




AUTÓMATAS PROGRAMABLES

Guía de ciberseguridad



FP-Industry 4.0 Communicator
(FP-I4C)

Responsabilidad y copyright

Este manual y todo su contenido están protegidos mediante copyright. No está permitida la copia total o parcial de este manual sin el consentimiento previo de Panasonic Electric Works Europe AG (PEWEU).

PEWEU sigue una política de mejora continua del diseño y funcionalidad de sus productos. Por lo tanto, se reserva el derecho de modificar el manual o el producto sin previo aviso. PEWEU no se hace responsable de posibles daños producidos como consecuencia de algún defecto del producto o de la documentación, incluso si se advierte de la posibilidad de dichos daños.

Para solicitar cualquier tipo de soporte técnico póngase en contacto con la delegación de Panasonic en su zona.

Panasonic Electric Works Europe AG (PEWEU)

Caroline-Herschel-Strasse 100

85521 Ottobrunn, Alemania

Tel: +49 89 45 354-1000

Tabla de contenidos

Responsabilidad y copyright.....	2
1 Acerca de este documento	4
2 Política de seguridad de los productos Panasonic.....	4
3 Configuración por defecto del módulo FP-I4C	4
4 Escenarios de riesgos potenciales.....	6
5 Medidas de seguridad generales	7
6 Buenas prácticas para proteger el módulo FP-I4C	8
6.1 Ajustes del Sistema	8
6.1.1 Protección por contraseña	8
6.1.2 Configuración del Firewall	8
6.1.3 Archivos de Log y funcionalidad de depuración SSH	9
6.2 Ajustes de la Aplicación.....	9
7 FAQ.....	11
8 Lista de verificación de la configuración de seguridad	12
Hotline de Panasonic	13
Histórico de cambios	14

1 Acerca de este documento

A medida que aumenta la digitalización y la interconexión de redes, aparecen nuevos y más complejos riesgos internos y externos de ciberseguridad.

El BSI (German Federal Office for Information Security), por ejemplo, publicó un informe con las 10 principales amenazas, definiendo las reglas y recomendaciones para los equipos de red en los sistemas de control industrial (ICS):

- Infiltración de malware a través de dispositivos USB y hardware externo
- Infección por malware vía Internet e Intranet
- Fallos humanos y sabotajes
- Vulnerabilidad de seguridad de los componentes en la Extranet y en la nube
- Ingeniería social y phishing
- Ataques de Denegación de Servicio (DDoS)
- Componentes de control conectados a Internet
- Intrusión vía acceso remoto
- Fallos técnicos y de fuerza mayor
- Vulnerabilidad de seguridad de smartphones en entornos de producción

Fuente: <https://www.bsi.bund.de/ICS>

Este documento contiene la información necesaria del módulo FP-I4C para su integración segura en la red y para su protección de los riesgos de seguridad.

2 Política de seguridad de los productos Panasonic

Los productos y servicios de Panasonic siempre están en continua mejora. El desarrollo de nuestros productos sigue estrictamente las directivas de seguridad corporativas que incluyen un test exhaustivo antes del envío de los productos desde fábrica. La política de seguridad de Panasonic se basa en las guías internacionales recogidas en la IEC 62443 y ISO/IEC 27001.

El [Panasonic Product Security Incident Response Team](#) (Panasonic PSIRT) es el centro de coordinación de vulnerabilidades asociadas a los productos de Panasonic.

3 Configuración por defecto del módulo FP-I4C

La funcionalidad de red integrada en el módulo de comunicaciones FP-I4C representa en sí misma un riesgo de seguridad. Para eliminar o minimizar este riesgo, se debe personalizar y reajustar la configuración de red por defecto.

