# **PacT** Series

## Master**PacT,** Com**PacT,** Power**PacT**

## Guía de ciberseguridad

**PacT** Series ofrece interruptores e interruptores automáticos de primer nivel

**DOCA0122ES-11**
**09/2025**

www.se.com

# Información legal

La información proporcionada en este documento contiene descripciones generales, características técnicas o recomendaciones relacionadas con productos o soluciones.

Este documento no pretende sustituir a un estudio detallado o un plan de desarrollo o esquemático específico de operaciones o sitios. No debe usarse para determinar la adecuación o la fiabilidad de los productos o las soluciones para aplicaciones de usuario específicas. Es responsabilidad del usuario realizar o solicitar a un experto profesional (integrador, especificador, etc.) que realice análisis de riesgos, evaluación y pruebas adecuados y completos de los productos o las soluciones con respecto a la aplicación o el uso específicos de dichos productos o dichas soluciones.

La marca Schneider Electric y cualquier otra marca comercial de Schneider Electric SE y sus filiales mencionadas en este documento son propiedad de Schneider Electric SE o sus filiales. Todas las otras marcas pueden ser marcas comerciales de sus respectivos propietarios.



Schneider Electric se reserva el derecho de realizar cambios o actualizaciones con respecto a o en el contenido de este documento o con respecto a o en el formato de dicho documento en cualquier momento sin previo aviso.

**En la medida permitida por la ley aplicable, Schneider Electric y sus filiales no asumen ninguna responsabilidad u obligación por cualquier error u omisión en el contenido informativo de este documento o por el uso no previsto o el mal uso del contenido de dicho documento.**

# Tabla de contenido

# Información de seguridad

## Información importante

Lea atentamente estas instrucciones y observe el equipo para familiarizarse con el dispositivo antes de instalarlo, utilizarlo, revisarlo o realizar su mantenimiento. Los mensajes especiales que se ofrecen a continuación pueden aparecer a lo largo de la documentación o en el equipo para advertir de peligros potenciales, o para ofrecer información que aclara o simplifica los distintos procedimientos.

La inclusión de este icono en una etiqueta “Peligro” o “Advertencia” indica que existe un riesgo de descarga eléctrica, que puede provocar lesiones si no se siguen las instrucciones.

Éste es el icono de alerta de seguridad. Se utiliza para advertir de posibles riesgos de lesiones. Observe todos los mensajes que siguen a este icono para evitar posibles lesiones o incluso la muerte.

**⚠ PELIGRO**

**PELIGRO** indica una situación de peligro que, si no se evita, **provocará** lesiones graves o incluso la muerte.

**⚠ ADVERTENCIA**

**ADVERTENCIA** indica una situación de peligro que, si no se evita, **podría provocar** lesiones graves o incluso la muerte.

**⚠ ATENCIÓN**

**ATENCIÓN** indica una situación peligrosa que, si no se evita, **podría provocar** lesiones leves o moderadas.

***AVISO***

***AVISO*** indica una situación potencialmente peligrosa que, si no se evita, **puede provocar** daños en el equipo.

## Tenga en cuenta

La instalación, manejo, puesta en servicio y mantenimiento de equipos eléctricos deberán ser realizados sólo por personal cualificado. Schneider Electric no se hace responsable de ninguna de las consecuencias del uso de este material.

Una persona cualificada es aquella que cuenta con capacidad y conocimientos relativos a la construcción, el funcionamiento y la instalación de equipos eléctricos, y que ha sido formada en materia de seguridad para reconocer y evitar los riesgos que conllevan tales equipos.

# Acerca del documento

## Ámbito del documento

Esta guía proporciona información sobre aspectos de ciberseguridad para interruptores automáticos MasterPacT, ComPacT y PowerPacT con unidades de control y disparo remoto MicroLogic para ayudar a los diseñadores y operadores de sistemas a promover e implementar un entorno de funcionamiento seguro para el producto.

**NOTA:**

- La información relacionada con la nueva generación de interruptores automáticos ComPacT NS y PowerPacT Py R (marcos) de este documento también se aplica a la gama existente de interruptores automáticos ComPact NS y PowerPact Py R (marcos). Se mencionan excepciones siempre que sea aplicable.
- La información relacionada con la nueva generación de interruptores automáticos ComPacT NSX y PowerPacT H-, J-, and L-Frame de este documento también se aplica a la gama existente de interruptores automáticos ComPact NSX y Marcos PowerPact H, J y L. Se mencionan excepciones siempre que sea aplicable.
- Estas nuevas gamas se basan en la misma arquitectura técnica y dimensional que la de la gama existente de interruptores automáticos.

En esta guía no se trata el tema más general de cómo proteger su red de tecnología operativa o su red Ethernet empresarial. Para ver una introducción general a las amenazas de ciberseguridad y cómo afrontarlas, consulte *How Can I Reduce Vulnerability to Cyber Attacks?*.

**NOTA:** En esta guía, el término **seguridad** se utiliza para hacer referencia a la ciberseguridad.

## Campo de aplicación

La información de esta guía se aplica a los siguientes interruptores automáticos:

- Interruptores automáticos MasterPacT MTZ con unidades de control MicroLogic X
- Interruptores automáticos MasterPacT MTZ con unidades de control MicroLogic Active
- Interruptores automáticos MasterPacT NT/NW con unidades de disparo remoto MicroLogic
- Interruptores automáticos ComPacT NS con unidades de disparo remoto MicroLogic
- Interruptores automáticos PowerPacT de marcos P y R con unidades de disparo remoto MicroLogic
- Interruptores automáticos ComPacT NSX con unidades de disparo remoto MicroLogic
- Interruptores automáticos PowerPacT de marcos H, J y L con unidades de disparo remoto MicroLogic

**NOTA:** La información de esta guía también se aplica a las gamas ComPact y PowerPact heredadas.

## Información en línea

Las características de los productos descritos en este documento tienen como objetivo coincidir con las características disponibles en www.se.com. Como parte de nuestra estrategia corporativa de mejora constante, podemos revisar el

contenido con el tiempo con el fin de elaborar documentos más claros y precisos. Si ve una diferencia entre las características de este documento y las características que aparecen en www.se.com, tenga en cuenta que www.se.com contiene la información más reciente.

# Información general sobre ciberseguridad

En los últimos años, el creciente número de equipos y plantas de producción conectados a la red ha aumentado de la mano del potencial de las amenazas cibernéticas, como el acceso no autorizado, violaciones de datos e interrupciones operativas. Por lo tanto, es recomendable considerar todas las medidas de ciberseguridad posibles con el fin de ayudar a proteger los activos y los sistemas de dichas amenazas.

Para mantener sus productos de Schneider Electric seguros y protegidos, es conveniente que implemente las prácticas recomendadas de ciberseguridad que se indican en el documento Cybersecurity Best Practices.

Schneider Electric proporciona información y asistencia adicionales:

- Suscríbase al boletín de seguridad de Schneider Electric .
- Consulta la página web de Cybersecurity Support Portal para:
  - Buscar notificaciones de seguridad.
  - Notificar vulnerabilidades e incidentes.
- Consulta la página web de Schneider Electric Cybersecurity and Data Protection Posture para:
  - Acceder a la perspectiva de ciberseguridad.
  - Obtener más información sobre la ciberseguridad en la academia de ciberseguridad.
  - Explorar los servicios de ciberseguridad de Schneider Electric.

# Información de ciberseguridad relacionada con el producto

**⚠ADVERTENCIA**

**RIESGO POTENCIAL PARA LA DISPONIBILIDAD, LA INTEGRIDAD Y LA CONFIDENCIALIDAD DEL SISTEMA**

- La primera vez que utilice el sistema, cambie los códigos PIN y las contraseñas predeterminados para evitar el acceso no autorizado a la configuración, los controles y la información del dispositivo.
- Desactive los puertos/servicios no utilizados y las cuentas predeterminadas para ayudar a reducir al mínimo los caminos de entrada de posibles ataques.
- Coloque los dispositivos en red tras varias capas de ciberdefensas (como cortafuegos, segmentación de red y protección y detección de intrusiones en red).
- Siga las prácticas recomendadas de ciberseguridad (por ejemplo, privilegio mínimo, separación de tareas) para evitar exposiciones no autorizadas, pérdidas, modificaciones de datos y registros, o interrupciones de los servicios.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

# Datos ambientales

Para obtener más información sobre el cumplimiento de los productos y el ambiente, consulte el Environmental Data Program de Schneider Electric.

