de alimentación



1	<p>LED de la fuente de alimentación:</p> <ul style="list-style-type: none"> • Verde: modo activo • Verde, intermitente: modo de espera • Verde, intermitente: proceso de carga de arranque • Ámbar: no hay alimentación de CA, pero el otro módulo de fuente de alimentación del sistema está en funcionamiento • Ámbar, intermitente: evento de advertencia (alta temperatura o falla del ventilador) • Apagado: sin alimentación de entrada
----------	---

Módulos de ventiladores

Secure Firewall de la serie 6100 tiene cuatro módulos de ventilador axial de rotor doble. Cuando falla un ventilador, los otros módulos de ventilador giran a la velocidad máxima para que el sistema siga funcionando. Los módulos de ventilador tienen capacidad de intercambio con el sistema activo y se instalan en la parte posterior del chasis. Están etiquetados desde FAN-1 hasta FAN-4 de izquierda a derecha en la parte posterior del chasis.

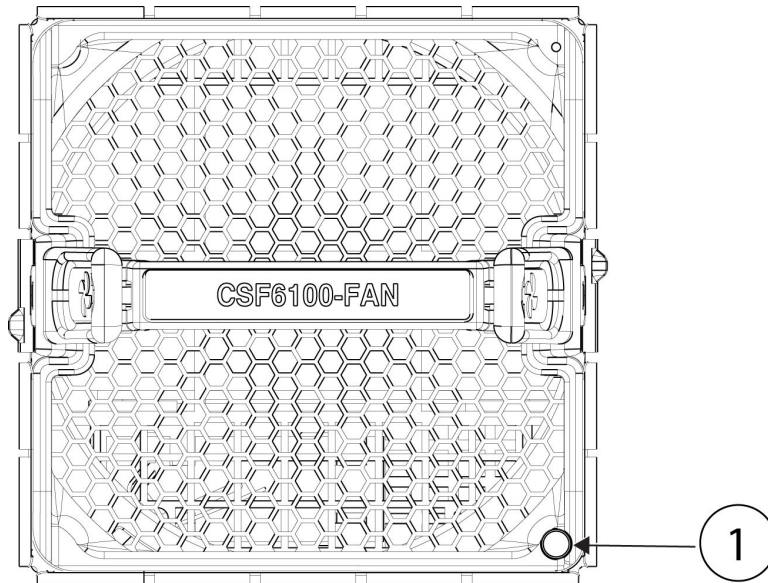


Precaución

Si falla un módulo de ventilador, quítelo del chasis y reemplácelo en 30 segundos. Después de 30 segundos, la temperatura de la CPU puede superar la temperatura de funcionamiento, lo que puede reducir el rendimiento. Consulte [Quite y reemplace el módulo de ventilador](#) si desea conocer el procedimiento para quitar y reemplazar el módulo de ventilador.

En la siguiente imagen, se muestra la ubicación del LED del ventilador en el módulo de ventilador.

Figura 8: LED del módulo de ventilador



1	LED de dos colores (verde y amarillo)
----------	---------------------------------------

El módulo de ventilador tiene un LED de dos colores que se encuentra en la esquina superior izquierda del ventilador.

- Apagado: no hay alimentación o el sistema se está encendiendo.
- Verde: los ventiladores funcionan con normalidad. Después de conectar la alimentación, puede tardar hasta un minuto en volverse verde.
- Amarillo intermitente: una o más RPM del rotor del ventilador no son normales. Se requiere atención inmediata.
- Amarillo: uno o más rotores de ventiladores han fallado. El sistema puede continuar funcionando normalmente, pero los ventiladores requieren mantenimiento.

Más información

- Consulte [Números de ID del producto](#) para obtener una lista de los PID asociados con los ventiladores de Secure Firewall de la serie 6100.
- Consulte [Quite y reemplace el módulo de ventilador](#) si desea conocer el procedimiento para quitar y reemplazar los módulos de ventilador.