- La contraseña por defecto permite la configuración del módulo FP-I4C. Se recomienda modificar esta contraseña una vez se acceda al equipo por primera vez.
- Los puertos ETH0 y ETH1 tienen configuraciones diferentes: ETH0 está configurado como cliente DHCP y el puerto ETH1 tiene una IP fija: 192.168.0.1.
- Por defecto, el módulo se suministra con los siguientes puertos abiertos y escuchando:

Nº de puerto	Protocolo	Función
80, 8081, 443	TCP/IP	Se utiliza en la página de configuración y en las páginas web de usuario

N° de puerto	Protocolo	Función
53	TCP/IP	Se utiliza para los servicios DNS
990-991	UDP	Se utiliza para el descubrimiento de dispositivos de red por difusión
21	TCP/IP	Tiempo de ejecución y gestión del proyecto (FTP modo pasivo: 16384-17407/TCP, 18756-18759/TCP)
16384-17407, 18756-18759	TCP/IP	FTP Modo pasivo

- El equipo se suministra de fábrica con todas las funcionalidades y servicios que puedan representar un riesgo de seguridad, deshabilitados.

En `Ip/machine_config/#/services` se puede ver un listado de los servicios.

Servicio	Riesgo de seguridad
Scripts autoejecutables	Programas que se ejecutan desde una unidad de almacenamiento externa p.ej. desde una memoria USB.
Demonio Avahi	Abre el puerto 5353 (se utiliza para recopilar información y encontrar características)
Servicios en la nube	P.ej., una configuración de un servidor OpenVPN utilizada con anterioridad
Servidor DHCP	Abre los puertos 67, 68
Servidor SNMP	Abre los puertos 161, 10161 (para la recopilación de información)
Servidor SSH	Abre el puerto 22 (Inicio de sesión con credenciales de administrador y ejecución de comandos)
Servidor VNC	Abre el puerto 5900 (Página web y control de dispositivos)

- Por defecto, el firewall del módulo FP-I4C (`Ip/machine_config/#/services`) está deshabilitado.
- El módulo FP-I4C registra en los archivos de log, los datos e información relacionada con un funcionamiento atípico del dispositivo. Estos archivos se almacenan en el módulo y se pueden descargar accediendo con credenciales de administrador.

Nota:

Utilizar el firewall para cerrar cualquier puerto que no se utilice, pero asegurarse de mantener abiertos los puertos Ethernet 80 y 443 en la configuración del firewall. Si se cierran estos puertos, se denegará permanentemente el acceso a la página de configuración del sistema.

Temas relacionados:

[Configuración del Firewall](#)

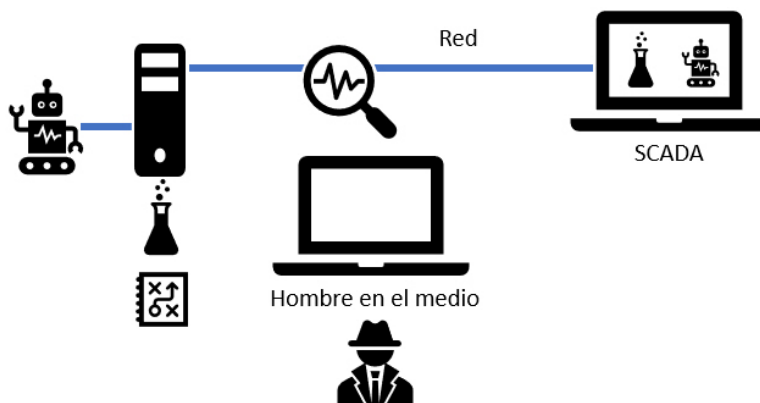
4 Escenarios de riesgos potenciales

Para una mejor comprensión y toma de conciencia de los riesgos potenciales de seguridad, a continuación se exponen algunos ejemplos típicos de ciberamenazas.

- Captura de datos

Hoy en día existen multitud de herramientas para leer el tráfico de red, incluido el nombre de usuario, las contraseñas y otros datos sensibles como datos de proceso, recetas, etc.

Especialmente si el tráfico de red no está encriptado, se convierte en un objetivo fácil para la captura de información disponible en la red por parte de espías.