# Idiomas disponibles del documento

Este documento está disponible en los siguientes idiomas:

- Inglés (DOCA0122EN), idioma original
- Español (DOCA0122ES)
- Francés (DOCA0122FR)
- Chino (DOCA0122ZH)

# Documentos relacionados para dispositivos IEC

| Título de la documentación | Número de referencia |
|---|---|
| *MasterPacT MTZ - MicroLogic X* | DOCA0102EN<br>DOCA0102ES<br>DOCA0102FR<br>DOCA0102ZH |
| *MasterPacT MTZ - Unidad de control MicroLogic Active - Guía del usuario* | DOCA0265EN<br>DOCA0265ES<br>DOCA0265ZH |
| *ComPacT NSX – Unidades de disparo remoto electrónicas Micrologic 5/6/7 - Guía del usuario* | DOCA0188EN<br>DOCA0188ES<br>DOCA0188FR<br>DOCA0188ZH |
| *ComPact NSX – Unidades de disparo remoto electrónicas Micrologic 5/6/7 - Guía del usuario* | DOCA0141EN<br>DOCA0141ES<br>DOCA0141FR<br>DOCA0141ZH |
| *Unidades de disparo remoto MasterPacT NT/NW - MicroLogic A y E - Guía del usuario* | 04443724AA (EN)<br>EAV16735 (ES)<br>04443723AA (FR) |
| *Unidades de disparo remoto MasterPacT NT/NW - MicroLogic P - Guía del usuario* | 04443726AA (EN)<br>EAV16736 (ES)<br>04443725AA (FR) |
| *Unidades de disparo remoto MasterPacT NT/NW - MicroLogic H - Guía del usuario* | 04443728AA (EN)<br>EAV16737 (ES)<br>04443727AA (FR) |
| *ComPacT NS - Unidades de control MicroLogic A/E - Guía del usuario* | DOCA0218EN<br>DOCA0218ES<br>DOCA0218FR<br>DOCA0218ZH |
| *ComPacT NS - Unidades de control MicroLogic P - Guía del usuario* | DOCA0219EN<br>DOCA0219ES<br>DOCA0219FR<br>DOCA0219ZH |
| *Enerlin'X EIFE - Interfaz Ethernet integrada para un interruptor automático MasterPacT MTZ seccionable - Guía del usuario* | DOCA0106EN<br>DOCA0106ES<br>DOCA0106FR<br>DOCA0106ZH |
| *Enerlin'X IFE - Servidor de panel Ethernet - Guía del usuario* | DOCA0084EN<br>DOCA0084ES<br>DOCA0084FR<br>DOCA0084ZH |
| *Enerlin'X IFE - Interfaz Ethernet para un interruptor automático - Guía del usuario* | DOCA0142EN<br>DOCA0142ES<br>DOCA0142FR<br>DOCA0142ZH |

| Título de la documentación | Número de referencia |
|---|---|
| *How Can I Reduce Vulnerability to Cyber Attacks?* | Cybersecurity System Technical Note |
| *MicroLogic Trip Units and Control Units - Firmware History* | DOCA0155EN |
| *MasterPacT MTZ - MicroLogic X Control Unit - Firmware Release Notes* | DOCA0144EN |
| *MasterPacT MTZ - MicroLogic Active Control Unit - Firmware Release Notes* | DOCA0267EN |
| *Enerlin'X IFM - Interfaz Modbus-SL para un interruptor automático (TRV00210/STRV00210) - Notas de la versión de firmware* | DOCA0145EN |
| *Enerlin'X IFM - Modbus-SL Interface for One Circuit Breaker (LV434000) - Firmware Release Notes* | DOCA0146EN |
| *Enerlin'X IFE/EIFE Ethernet Interface - Notas de la versión de firmware* | DOCA0147EN |
| *Enerlin'X IFE Switchboard Server - Firmware Release Notes* | DOCA0148EN |
| *Enerlin'X IO Input/Output Application Module for One Circuit Breaker - Notas de la versión de firmware* | DOCA0149EN |
| *Enerlin'X FDM121 - Notas de la versión de firmware* | DOCA0150EN |
| *Enerlin'X FDM128 - Ethernet Display for Eight Devices - Firmware Release Notes* | DOCA0151EN |
| *BCM ULP - Notas de la versión de firmware* | DOCA0152EN |
| *ComPacT NSX / PowerPacT H-, J- y L-Frame MicroLogic 5/6 - Notas de la versión de firmware* | DOCA0153EN |
| *ComPacT NSX - MicroLogic 7 Trip Unit - Firmware Release Notes* | DOCA0154EN |
| *Módulo ComPacT NSX BSCM Modbus SL/ULP - Notas de la versión de firmware* | DOCA0329EN |
| *Módulo de comunicación y aislamiento del interruptor (BCIM) para la unidad de control MicroLogic Active - Notas de la versión del firmware* | DOCA0395ES |
| *EcoStruxure Cybersecurity Admin Expert User Guide* | CAE_EN_UM_B4.1 |
| *EcoStruxure Panel Server - Guía del usuario* | DOCA0172EN<br>DOCA0172ES<br>DOCA0172FR<br>DOCA0172DE<br>DOCA0172IT<br>DOCA0172PT |

Puede descargar estas publicaciones técnicas y otra información técnica de nuestro sitio web (www.se.com/ww/en/download/).

# Documentos relacionados con los dispositivos UL/ANSI

| Título de la documentación | Número de referencia |
|---|---|
| *MasterPacT MTZ - MicroLogic X* | DOCA0102EN<br>DOCA0102ES<br>DOCA0102FR<br>DOCA0102ZH |
| *PowerPacT H-, J-, and L-Frame - 5 y 6 unidades de disparo MicroLogic - Guía del usuario* | 48940-312-01 (EN, ES, FR) |
| *Unidades de disparo remoto MasterPacT NT/NW - MicroLogic A - Guía del usuario* | 48049-136-05 (EN, ES, FR) |
| *MasterPacT NT/NW - MicroLogic P Trip Units - User Guide* | 48049-137-05 (EN) |
| *Unidades de disparo remoto MasterPacT NT/NW - MicroLogic H - Guía del usuario* | 48049-330-03 (EN, ES, FR) |
| *Enerlin'X EIFE - Interfaz Ethernet integrada para un interruptor automático MasterPacT MTZ seccionable - Guía del usuario* | DOCA0106EN<br>DOCA0106ES<br>DOCA0106FR |

| Título de la documentación | Número de referencia |
|---|---|
| | DOCA0106ZH |
| *Enerlin'X IFE - Servidor de panel Ethernet - Guía del usuario* | DOCA0084EN<br>DOCA0084ES<br>DOCA0084FR<br>DOCA0084ZH |
| *Enerlin'X IFE - Interfaz Ethernet para un interruptor automático - Guía del usuario* | DOCA0142EN<br>DOCA0142ES<br>DOCA0142FR<br>DOCA0142ZH |
| *How Can I Reduce Vulnerability to Cyber Attacks?* | Cybersecurity System Technical Note |
| *MicroLogic Trip Units and Control Units - Firmware History* | DOCA0155EN |
| *MasterPacT MTZ - MicroLogic X Control Unit - Firmware Release Notes* | DOCA0144EN |
| *Enerlin'X IFM - Interfaz Modbus-SL para un interruptor automático (TRV00210/STRV00210) - Notas de la versión de firmware* | DOCA0145EN |
| *Enerlin'X IFM - Modbus-SL Interface for One Circuit Breaker (LV434000) - Firmware Release Notes* | DOCA0146EN |
| *Enerlin'X IFE/EIFE Ethernet Interface - Notas de la versión de firmware* | DOCA0147EN |
| *Enerlin'X IFE Switchboard Server - Firmware Release Notes* | DOCA0148EN |
| *Enerlin'X IO Input/Output Application Module for One Circuit Breaker - Notas de la versión de firmware* | DOCA0149EN |
| *Enerlin'X FDM121 - Notas de la versión de firmware* | DOCA0150EN |
| *Enerlin'X FDM128 - Ethernet Display for Eight Devices - Firmware Release Notes* | DOCA0151EN |
| *BCM ULP - Notas de la versión de firmware* | DOCA0152EN |
| *ComPacT NSX / PowerPacT H-, J- y L-Frame MicroLogic 5/6 - Notas de la versión de firmware* | DOCA0153EN |
| *Módulo ComPacT NSX BSCM Modbus SL/ULP - Notas de la versión de firmware* | DOCA0329EN |
| *EcoStruxure Cybersecurity Admin Expert User Guide* | CAE_EN_UM_B4.1 |
| *EcoStruxure Panel Server - Guía del usuario* | DOCA0172EN<br>DOCA0172ES<br>DOCA0172FR<br>DOCA0172DE<br>DOCA0172IT<br>DOCA0172PT |

Puede descargar estas publicaciones técnicas y otra información técnica de nuestro sitio web (www.se.com/us/en/download/).