SSD

Secure Firewall de la serie 6100 tiene dos ranuras para SSD, cada una de las cuales contiene una SSD de memoria no volátil exprés (NVMe, Non-Volatile Memory Express). De manera predeterminada, Secure Firewall de la serie 6160 se envía con dos SSD de 3,6 TB instalados en la ranura 1 y la ranura 2. Secure Firewall 6170 se envía con dos SSD de 7,2 TB instalados en la ranura 1 y la ranura 2. El software RAID1 ya se envía configurado.

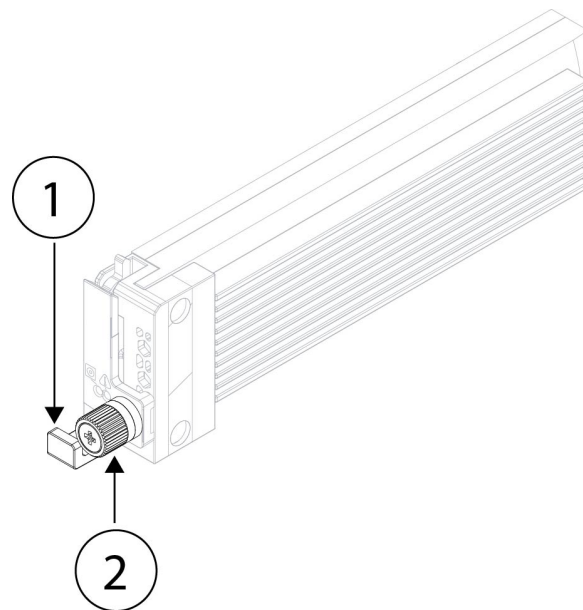
Se admite el intercambio con el sistema activo. Puede intercambiar SSD sin apagar el chasis. Sin embargo, antes de intercambiar SSD con el sistema activo, debe emitir el comando **raid remove-Secure local-disk 1|2** para preparar la SSD para su extracción. Este comando conserva los datos en la SSD. Después de extraer y reemplazar la SSD, debe volver a agregarla a la configuración de RAID1 con el comando **raid add local-disk 1|2**. Consulte la guía de configuración si desea conocer los procedimientos para quitar una SSD de manera segura.



Precaución El comando **raid remove-Secure local disk** borra de forma segura los datos de la SSD especificados.

Los identificadores de la unidad de SSD son `disco0:` y `disco1:`.

Figura 9: SSD



1	Ficha de liberación de SSD	2	Tornillo cautivo
---	----------------------------	---	------------------

Puesta a tierra del chasis



Nota Es necesario conectar el chasis a tierra, incluso si el rack ya está conectado. Se proporciona un kit de puesta a tierra para conectar un terminal de puesta a tierra. El terminal de puesta a tierra debe estar enumerado en un laboratorio de pruebas reconocido a nivel nacional (NRTL). Además, se debe utilizar un conductor de cobre (cables) que cumpla con los códigos locales para la ampacidad.

La placa de puesta a tierra se encuentra en el lado izquierdo del chasis cuando se orienta hacia el panel posterior con las fuentes de alimentación y los ventiladores. Puede conectar un terminal de puesta a tierra con un cable que proporcione.

Requisitos de instalación de terminales de puesta a tierra

Necesita los siguientes elementos:

- Herramienta de alambre
- Tenaza engarzadora
- Cable de puesta a tierra
- Necesita los siguientes elementos del kit de accesorios:
 - Un terminal de puesta a tierra (#6AWG de 0,25 pulgadas)
 - Dos tornillos de cabeza semiesférica de ¼-20 x 0,297 pulgadas
 - Dos arandelas de 0,469 pulgadas de diámetro exterior, 0,261 pulgadas de diámetro interior y 0,025 pulgadas de espesor

Advertencias de seguridad

Tenga en cuenta las siguientes advertencias:



Advertencia

This equipment must be grounded. To reduce the risk of electric shock, never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.