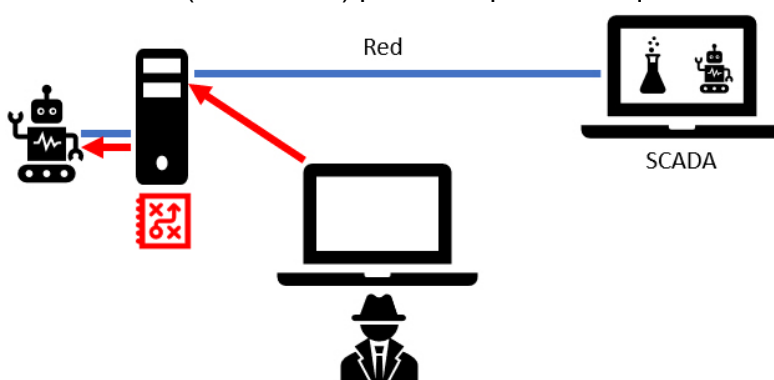


Contramedidas:

Nunca utilizar, para la transmisión de datos sensibles, protocolos FTP o Telnet fuera de una red encapsulada. Estos protocolos suponen un alto riesgo de seguridad ya que los nombres de usuario y las contraseñas se transmiten en texto plano.

- Acceso no autorizado a los sistemas de control

Conociendo las credenciales o el protocolo utilizado, se pueden provocar fallos o sabotajes en las máquinas. Además, los dispositivos se pueden quedar secuestrados en una bonet (red de bots) para manipular o bloquear a otros dispositivos.

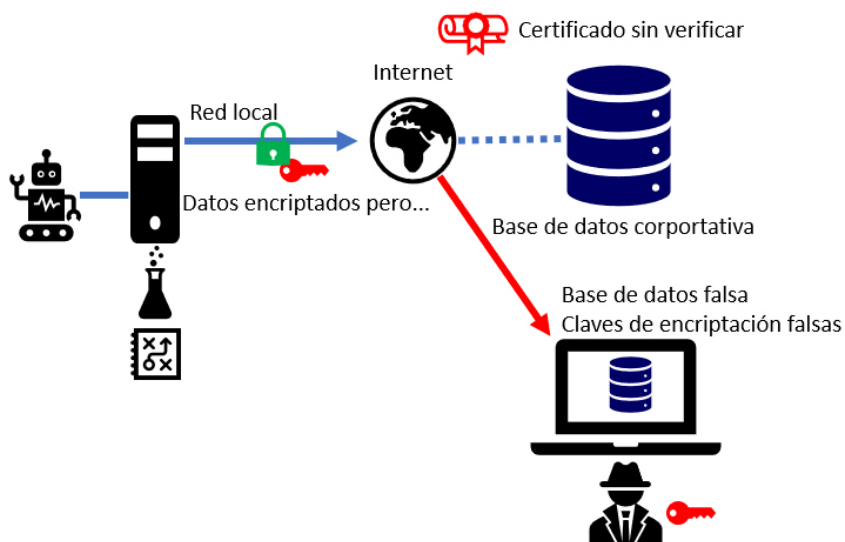


Contramedidas:

No permitir el acceso o el control desde equipos de terceros.

- Suplantación de identidad

Las conexiones con páginas Web cuyas identidades no están verificadas por una autoridad de certificación pueden ser peligrosas puesto que son susceptibles de una suplantación de identidad y pueden redirigir la comunicación. De esta forma, los atacantes pueden obtener información sensible (p. ej. usuarios, contraseñas, datos del proceso, o recetas). Con esa información se pueden causar daños graves manipulando las máquinas.



Contramiedas:

Siempre utilizar certificados para autenticar la identidad del servidor al que se pretende acceder.

5 Medidas de seguridad generales

La implementación de las medidas necesarias para proteger la red es crucial para el mantenimiento de la misma y para garantizar un tráfico seguro.