# Información sobre terminología no inclusiva o insensible

Como empresa responsable e inclusiva, Schneider Electric actualiza constantemente sus comunicaciones y productos que contienen terminología no inclusiva o insensible. Sin embargo, a pesar de estos esfuerzos, nuestro contenido aún puede contener términos que algunos clientes consideren inapropiados.

# Marcas comerciales

*QR Code* es una marca comercial registrada de DENSO WAVE INCORPORATED en Japón y otros países.

# Introducción a la ciberseguridad

## Contenido de esta parte



# Descripción general

En este apartado se incluye información general sobre la política de ciberseguridad de Schneider Electric y se explica por qué la ciberseguridad es importante para los interruptores automáticos MasterPacT, ComPacT y PowerPacT con unidades de control o disparo MicroLogic.

# Introducción a la ciberseguridad

## Introducción

La ciberseguridad tiene como objetivo proteger su red de comunicaciones y todos los equipos conectados a ella frente a ataques que puedan interrumpir las operaciones (disponibilidad), modificar la información (integridad) o revelar información confidencial (confidencialidad). El objetivo de la ciberseguridad es proporcionar mayores niveles de protección contra robo, corrupción, mal uso o accidentes de la información y los activos físicos y, a la vez, garantizar el acceso a los usuarios legítimos. Hay muchos aspectos que tener en cuenta por lo que respecta a la ciberseguridad, incluido el diseño de sistemas seguros, la restricción del acceso utilizando métodos físicos y digitales, la identificación de los usuarios y la implementación de procedimientos de seguridad y políticas de mejores prácticas.

## Directrices de Schneider Electric

Además de las recomendaciones que se ofrecen en esta guía, que son específicas de los interruptores automáticos MasterPacT, ComPacT y PowerPacT, debe seguir el método de defensa exhaustivo de Schneider Electric para la ciberseguridad.

Este método se describe en la nota técnica del sistema *How Can I Reduce Vulnerability to Cyber Attacks?*.

Además, encontrará numerosos recursos útiles e información actualizada en el Cybersecurity Support Portal del sitio web global de Schneider Electric, página 64.

# Serie maestra PacT Series

Prepare su instalación para el futuro con la PacT Series de baja y media tensión de Schneider Electric. Basada en la legendaria innovación de Schneider Electric, la PacT Series incluye interruptores automáticos, interruptores, dispositivos de corriente residual y fusibles de primer nivel para todas las aplicaciones estándar y específicas. Disfrute de un sólido rendimiento con PacT Series en los equipos de conmutación preparados para EcoStruxure, de 16 a 6300 A en baja tensión y hasta 40,5 kV en media tensión.

# Por qué es importante la ciberseguridad para los interruptores automáticos MasterPacT, ComPacT y PowerPacT

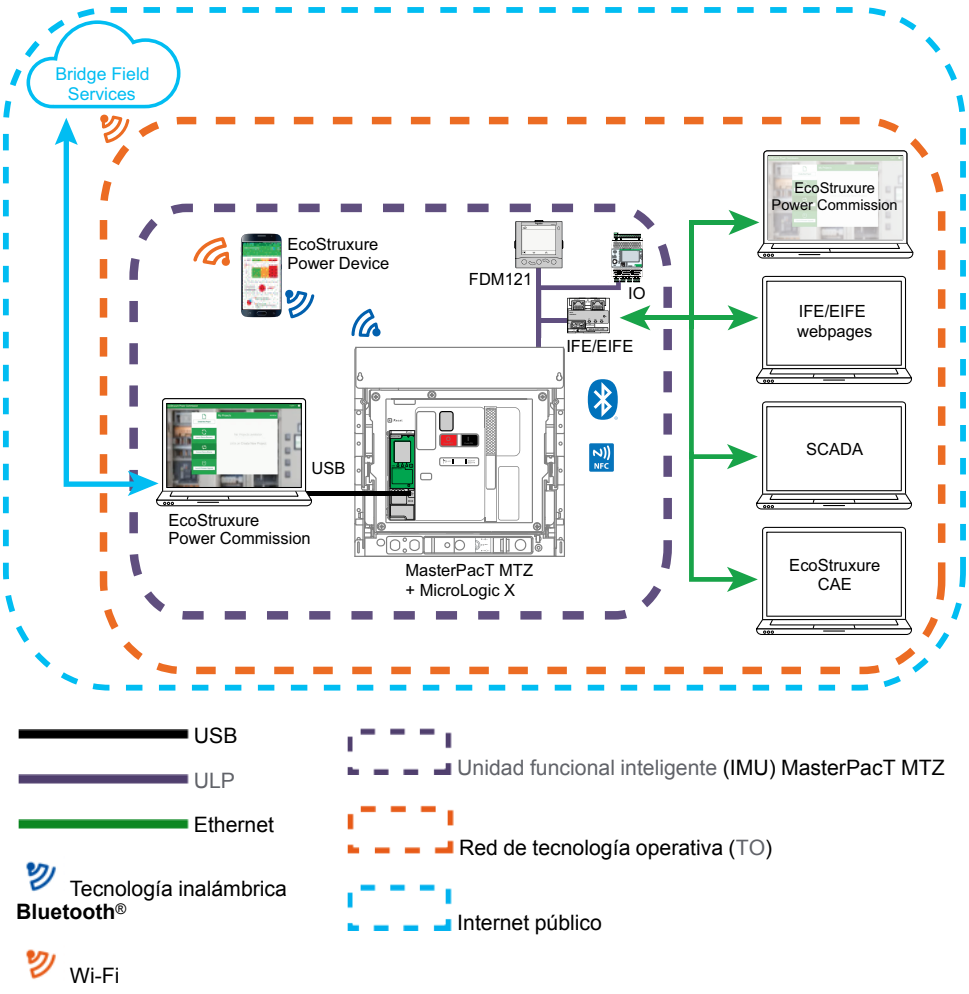
## Descripción general

El interruptor automático MasterPacT, ComPacT y PowerPacT es un componente clave de cualquier planta o equipo porque controla la alimentación eléctrica del proceso, proporciona protección eléctrica y ofrece información crítica.

MasterPacT, ComPacT y PowerPacTLos interruptores automáticos con funciones de comunicación también proporcionan acceso 24 horas al día y 7 días a la semana a funciones de control en tiempo real y a datos de supervisión. Estas funciones aumentan la eficiencia y la flexibilidad de gestión del sistema de distribución eléctrica. Sin embargo, podrían quedar expuestas a ciberataques.

## Interruptor automático MasterPacT MTZ con entorno operativo de la unidad de control MicroLogic X

En la imagen siguiente se muestran las distintas maneras de comunicarse con la unidad de control MicroLogic X del interruptor automático MasterPacT MTZ.



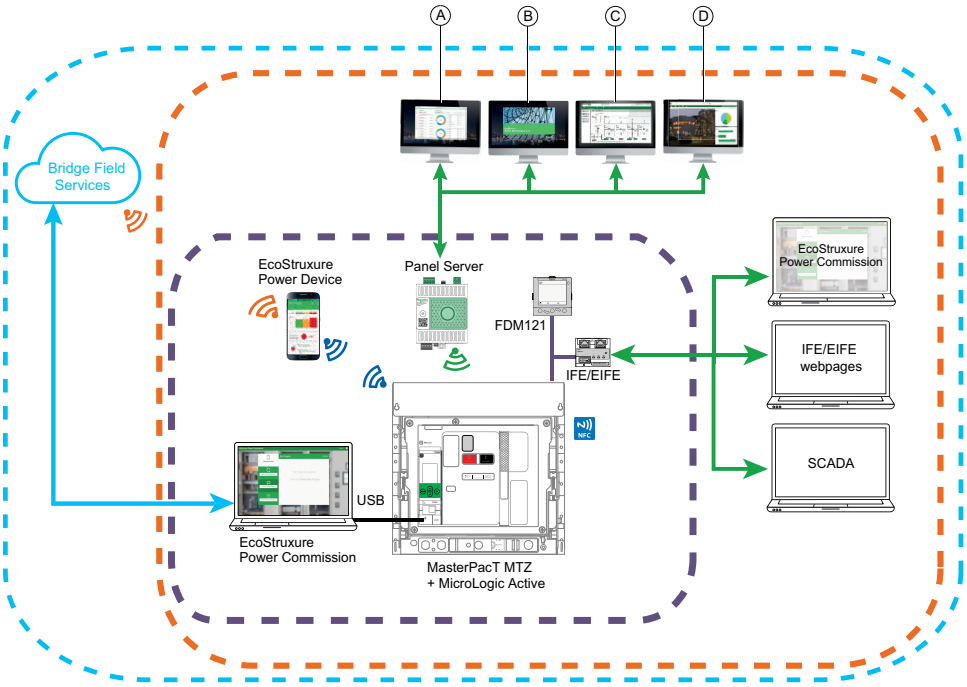

La unidad funcional modular inteligente (IMU) de MasterPacT MTZ representa el interruptor automático, la unidad de control MicroLogic X y los módulos ULP asociados, la interfaz de comunicación y los módulos IO.