Advertencia

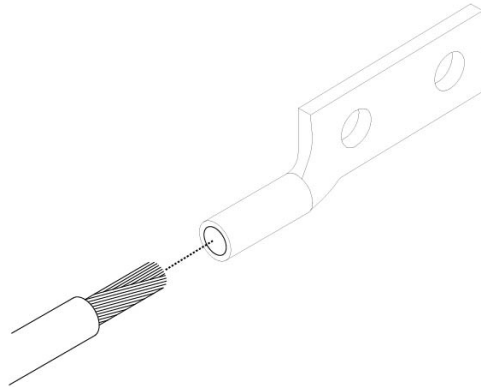
To reduce risk of electric shock, when installing or replacing the unit, the ground connection must always be made first and disconnected last.

If your unit has modules, secure them with the provided screws.

Procedimiento

-
- Paso 1** Utilice una herramienta pelacables para quitar aproximadamente 0,75 pulgadas (19 mm) de la cubierta del extremo del cable de conexión a tierra.
- Paso 2** Inserte el extremo pelado del cable de conexión a tierra en el extremo abierto del terminal de puesta a tierra.

Figura 10: Inserte el cable en el terminal de puesta a tierra

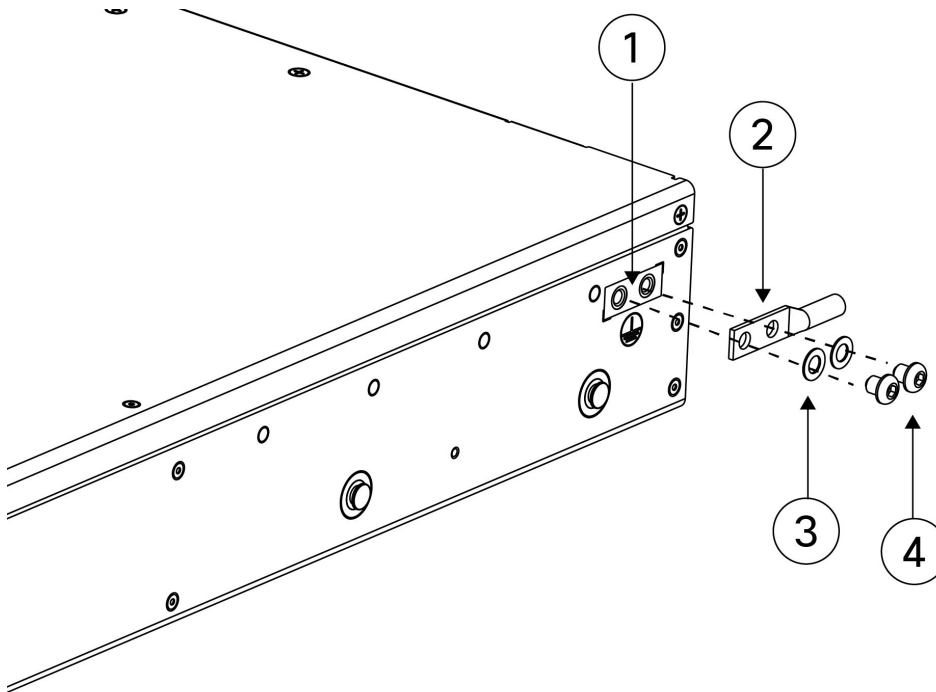


Paso 3 Use la herramienta de ondulación para apretar el cable de conexión a tierra al terminal de puesta a tierra.

Paso 4 Quite la etiqueta autoadhesiva del terminal de puesta a tierra del chasis.

Paso 5 Coloque el terminal de puesta a tierra contra la placa de puesta a tierra en el lado izquierdo del chasis de manera que haya contacto sólido de metal a metal e inserte los dos tornillos de cabeza semiesférica de 1/4-20 x 0,297 pulgadas en la placa de puesta a tierra.

Figura 11: Coloque el terminal de puesta a tierra



1	Descarga a tierra	2	Dos arandelas de bloqueo internas
3	Lado izquierdo del chasis orientado hacia el panel posterior	4	Dos tornillos de cabeza semiesférica de 1/4-20 x 0,297 pulgadas

5	Terminal de puesta a tierra		—
---	-----------------------------	--	---

Paso 6 Asegúrese de que el terminal y el cable no interfieran con los otros equipos.

Paso 7 Prepare el extremo opuesto del cable de conexión a tierra y conéctelo a la descarga a tierra correspondiente del sitio para garantizar la correcta conexión a tierra del switch.