Puesto que este equipo se utiliza conectado a una red, se advierte de los siguientes riesgos de seguridad.

- Fuga o robo de datos a través del equipo.
- Uso de este equipo por personas malintencionadas para realizar operaciones ilegales.
- Interferencia o anulación de este equipo por parte de personas con intenciones maliciosas.
- Es responsabilidad del usuario tomar las precauciones necesarias como las descritas abajo para proteger la red de los riesgos de seguridad.
- Si se conecta este módulo a una red donde hay conectados ordenadores personales, asegurarse de que el sistema no se infecte por virus informáticos u otras entidades maliciosas (instalar un antivirus actualizado, programas antispyware, etc.).
- Utilizar este equipo en un entorno que tenga una LAN, una VPN (red privada virtual) o una red dedicada.
- Utilizar este equipo en un entorno al que solamente pueda acceder el personal con los privilegios de acceso legítimos.
- Utilizar este equipo y otros dispositivos conectados a través de la red como un PC, una tableta, etc. solamente si se han implementado las medidas de protección que garanticen la seguridad del sistema.
- No utilizar este equipo en lugares donde los cables o el propio equipo puedan ser dañados o inutilizados por personas con intenciones maliciosas.

Tener en cuenta que la configuración incorrecta de la conexión en la LAN existente, podría causar un funcionamiento incorrecto de los dispositivos de red. Consultar al administrador de la red antes de realizar la conexión.

6 Buenas prácticas para proteger el módulo FP-I4C

Se pueden minimizar los riesgos de seguridad implementando las siguientes medidas preventivas y realizando la configuración adecuada del sistema y de las aplicaciones. Utilizar la lista de verificación que se proporciona en esta guía para garantizar que se toman todas las medidas necesarias para securizar el módulo FP-I4C.

Temas relacionados:

[Lista de verificación de la configuración de seguridad](#)

6.1 Ajustes del Sistema

Ir a “System Settings” (Ajustes del sistema) (IP/machine_config) para configurar la contraseña y el firewall, para acceder a los archivos de log y para usar la funcionalidad de depuración SSH.

6.1.1 Protección por contraseña

El módulo se suministra con una contraseña de fábrica. Se debe modificar la contraseña por defecto por una contraseña robusta que incluya letras mayúsculas, minúsculas, números y caracteres especiales (excepto espacios en blanco).

Utilizar una contraseña diferente para el servidor FTP en HMWIN Studio y para el módulo FP-I4C.

6.1.2 Configuración del Firewall

Utilizar el firewall (IP/machine_config/#/services) para cerrar cualquier puerto que no se utilice.

Cuando se habilita el “Firewall Service” (Servicio Firewall) (IP/machine_config/#/services), se habilitan todas las funcionalidades vinculadas a las configuraciones y los puertos respectivos. Deshabilitar los servicios y puertos no utilizados o denegar el acceso a interfaces dedicadas (ETH0 o ETH1).

Nota:

Comprobar que “Web Server – HTTP” (Servidor Web – HTTP) y “Web Server – HTTPS” (Servidor Web – HTTPS) están habilitados y que los puertos Ethernet 80 y 443 están abiertos. Si se cierran estos puertos, se denegará permanentemente el acceso a la página de configuración del sistema.

Ejemplo de configuración del Firewall:

Nombre	Interfaz	Puerto o rango	Protocolo	Obligatorio
Servidor Web - HTTP (necesario para la configuración)	Cualquiera	80	TCP/IP	✓
Servidor Web - HTTPS (necesario para la configuración)	Cualquiera	443	TCP/IP	✓
Descubrimiento de dispositivos de red	Cualquiera	990–991	UDP	✓
Puerto comando FTP, necesario para operar con HMWIN Studio	Cualquiera	21	TCP/IP	
Modo FTP pasivo, necesario para operar con HMWIN Studio	Cualquiera	18756–18760	TCP/IP	

Nombre	Interfaz	Puerto o rango	Protocolo	Obligatorio
Servidor SSH	Cualquiera	22	TCP/IP	
Servidor VNC	Cualquiera	5900	TCP/IP	
Servidor DHCP	Cualquiera	67	UDP	
Servidor SNMP	Cualquiera	161	UDP	
Puertos PEW	Cualquiera	9094–9097	TCP/IP	

6.1.3 Archivos de Log y funcionalidad de depuración SSH

Sirven para detectar operaciones atípicas. Solo se pueden utilizar con credenciales de administrador.