Para comunicarse con el interruptor automático MasterPacT MTZ por medio de su unidad de control MicroLogic X, se encuentran disponibles las siguientes rutas de comunicación:

- MicroLogic X Interfaz hombre-máquina (HMI) de)
- Unidad de visualización frontal FDM121 para un interruptor automático
- Conexión inalámbrica NFC desde un smartphone
- Conexión inalámbrica Bluetooth Low Energy desde un smartphone
- Conexión al puerto mini tipo B USB de la unidad de control MicroLogic X desde:
  - Un PC que ejecuta el software EcoStruxure™ Power Commission
  - Un smartphone que tenga instalada la aplicación Aplicación EcoStruxure Power Device
- Ethernet (protocolos Modbus TCP/IP o IEC 61850) a través de la tecnología operativa (OT) cuando están presentes la interfaz IFE o EIFE, o el servidor IFE
- Conexión Modbus-SL a través de la red de tecnología operativa (OT) cuando la interfaz IFM está presente

# Interruptor automático MasterPacT MTZ con entorno operativo de la unidad de control MicroLogic Active

En la imagen siguiente se muestran las distintas maneras de comunicarse con la unidad de control MicroLogic Active del interruptor automático MasterPacT MTZ.




USB

NFC

Wi-Fi

Zigbee

Unidad funcional inteligente (IMU) MasterPacT MTZ

Red de tecnología operativa (TO)

Internet público

**A** Panel Server páginas web

Software **B** EcoStruxure Power Monitoring Expert (PME)

Software **C** EcoStruxure Power Operation (PO)

**D** POI Plus, estación de trabajo industrial con software de gestión de energía

La unidad funcional modular inteligente (IMU) de MasterPacT MTZ representa el interruptor automático, la unidad de control MicroLogic Active, los módulos ULP asociados, y la interfaz de comunicación.

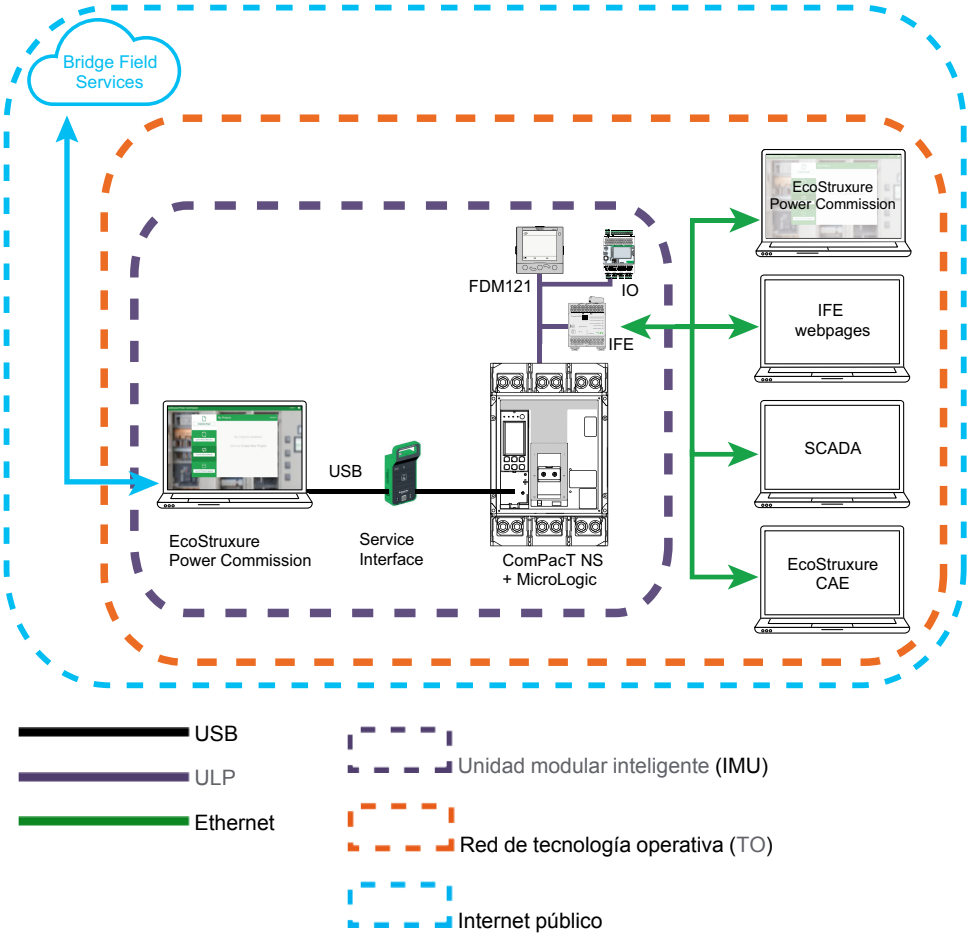
Para comunicarse con el interruptor automático MasterPacT MTZ por medio de su unidad de control MicroLogic Active, se encuentran disponibles las siguientes rutas de comunicación:

- MicroLogic Active Interfaz hombre-máquina (HMI) de)
- Unidad de visualización frontal FDM121 para un interruptor automático
- Conexión inalámbrica NFC desde un smartphone
- Conexión al puerto USB-C de la unidad de control MicroLogic Active desde:
  - Un PC que ejecuta el software EcoStruxure™ Power Commission
  - Un smartphone que tenga instalada la aplicación Aplicación EcoStruxure Power Device
- Conexión Zigbee inalámbrica a un Panel Server para unidades de control MicroLogic Active AP/EP.
- Ethernet (protocolo Modbus TCP/IP) a través de la tecnología operativa (OT) cuando están presentes la interfaz IFE o EIFE, o el servidor IFE

- Conexión Modbus-SL a través de la red de tecnología operativa (OT) cuando la interfaz IFM está presente

# Entorno operativo del interruptor automático MasterPacT NT/NW, ComPacT NS y PowerPacT de marcos P y R

En la imagen siguiente se muestran las distintas maneras de comunicarse con la unidad de disparo remoto MicroLogic del interruptor automático.