Qué hacer a continuación

Instale los cables según la configuración de software predeterminada como se describe en las [Guías de primeros pasos](#).

Colocación

Este equipo está diseñado para uso industrial y comercial en entornos libres de riesgos para la salud y la seguridad. Se permite el funcionamiento sin supervisión continua. La instalación y el mantenimiento del equipo deben estar a cargo de personal debidamente calificado con los conocimientos y las habilidades suficientes.

Producto de clase A

Este producto puede causar interferencias de radio en un entorno doméstico, en cuyo caso puede ser necesario que el usuario tome las medidas adecuadas.

Almacenamiento, transporte, venta y eliminación

Almacene el equipo en el interior en su embalaje original.

- Rango de temperatura de almacenamiento (cuando está apagado): -40 °C a 65 °C
- Rango de humedad relativa (cuando está apagado): 5 % a 95 % sin condensación

Transporte el equipo en su embalaje original dentro de vehículos cerrados en cualquier medio de transporte.

- Rango de temperatura de transporte: -40 °C a 65 °C
- Rango de humedad relativa: 5 % a 95 % sin condensación

Los términos y condiciones en los que se vende el equipo se rigen por los contratos entre Cisco o los partners autorizados de Cisco y los compradores de los equipos.

La eliminación del equipo en el fin de la vida útil debe realizarse en cumplimiento de todas las leyes y normativas nacionales aplicables.

Qué hacer si el equipo funciona mal

Si experimenta problemas de funcionamiento del equipo o desea presentar un reclamo sobre la calidad, comuníquese con su proveedor de equipos.

También puede encontrar información sobre el soporte técnico de Cisco en su sitio web oficial:

https://www.cisco.com/c/es_mx/index.html

La garantía del fabricante establece que el equipo cumple con las especificaciones de la etiqueta siempre que se haya almacenado, transportado, instalado y operado según la documentación técnica asociada.

La garantía y el soporte de servicio no se aplican al equipo en los siguientes casos:

- Si ha sufrido cambios, modificaciones, manejo incorrecto, destrucción o daños debido a cualquiera de las siguientes condiciones:
 - Causas naturales
 - Exposición ambiental
 - No tomar las medidas requeridas
 - Negligencia, actos intencionales o uso indebido
 - Uso para fines distintos a los especificados en la documentación correspondiente
 - Acto u omisión de un tercero
 - Signos de haber sido sometido a fuego, agua, sustancias químicas, incluyendo pero no limitado a la aplicación de pintura y otros tipos de revestimientos
 - Reparación o modificaciones internas no autorizadas
 - Daño mecánico
 - Signos de entrada de objetos extraños, líquidos o insectos
 - Daños causados por el incumplimiento de las regulaciones técnicas existentes, las normas estatales, las regulaciones relacionadas con el funcionamiento del hardware en una red de comunicaciones pública y otros requisitos oficiales aplicables para los parámetros de redes de alimentación, telecomunicaciones y cable, así como otros factores externos similares.

Consulte la tabla a continuación para obtener instrucciones sobre cómo encontrar la fecha de fabricación para cada modelo.

Contenido del modelo	Fecha de fabricación
CSF-6160 CSF-6170	La semana de fabricación está codificada dentro del número de serie estándar de Cisco de 11 caracteres que tiene el formato LLLYYWSSSS, en el cual: LLL es el código de ubicación alfanumérico del proveedor en Base 34 YYWW es la concatenación del código decimal del año y el número de la semana SSSS es el número de serie secuencial alfanumérico en Base 34

Información adicional

Para obtener instrucciones de instalación más detalladas, consulte las guías de instalación en el sitio web oficial de Cisco:

<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/6100/fw-6100-install.html>

<https://www.cisco.com/c/en/us/support/security/secure-firewall-6100-series/series.html>

Acerca de la traducción

Es posible que Cisco proporcione traducciones de este contenido al idioma local en algunas ubicaciones. Tenga en cuenta que las traducciones se ofrecen únicamente con fines informativos y, si hubiera alguna discrepancia, prevalecerá la versión en inglés del contenido.