6.2 Ajustes de la Aplicación

Ir a “Application Settings” (Ajustes de la aplicación) (IP/fp_config) para realizar la configuración específica de la aplicación en la página de configuración correspondiente.

- Configuración del puerto

Se pueden configurar los puertos TCP que están escuchando en la página “Port” (Puerto) de la página de configuración del FP-I4C. Puesto que la mayoría de los protocolos de comunicación industriales no proporcionan protección de acceso, utilizar estos puertos solamente para la comunicación interna dentro de una red encapsulada.

Implementar además, las medidas adicionales necesarias para minimizar los riesgos de un ataque por control no autorizado al PLC conectado:

- Eliminar la configuración de los puertos que no estén en uso.
- Siempre que sea posible, otorgar solamente permisos de solo lectura a los datos del sistema.
- Bloquear la transmisión de datos para todos los datos internos del PLC.
- Minimizar el número de registros de control (como valores de preselección o comandos) a los estrictamente necesarios para las operaciones de escritura.
- Definir las direcciones IP que están permitidas en la comunicación. Para la comunicación con dispositivos internos (p. ej. acceso vía página web), asignar la dirección IP 127.0.0.1 (local host).
- Cualquier PLC conectado debería tener su propia protección de acceso de forma que el programa del PLC en funcionamiento no pueda ser modificado.

- Servicio de histórico de datos (data logger)

El histórico de datos (data logger) no abre ningún puerto de escucha. Los datos se recopilan a través de los puertos RS232, RS485, USB, y conexiones Ethernet TCP cliente. Ninguno de los protocolos soportados en la recopilación de datos usa encriptación.

Por esta razón, cuando se recopilan datos a través de redes públicas, siempre se debe utilizar una solución VPN.

- Servicio MQTTs

El protocolo IoT (Internet of Things) soporta comunicación en texto plano y encriptación así como control de acceso adicional.

- Cuando se transmiten datos a través de redes públicas, utilizar certificados AC

raíz para verificar la identidad del broker/servidor.

- Utilizar conexiones encriptadas entre el módulo FP-I4C y el broker.

Puesto que los datos no están encriptados dentro del broker, se podrían reenviar datos sensibles a través de conexiones en texto plano (no encriptadas). Por este motivo, el broker tiene que estar protegido contra accesos no autorizados mediante un control de acceso basado en roles.

- Cliente FTP

El cliente FTP establece conexiones con servidores FTP para la transmisión de archivos. En las transmisiones FTP estándar, las credenciales del usuario no están encriptadas. Se recomienda utilizar solamente transmisiones FTPS. Si se transmiten datos a través de redes públicas, utilizar adicionalmente certificados AC raíz.

Si el servidor FTP rechaza la conexión encriptada, el handshake falla y finaliza la transmisión.

- Servicio de Scripts

Consiste en un pequeño intérprete encapsulado, con funcionalidad limitada, creado para proporcionar información del dispositivo al PLC conectado.

- Para modificar los scripts es necesario estar autenticado con credenciales de administrador.
- No se ha implementado ningún script para abrir puertos de escucha.
- Se ha implementado una función para la transmisión de datos como cliente TCP.

- Servicio Cliente SQL

El cliente SQL permite la comunicación con bases de datos. Normalmente, las bases de datos usan su propia autenticación encriptada. Se debe garantizar la seguridad de la infraestructura de la base de datos, ya que pueden contener datos sensibles.

Utilizar el cliente SQL únicamente para la conexión con partes no sensibles de la infraestructura de la base de datos.