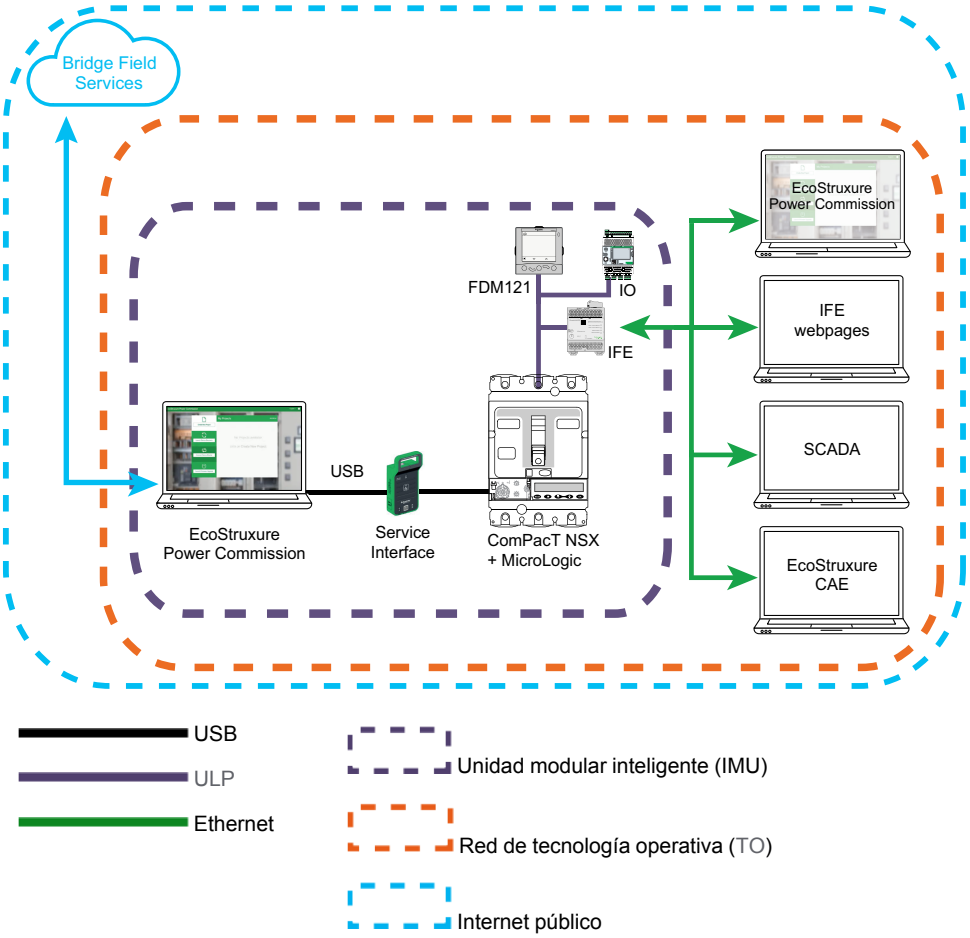

La unidad funcional modular inteligente (IMU) representa el interruptor automático MasterPacT NT/NW, ComPacT NS y PowerPacT de marcos P y R, la unidad de disparo MicroLogic y los módulos ULP asociados, la interfaz de comunicación y los módulos IO.

Para comunicarse con el interruptor automático por medio de su unidad de disparo remoto MicroLogic, se encuentran disponibles las siguientes rutas de comunicación:

- MicroLogic Interfaz hombre-máquina (HMI) de)
- Unidad de visualización frontal FDM121 para un interruptor automático
- Conexión con la unidad de disparo remoto MicroLogic desde un PC con el software EcoStruxure Power Commission a través de la interfaz de servicio
- Ethernet (protocolo Modbus TCP/IP) a través de la tecnología operativa (OT) cuando están presentes la interfaz IFE o el servidor IFE
- Conexión Modbus-SL a través de la red de tecnología operativa (OT) cuando la interfaz IFM está presente

# Entorno operativo del interruptor automático ComPacT NSX y PowerPacT de marcos H, J y L

En la imagen siguiente se muestran las distintas maneras de comunicarse con la unidad de disparo remoto MicroLogic del interruptor automático.




La unidad funcional modular inteligente (IMU) representa el interruptor automático ComPacTNSX o PowerPacT de marcos P y R, la unidad de disparo MicroLogic y los módulos ULP asociados, la interfaz de comunicación y los módulos IO.

Para comunicarse con el interruptor automático por medio de su unidad de disparo remoto MicroLogic, se encuentran disponibles las siguientes rutas de comunicación:

- MicroLogic Interfaz hombre-máquina (HMI) de)
- Unidad de visualización frontal FDM121 para un interruptor automático
- Conexión a la unidad de disparo MicroLogic desde un PC con el software EcoStruxure Power Commission a través de la interfaz de servicio o la interfaz de mantenimiento USB
- Ethernet (protocolo Modbus TCP/IP) a través de la tecnología operativa (OT) cuando están presentes la interfaz IFE o el servidor IFE
- Modbus-SL conexión a través de la tecnología operativa (OT) cuando el IFM interfaz o BSCM Modbus SL/ULP módulo está presente

# Vulnerabilidad del sistema frente a ciberataques

Cada una de las rutas de comunicación enumeradas anteriormente representa un punto vulnerable de su sistema si no se toman medidas de seguridad. Esta guía

ofrece directrices para ayudar a proteger estas rutas de comunicación frente a ataques intencionados o mal uso accidental.

Las siguientes características de seguridad pretenden mitigar las amenazas inherentes vinculadas al uso de las interfaces IFE y EIFE, el servidor IFE y los dispositivosMasterPacT, ComPacT y PowerPacT en una entorno de tecnología operativa (OT).

# Funciones de seguridad incluidas

Las IMU MasterPacT, ComPacT y PowerPacT admiten las siguientes funciones de ciberseguridad:

- Gestión de cuentas de usuario:
  - En interfaces IFE y EIFE
  - En el servidor IFE
  - En la unidad de control MicroLogic Active
- Protección mediante código de acceso
- Servicios y ajustes de seguridad configurables
- Mecanismo de actualización del firmware
- Comunicación segura máquina a máquina mediante Modbus TCP/TLS (en interfaces IFE y EIFE, y servidor IFE)
- Registros de seguridad en formato Syslog o formato CSV (en interfaces IFE y EIFE, y servidor IFE)

Estas funciones proporcionan funcionalidades de seguridad que contribuyen a proteger el producto de posibles amenazas a la seguridad que podrían:

- Interrumpir el funcionamiento del producto (disponibilidad)
- Modificar la información (integridad)
- Revelar información confidencial (confidencialidad)

# Comparación de las funciones de seguridad entre la interfaz IFE/EIFE y el servidor IFE

En la siguiente tabla se proporciona una comparativa entre las características de seguridad disponibles en estas versiones de firmware:

- La interfaz IFE/EIFE con versiones de firmware 004.•••.••• y 005.•••.•••
- El servidor IFE con versión de firmware 003.•••.•••
- El servidor IFE con versión de firmware 005.•••.•••

Schneider Electric recomienda actualizar la versión de firmware de la interfaz IFE/EIFE y el servidor IFE para utilizar las funciones más recientes.

| **Características** | **Disponibilidad** | | | **Estado predeterminado de las funciones disponibles** |
|---|---|---|---|---|
| | **Interfaz EIFE (LV851001)**<br><br>**Interfaz IFE (LV434001)** | **Servidor IFE (LV434002)**<br><br>**(versión de firmware 003.•••.•••)** | **Servidor IFE (LV434002)**<br><br>**(versión de firmware 005.•••.•••)** | |
| **HTTP** | Sí | Sí | Sí | Activado |
| **HTTPS** | Sí | No | Sí | Activado |
| **Servidor FTP** | Sí | Sí | Sí | Deshabilitado |
| **Cliente FTP** | Sí | Sí | Sí | Deshabilitado |
| **FTPS** | Sí | No | Sí | Activado |

| Características | Disponibilidad | | | Estado predeterminado de las funciones disponibles |
|---|---|---|---|---|
| | **Interfaz EIFE (LV851001)**<br><br>**Interfaz IFE (LV434001)** | **Servidor IFE (LV434002)**<br><br>**(versión de firmware 003.•••.•••)** | **Servidor IFE (LV434002)**<br><br>**(versión de firmware 005.•••.•••)** | |
| **NTP** | Sí | No | Sí | Deshabilitado |
| **SNTP** | No | Sí | No | Desactivado |
| **RSTP** | Sí | No | Sí | Deshabilitado |
| **Modbus TCP** | Sí | Sí | Sí | Activado |
| **Modbus Secure** | Sí | No | Sí | Deshabilitado |
| **RBAC** | Sí | No | Sí | Activado |
| **IEC 61850** | Sí | No | Sí | Deshabilitado |
| **Syslog** | Sí | No | Sí | Activado |
| **SMTP** | Sí | Sí | Sí | Deshabilitado |
| **Compatibilidad con IPv6 y detección de DPWS** | Sí | No | Sí | Activado |
| **SNMP** | Sí | Sí | Sí | Deshabilitado |
| **Tiempo para actualizar el firmware** | 4 minutos aproximadamente | 16 minutos aproximadamente | 4 minutos aproximadamente | – |

# Recomendaciones de ciberseguridad para el diseño, la planificación y la instalación del sistema

## Contenido de esta parte



# Descripción general

En este apartado se proporciona información importante que debe tenerse en cuenta durante las fases de diseño, planificación e instalación de una red de tecnología operativa (TO) que incluya la unidad funcional inteligente (IMU) MasterPacT, ComPacT y PowerPacT. Las recomendaciones y directrices de este apartado ayudan a crear un entorno operativo seguro.