- Servicio IEC60870

El protocolo de telecontrol IEC60870 utiliza un puerto de escucha sin protección de acceso. Utilizar este protocolo exclusivamente dentro de redes encapsuladas.

Existe un alto riesgo de perder el control del PLC conectado, de la máquina, o de la subestación. Para minimizar este riesgo, se recomienda tomar las siguientes medidas:

- Especificar las direcciones IP de emparejamiento permitidas.
- Utilizar túneles VPN encriptados.
- Todos los comandos y valores de preselección se gestionan en el PLC. Los telegramas entrantes primero se procesan en el FP-I4C y después en el PLC. Se debe implementar un procedimiento en el PLC para identificar instrucciones maliciosas.
- Utilizar una marca de tiempo con todos los comandos en la dirección de control.
- Todos los PLCs conectados deberían tener una protección de acceso que evite la modificación no autorizada del programa en ejecución.

- Cliente HTTP

El cliente HTTP funciona como un navegador para recuperar y enviar información al servidor HTTP (computación en la nube).

- Cuando se transmiten datos a través de redes públicas, utilizar siempre certificados AC raíz para verificar que el módulo FP-I4C está conectado al servidor HTTP correcto.

- Utilizar conexiones encriptadas entre el módulo FP-I4C y el Servidor HTTP.
- Cliente de correo electrónico

El cliente de correo electrónico permite la conexión con un servidor de correo electrónico. Este servidor de correo debería proporcionar comunicaciones seguras y encriptadas y gestionar correctamente los privilegios de acceso de los usuarios. El cliente de correo electrónico puede enviar mensajes con archivos adjuntos siempre que no sean ejecutables.

 - Cuando se transmiten datos a través de redes públicas, utilizar siempre certificados AC raíz para verificar que el módulo FP-I4C está conectado al servidor de correo correcto.
 - Utilizar conexiones encriptadas entre el módulo FP-I4C y el servidor de correo electrónico en el proceso de Inicio de sesión.
- Servicio API REST

El servicio API REST funciona como un servidor HTTP que proporciona información y permite el control del PLC conectado.

Para minimizar los riesgos de seguridad, implementar la siguiente configuración en la página "Port" (Puerto):

 - Siempre que sea posible, otorgar solamente permisos de solo lectura a los datos del sistema.
 - Bloquear la transmisión de datos para todos los datos internos del PLC.
 - Minimizar el número de registros de control (como valores de preselección o comandos) a los estrictamente necesarios para las operaciones de escritura.
 - Definir las direcciones IP que están permitidas en la comunicación.
 - Utilizar conexiones encriptadas entre el módulo FP-I4C (como servidor HTTPS) y el cliente.

7 FAQ

1. ¿Se pueden obtener parches de seguridad y actualizaciones del firmware?
Se pueden descargar las últimas actualizaciones desde la página web de Panasonic: [Downloads | Panasonic Industry Europe GmbH](#)
2. ¿El módulo dispone de algún tipo de puerta trasera?
No. El módulo no tiene ninguna puerta trasera. Si se pierde la contraseña, no existe ninguna forma de recuperar la configuración.
3. ¿El módulo puede llamar a algún servidor de Panasonic?
Con la configuración por defecto, no existe ningún proceso que llame automáticamente a un servidor de Panasonic.

8 Lista de verificación de la configuración de seguridad

Utilizar esta lista de verificación para garantizar que se toman todas las medidas necesarias para securizar el módulo FP-I4C. Marcar todos los elementos de la lista que estén implementados. Al final de la lista hay espacio para añadir elementos adicionales.