# Identificación y protección de información y operaciones confidenciales y críticas

## Descripción general

Al planificar y diseñar una red de tecnología operativa, es importante identificar la información crítica o confidencial correspondiente a sus operaciones. Una vez identificada, esta información se debe proteger.

Como principio general:

- La información crítica incluye datos y operaciones accesibles a través de la IMU de MasterPacT, ComPacT y PowerPacT (por ejemplo, el estado del interruptor automático, el disparo o el comando de apertura o cierre).
- La información confidencial incluye cualquier información que se pueda utilizar para acceder a la instalación y la red de tecnología operativa (por ejemplo, contraseñas o códigos de acceso para equipos o salas cerradas).

Es responsabilidad suya determinar cómo se puede analizar y utilizar esta información en contra de la empresa.

## Información sobre la red de comunicación empresarial

Entre la información confidencial que se puede utilizar para acceder a su instalación y a su red de control se encuentra la siguiente:

- La arquitectura del sistema
- Direcciones IP o MAC de los dispositivos que se comunican en red
- Los números de puerto utilizados para la comunicación Ethernet
- ID y contraseñas de usuario

Esta lista no es exhaustiva, y es importante tener en cuenta toda la información específica de su organización que pueda facilitar el acceso a sistemas críticos.

## Control de accesos

Una parte importante de la ciberseguridad consiste en diseñar una política de control de accesos eficaz. El control de accesos consiste en identificar grupos de usuarios o empleados individuales de su organización y determinar el tipo y el nivel de acceso que necesitan para desempeñar sus trabajos eficazmente.

# Resumen de información y operaciones accesibles a través de cada ruta de acceso

En función de la interfaz de comunicación o la ruta de comunicación utilizadas para acceder a la unidad funcional inteligente (IMU) MasterPacT, ComPacT y PowerPacT, la información y las operaciones de control disponibles son diferentes.

En la tabla siguiente se resume el acceso a las operaciones de información y control a través de la IMU MasterPacT MTZ con la unidad de control MicroLogic X:

| **Información y operaciones de control** | **Acceso local** | | | | | **Acceso remoto** |
|---|---|---|---|---|---|---|
| | **MicroLogic X HMI** | **Unidad de visualización FDM121** | **NFC** | **Bluetooth Low Energy technology** | **USB** | **Ethernet / Modbus-SL** |
| Supervisión de datos | Lectura | Lectura | Lectura | Lectura | Lectura | Lectura |
| Ajustes de protección | Lectura/Escritura | Lectura | Lectura | Lectura/Escritura | Lectura/ Escritura | Lectura/Escritura |
| Otros ajustes | Lectura/Escritura | Lectura | Lectura | Lectura/Escritura | Lectura/ Escritura | Lectura/Escritura |
| Abrir/Cerrar/ Restablecer | No | Sí | No | Sí | Sí | Sí |

En la tabla siguiente se resume el acceso a las operaciones de información y control a través de la IMU MasterPacT MTZ con la unidad de control MicroLogic Active:

| **Información y operaciones de control** | **Acceso local** | | | | **Acceso remoto** | |
|---|---|---|---|---|---|---|
| | **MicroLogic Active HMI** | **Unidad de visualización FDM121** | **NFC** | **USB** | **Zigbee** | **Ethernet / Modbus-SL** |
| Supervisión de datos | Lectura | Lectura | Lectura | Lectura | Lectura | Lectura |
| Ajustes de protección | Lectura/ Escritura | Lectura | Lectura | Lectura/ Escritura | No | Lectura |
| Otros ajustes | Lectura/ Escritura | Lectura | Lectura | Lectura/ Escritura | Lectura | Lectura |
| Abrir/Cerrar/ Restablecer | No | Sí, solo en Auto Local control mode | No | Sí | No | Sí, solo en Auto Remote control mode |

En la tabla siguiente se resume el acceso a las operaciones de información y control a través de las IMU MasterPacT NT/NW, ComPacT NS y PowerPacT de marcos P y R:

| **Información y operaciones de control** | **Acceso local** | | | **Acceso remoto** |
|---|---|---|---|---|
| | **MicroLogic HMI** | **Unidad de visualización FDM121** | **Puerto de prueba** | **Ethernet / Modbus-SL** |
| Supervisión de datos | Lectura | Lectura | Lectura | Lectura |
| Ajustes de protección | Lectura/Escritura | Lectura | Lectura/ Escritura | Lectura/Escritura |
| Otros ajustes | Lectura/Escritura | Lectura | Lectura/ Escritura | Lectura/Escritura |
| Abrir/Cerrar/Restablecer | No | Sí | Sí | Sí |

En la tabla siguiente se resume el acceso a las operaciones de información y control a través de las IMU ComPacT NSX y PowerPacT de marcos H, J y L:

| Información y operaciones de control | Acceso local | | | Acceso remoto |
|---|---|---|---|---|
| | MicroLogic HMI | Unidad de visualización FDM121 | Puerto de prueba | Ethernet / Modbus-SL |
| Supervisión de datos | Lectura | Lectura | Lectura | Lectura |
| Ajustes de protección | Lectura/Escritura | Lectura | Lectura/Escritura | Lectura/Escritura |
| Otros ajustes | Lectura/Escritura | Lectura | Lectura/Escritura | Lectura/Escritura |
| Abrir/Cerrar/Restablecer | No | Sí | Sí | Sí |

Para obtener información sobre la protección de cada interfaz de comunicación y ruta de acceso, consulte las recomendaciones para el acceso local, página 33 o el acceso remoto, página 48, según corresponda.

# Diseño de una política de contraseñas

## Descripción general

Una política de contraseñas minuciosamente diseñada es la primera línea de defensa frente a ciberataques.

En el contexto de las instalaciones que incluyen el interruptor automático MasterPacT, ComPacT y PowerPacT con una unidad de control o disparo remoto MicroLogic, se requieren contraseñas para:

- Ejecutar comandos intrusivos en la unidad de control MicroLogic, sea cual sea el modo de acceso (por medio de Modbus-TCP / Modbus-SL, una conexión USB o la tecnología inalámbrica Bluetooth)
- Ejecutar comandos intrusivos en la unidad de disparo remoto MicroLogic, sea cual sea el modo de acceso (por medio de Modbus-TCP / Modbus-SL, Unidad de visualización FDM121 o un puerto de prueba)
- Iniciar sesión en el PC en el que se ejecuta el software deEcoStruxure Power Commission
- Iniciar sesión en las páginas web de las interfaces IFE y EIFE
- Iniciar sesión en las páginas web del servidor IFE
- Iniciar sesión en las páginas web de la interfaz IFE y EIFE, y el servidor IFE, mediante el software de EcoStruxure Power Commission de una IMU MasterPacT MTZ
- Inicio de sesión en el servidor FTPS para la configuración de IEC 61850 en las interfaces IFE y EIFE, y el servidor IFE, desde un MasterPacT MTZ

## Recomendaciones de ciberseguridad referentes a la política de contraseñas

**⚠ADVERTENCIA**

**RIESGO POTENCIAL PARA LA DISPONIBILIDAD, LA INTEGRIDAD Y LA CONFIDENCIALIDAD DEL SISTEMA**

La primera vez que utilice el sistema, cambie las contraseñas predeterminadas para evitar el acceso no autorizado a la configuración, los controles y la información del aparato.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

La política de contraseñas es uno de los elementos principales de la política de ciberseguridad. Una buena política de contraseñas consiste en:

- Usar contraseñas seguras
- Cambiar periódicamente las contraseñas
- Usar un gestor de contraseñas para gestionar las contraseñas de acceso
- Prohibir la reutilización de contraseñas antiguas
- Recordar periódicamente a los usuarios las prácticas recomendadas sobre las contraseñas

Para contribuir a proteger su sistema, lo mínimo es:

- Aplicar el uso de contraseñas seguras
- Establecer la longitud mínima de las contraseñas en 10 caracteres
- Cambiar la contraseña periódicamente

Todos los usuarios deben conocer las prácticas referentes a las contraseñas. Son las siguientes:

- No compartir contraseñas personales
- No mostrar las contraseñas al introducirlas
- No transmitir contraseñas por correo electrónico ni por ningún otro medio
- No guardar las contraseñas en los PC u otros dispositivos

# Contraseña para ajustes y controles críticos de MicroLogic Active

Al acceder a la unidad de control MicroLogic Active mediante un software Aplicación EcoStruxure Power Device o EcoStruxure Power Commission, cualquier comando intrusivo que modifique el comportamiento del interruptor automático MasterPacT MTZ con una unidad de control MicroLogic Active requerirá una contraseña. Por ejemplo, para realizar cambios en los ajustes de protección o para utilizar el interruptor automático, se necesita la contraseña de MicroLogic Active.

Se han definido una cuenta de usuario y una contraseña únicos para la unidad de control MicroLogic Active.

Cuando se realiza la conexión por medio de Aplicación EcoStruxure Power Device o el software EcoStruxure Power Commission, se solicita al usuario que proporcione esta contraseña.

La contraseña consta de 8 a 32 caracteres ASCII, con las siguientes restricciones:

- Solo se permiten caracteres ASCII [32-126]
- Al menos un carácter en mayúsculas
- Al menos un carácter en minúsculas
- No debe contener el nombre de usuario
- Debe ser diferente de la contraseña anterior

Las contraseñas predeterminadas deben cambiarse en la primera instalación del interruptor automático MasterPacT MTZ con una unidad de control MicroLogic Active y periódicamente tras la primera instalación, usando el software EcoStruxure Power Commission. Almacene las contraseñas usando un gestor de contraseñas. Comparta las contraseñas con un número limitado de usuarios de confianza. Siga las recomendaciones de la política de contraseñas cuando corresponda.

**IMPORTANTE:**

- Cuando se conecta desde una pantalla FDM121, solo se permiten comandos intrusivos en Auto Local control mode.
- Cuando se conecta desde una interfaz de supervisión y control remoto, solo se permiten comandos intrusivos en Auto Remote control mode.
- Los comandos intrusivos no están permitidos en Manual control mode.

# Contraseña para otros ajustes y controles críticos de MicroLogic

Al acceder a la unidad de control o disparo remoto MicroLogic mediante una interfaz de comunicación, cualquier comando intrusivo que modifique el comportamiento del interruptor automático MasterPacT, ComPacT y PowerPacT requerirá una contraseña. Por ejemplo, para realizar cambios en los ajustes de protección o para utilizar el interruptor automático, se necesita la contraseña de MicroLogic.

Se definen cuatro contraseñas para una unidad de control o disparo remoto MicroLogic, una para cada uno de los siguientes cuatro perfiles de usuario:

- Administrador
- Servicios
- Ingeniero
- Operador

Para obtener más información sobre los perfiles de usuario, consulte las guías del usuario de MicroLogic, página 8.

Cuando se realiza la conexión por medio de Aplicación EcoStruxure Power Device o el software EcoStruxure Power Commission, se solicita al usuario que proporcione una de estas contraseñas.

Cuando se realiza la conexión desde una interfaz de supervisión y control remota, la contraseña debe formar parte de la solicitud de comunicación.

La contraseña consta de cuatro caracteres ASCII. La contraseña distingue mayúsculas y minúsculas y los caracteres permitidos son:

- Dígitos del 0 al 9
- Letras minúsculas de la "a" a la "z"
- Letras mayúsculas de la "A" a la "Z"

Las contraseñas predeterminadas deben cambiarse en la primera instalación del interruptor automático MasterPacT, ComPacT y PowerPacT y periódicamente tras la primera instalación, usando el software EcoStruxure Power Commission. Almacene las contraseñas usando un gestor de contraseñas. Comparta las contraseñas con un número limitado de usuarios de confianza. Siga las recomendaciones de la política de contraseñas cuando corresponda.

# Contraseña para acceso remoto a la unidad de control MicroLogic mediante la interfaz IFE o EIFE, o el servidor IFE

En una IMU MasterPacT MTZ, el acceso a la unidad de control MicroLogic X o MicroLogic Active se comprueba mediante un mecanismo de control de acceso basado en roles (RBAC) cuando se realiza la conexión con:

- Software EcoStruxure Power Commission a través de Ethernet
- Páginas web de la interfaz IFE o del servidor IFE
- Páginas web de la interfaz EIFE
- Servidor FTPS para las interfaces IFE y EIFE, y el servidor IFE.

Para obtener más información sobre el mecanismo RBAC, consulte *Contraseñas para páginas web de la interfaz IFE o EIFE y el servidor IFE o EIFE FTPS*, página 28.

# Contraseña para acceso remoto a las unidades de disparo ComPacT NSX mediante interfaz IFE o servidor IFE

En una IMU ComPacT NSX equipada con una unidad de control MicroLogic 5, 6 o 7, el acceso a la unidad de disparo remoto MicroLogic se comprueba mediante un mecanismo de control de acceso basado en funciones (RBAC) cuando la conexión se realiza a través de:

- Software EcoStruxure Power Commission a través de Ethernet
- Páginas web de la interfaz IFE o del servidor IFE
- Servidor FTPS para la interfaz IFE o el servidor IFE.

Para obtener más información sobre el mecanismo RBAC, consulte *Contraseñas para páginas web de la interfaz IFE o EIFE y el servidor IFE o EIFE FTPS*, página 28.

# Contraseñas e ID de usuario para PC en red

Los PC en los que se ejecuta el software EcoStruxure Power Commission o que acceden a la unidad de control o disparo remoto MicroLogic utilizando cualquier otro medio (por ejemplo, páginas web de IFE o SCADA) deben solicitar a los usuarios un nombre de usuario y una contraseña. Debe asegurarse de que los usuarios definan contraseñas seguras y las cambien periódicamente. Además, debe ajustar un temporizador para bloquear la pantalla del PC automáticamente después de un periodo de tiempo de inactividad.

Una contraseña segura incluye letras mayúsculas y minúsculas, números y caracteres especiales, si es posible utilizarlos. Debe tener una longitud mínima de 10 caracteres.

Siga las recomendaciones de la política de contraseñas cuando corresponda.

# Contraseñas para las páginas web de la interfaz IFE/EIFE o del servidor IFE (con versión de firmware 005.•••.•••) y servidor FTPS

El acceso a las páginas web de la interfaz IFE, las páginas web de la interfaz EIFE, las páginas web del servidor IFE, y el servidor FTPS para interfaces IFE y EIFE o servidor IFE lo comprueba el mecanismo de control de acceso basado en roles (RBAC).

Con RBAC, a los usuarios se les asigna un rol que define las funciones a las que pueden acceder.

El administrador de seguridad del sistema enumera los usuarios del sistema y asigna un rol a cada uno de ellos.

El administrador de seguridad puede administrar los usuarios de la interfaz IFE o EIFE, o el servidor IFE:

- En las páginas web de la interfaz IFE o EIFE, o del servidor IFE
- Con el software EcoStruxure Cybersecurity Admin Expert (CAE)

El administrador de seguridad puede utilizar el software CAE para definir la política de seguridad del sistema.

La política de seguridad se aplica a todos los elementos del sistema que son compatibles con el software CAE. Para sistemas de baja tensión, se aplica a las interfaces IFE y EIFE, y al servidor IFE en el sistema.

El administrador de seguridad puede definir los siguientes parámetros de la política de seguridad con el software CAE:

- Período mínimo de inactividad. Después de transcurrir este tiempo sin que el usuario realice ninguna acción, se bloquean las páginas web de la interfaz IFE o EIFE. El usuario deberá volver a introducir su contraseña para desbloquearlas.
- Número máximo de intentos de inicio de sesión
- Duración del período de bloqueo

Para obtener más información, consulte CAE_EN_UM_B4.1 *EcoStruxure Cybersecurity Admin Expert User Guide*.

# Contraseñas de las páginas web del servidor IFE (con versión de firmware 003.•••.•••)

Para el servidor IFE con versión de firmware 003.•••.•••, cada usuario de las páginas web del servidor IFE tendrá un ID de usuario personal y una contraseña con los que iniciar sesión en las páginas web. Los usuarios deben cambiar su contraseña después de iniciar sesión en las páginas web por primera vez.

Debe definir qué usuarios de su organización deben iniciar sesión en las páginas web del servidor IFE y seguir las recomendaciones de la política de contraseñas cuando corresponda.

# Diseñar una política de códigos PIN

## Descripción general

En el contexto del interruptor automático MasterPacT MTZ con unidad de control MicroLogic Active, el acceso local a los datos de la HMI de MicroLogic Active puede protegerse con un código PIN.