Hecho	Riesgo ¹⁾	Área	Página de configuración	Acción
	Alto	Contraseñas (administrador, usuario)	IP/machine_config/#!/authentication	Modificar las contraseñas de administrador y de los usuarios
	Alto	Servicio: Scripts autoejecutables	IP/machine_config/#!/services	Deshabilitar
	Alto	Servicio: Servidor SSH	IP/machine_config/#!/services	Deshabilitar si no se necesita
	Bajo	Demonio Avahi	IP/machine_config/#!/services	Deshabilitar si no se necesita
	Bajo	Servicios en la nube	IP/machine_config/#!/services	Deshabilitar si no se necesita
	Bajo	Servidor DHCP	IP/machine_config/#!/services	Deshabilitar si no se necesita
	Bajo	Servicio VNC	IP/machine_config/#!/services	Deshabilitar si no se necesita
	Bajo	Firewall	IP/machine_config/#!/services	Habilitar y personalizar la configuración
	Alto	Contraseñas HMWIN (al menos de administrador, usuario, log) ²⁾	HMWIN Studio Project/Configuration/Security	Modificar las contraseñas de administrador y de usuario
	Medio	Funcionalidad ²⁾ HMWIN OPC UA	HMWIN Studio Project/Configuration/Security	Comprobar el acceso al servidor
	Alto	Configuración del puerto	IP/fp_config → "Port" (Puerto)	Configurar el acceso al área de datos (lectura, escritura, o bloque)
	Medio	Servicio MQTT	IP/fp_config → "MQTT"	Utilizar encriptación y certificados
	Medio	Cliente FTP	IP/fp_config → "FTP Client" (Cliente FTP)	Utilizar encriptación y certificados
	Medio	Cliente HTTP	IP/fp_config → "HTTP Client" (Cliente HTTP)	Utilizar encriptación y certificados
	Medio	Cliente de correo electrónico	IP/fp_config → "Email Client» (Cliente de correo electrónico)	Utilizar encriptación, certificados y contraseña
	Medio	Servicio API REST	IP/fp_config → "REST API"	Deshabilitar "Accept external requests" (Aceptar peticiones externas) si no se utiliza
			IP/fp_config → "Port" (Puerto)	Configurar el acceso al área de datos (lectura o escritura)

¹⁾ El riesgo depende de la aplicación.

²⁾ Si está instalado

Hotline de Panasonic

Si tiene dudas o preguntas que no quedan suficientemente aclaradas en los manuales o en la ayuda Online, póngase en contacto con su oficina de ventas.

Europa

Austria: 02236 / 2 68 46, info.pewat@eu.panasonic.com

Países Bajos: 0499 / 37 27 27, info.pewswe@eu.panasonic.com

Francia: 01 / 60 13 57 57, info.pewswef@eu.panasonic.com

Alemania: 089 / 45 354 2748, plc.peweu@eu.panasonic.com

Irlanda: 01 / 4 60 09 69, info.pewuk@eu.panasonic.com

Italia: 045 / 67 52 711, info.pewit@eu.panasonic.com

Escandinavia: 46 / 8 59 47 66 80, info.pewns@eu.panasonic.com

España: 91 / 3 29 38 75, info.pewes@eu.panasonic.com

Suiza: 041 / 799 70 50, info.pewch@eu.panasonic.com

Reino Unido: 01908 / 23 15 55, info.pewuk@eu.panasonic.com

Norteamérica y Sudamérica

EE.UU.: 1 877 / 624 7872, iasupport@us.panasonic.com

Asia

China: 400-920-9200, <https://industrial.panasonic.cn/ea/>

Corea: +82-2-2052-1050, <http://pidskr.panasonic.co.kr/>

Taiwan: +886-2-2757-1900, <https://industrial.panasonic.com/>

Hong Kong: +852-2306-3128, <https://industrial.panasonic.com/>

Japón: 0120-394-205, <https://industrial.panasonic.com/>

Singapur: +65 / 635 92128, pewapfa@sg.pewg.panasonic.com

Histórico de cambios

Fecha	Descripción
2021.11, versión 1.1	Se ha añadido la sección 2 y se ha modificado el acceso la descripción del acceso de lectura en la sección 6.2
2021.08, versión 1.0	Primera edición