## Recomendaciones de ciberseguridad referentes a la política de códigos PIN

**⚠ADVERTENCIA**

**RIESGO POTENCIAL PARA LA DISPONIBILIDAD, LA INTEGRIDAD Y LA CONFIDENCIALIDAD DEL SISTEMA**

La primera vez que utilice el sistema, cambie los códigos PIN predeterminados para evitar el acceso no autorizado a la configuración, los controles y la información del dispositivo.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

La política de códigos PIN es uno de los elementos principales de la política de cibersesguridad. Una buena política de códigos PIN debe:

- Evitar códigos PIN que sean fáciles de adivinar, como fechas de cumpleaños, dígitos repetidos o secuencias numéricas
- Cambiar regularmente los códigos PIN
- Usar un gestor de contraseñas para gestionar los códigos PIN de acceso
- Prohibirla reutilización de códigos PIN antiguos
- Recordar periódicamente a los usuarios las prácticas recomendadas sobre los códigos PIN

Para contribuir a proteger su sistema, lo mínimo es:

- Imponer el uso de códigos PIN seguros
- Cambiar los códigos PIN periódicamente

Todos los usuarios deben conocer las prácticas referentes a los códigos PIN. Esto incluye:

- No compartir códigos PIN personales
- No mostrar los códigos PIN al introducirlos
- No transmitir códigos PIN por correo electrónico o por cualquier otro medio
- No guardar los códigos PIN en los PC u otros dispositivos

## Código PIN para ajustes y controles críticos de MicroLogic Active

Cuando acceda a un parámetro protegido en la HMI de MicroLogic Active, se le pedirá que cree una cuenta y establezca un código PIN. A continuación, se le pedirá que introduzca el código PIN cada vez que acceda a un parámetro protegido.

De forma predeterminada, el código PIN se asocia a la cuenta SecurityAdmin. Puede cambiar el nombre de esta cuenta con el software EcoStruxure Power Commission.

Las siguientes acciones están protegidas por código PIN:

- Modificación del código PIN de la HMI
- Ajuste de la función de protección
- Prueba de la función de protección
- Modificación de fecha y hora
- Modificación del modo de control
- Ajuste de sustitución de MicroLogic Active

El código PIN debe contener 6 dígitos, de 0 a 9.

Para obtener más información sobre cómo crear un código PIN, consulte *MasterPacT MTZ - Unidad de control MicroLogic Active - Guía del usuario*, página 8.

# Formación

## Descripción general

La concienciación y formación de los empleados es un fundamento sumamente importante de la estrategia de ciberseguridad. Debe asegurarse de que todos los usuarios con acceso a la red de comunicación TO de su instalación conozcan la política de información de seguridad corporativa. También debe asegurarse de que hayan recibido una formación adecuada para el desempeño de sus tareas de acuerdo con dicha política.

Concretamente, los usuarios deben conocer (y se les deben recordar periódicamente) las prácticas recomendadas referentes a lo siguiente:

- No compartir información confidencial, como contraseñas o códigos de acceso de equipos o de salas cerradas
- Mantener los PC bloqueados mientras no se utilicen
- Asegurarse de llevar siempre encima los smartphones que puedan utilizarse para acceder al sistema y de que estos estén protegidos ante posibles accesos no autorizados a través de la tecnología inalámbrica Bluetooth o de Internet
- No contravenir ninguna política de seguridad por motivos de comodidad

Para obtener más información sobre el diseño y la implementación de una buena política de formación, consulte *How Can I Reduce Vulnerability to Cyber Attacks?*.

# Recomendaciones de ciberseguridad para el acceso local

## Contenido de esta parte



# Descripción general

Esta sección enumera las rutas de acceso locales al interruptor automático MasterPacT, ComPacT y PowerPacT. También proporciona recomendaciones para proteger estas rutas de acceso. Son cuestiones importantes que tener en cuenta para el funcionamiento.

# Restricción del acceso local al interruptor automático MasterPacT, ComPacT y PowerPacT

## Descripción general

La unidad funcional modular inteligente (IMU) de MasterPacT, ComPacT y PowerPacT ofrece posibilidades de acceso local y remoto. Debe asegurarse de que solo se otorgue acceso a usuarios autorizados.

## Acceso local al interruptor automático MasterPacT, ComPacT y PowerPacT

El acceso local a la unidad funcional modular inteligente de MasterPacT, ComPacT y PowerPacT proporciona varias posibilidades para acceder a información sobre el sistema y controlarlo.

Por lo tanto, es importante restringir el acceso local al interruptor automático MasterPacT, ComPacT y PowerPacT instalándolo en un área cerrada para evitar:

- El acceso no autorizado a la HMI MicroLogic, con el riesgo de que se realicen cambios en los ajustes desde la HMI
- El acceso no autorizado a la comunicación inalámbrica Bluetooth, que supone el riesgo de que se realicen cambios en los ajustes desdeAplicación EcoStruxure Power Device
- El acceso no autorizado a la comunicación inalámbrica NFC, con el riesgo de revelación de datos
- La conexión no autorizada a través del puerto USB de la unidad de control MicroLogic, que supone el riesgo de que se realicen cambios en los ajustes desde el software EcoStruxure Power Commission o el smartphone con Aplicación EcoStruxure Power Device
- La conexión no autorizada a través del puerto de prueba de la unidad de disparo remoto MicroLogic, que supone el riesgo de que se realicen cambios en los ajustes desde el software EcoStruxure Power Commission mediante la interfaz de servicio o de mantenimiento USB
- El acceso no autorizado al módulo IO, que supone el riesgo de que se realicen cambios en el ajuste del conmutador para la aplicación predefinida que se está utilizando

También es importante implementar reglas para gestionar el acceso al área cerrada. Concretamente, se debe asegurar de que:

- El área se mantenga cerrada en todo momento.
- El área disponga de un sistema de autenticación y autorización.
- Solo el personal autorizado disponga de una llave o un código de acceso.
- Los cables de la red de comunicación que entren en la sala y los puertos de conexión de los dispositivos de comunicación de fuera de la sala estén protegidos.
- Todos los dispositivos, como PC, smartphones y tabletas que accedan a la unidad de control o disparo remoto MicroLogic estén protegidos de acuerdo con las directrices más recientes del proveedor.

Cuando el interruptor automático MasterPacT, ComPacT y PowerPacT esté instalado en un área cerrada, se debe implementar un proceso de apertura de emergencia. Por ejemplo:

- Debe disponer en el área como mínimo de un botón de parada de emergencia que resulte accesible desde el exterior.
- El interruptor automático debe disponer de una bobina de disparo por falta de tensión MN (sistema de modo seguro).

# Recomendaciones para proteger el acceso local a la HMI de MicroLogic

## Funciones accesibles desde la HMI

Cualquier persona que tenga acceso a la carcasa en la que se encuentra el interruptor automático tendrá acceso a la MicroLogic HMI.

Algunas funciones críticas, como los ajustes de protección del equipo, se pueden configurar desde la MicroLogic HMI.

## Recomendaciones para proteger el acceso a través de la HMI de MicroLogic Active

La MicroLogic Active HMI puede tener un código PIN protegido. Se recomienda utilizar la protección con código PIN en la unidad de control MicroLogic Active. Para obtener más información sobre la protección con código PIN, consulte Diseñar una política de códigos PIN, página 30.

Para mayor seguridad, debe:

- Sellar la cubierta protectora de la MicroLogic Active HMI.
- Sellar la cubierta protectora del puerto USB del MicroLogic Active.
- Instalar el interruptor automático en un área cerrada.
- Mantener el área cerrada en todo momento.
- Facilitar la llave o el código de acceso únicamente a personal autorizado.

Para obtener información adicional sobre cómo proteger el acceso al interruptor automático, consulte Implementación de una política de acceso restringido, página 34.

## Recomendaciones para proteger el acceso a través de otras MicroLogic HMI

La MicroLogic HMI de los siguientes interruptores automáticos no está protegida con código PIN ni con contraseña:

- Interruptores automáticos MasterPacT MTZ con unidades de control MicroLogic X
- Interruptores automáticos MasterPacT NT/NW con unidades de disparo remoto MicroLogic
- Interruptores automáticos ComPacT
- Interruptores automáticos PowerPacT

Además, no todas las MicroLogic HMI pueden bloquearse físicamente para evitar el acceso a la pantalla. Por lo tanto, para proteger el acceso a la HMI, debe:

- Precintar la cubierta de protección de la MicroLogic HMI, si la cubierta puede precintarse.
- Instalar el interruptor automático en un área cerrada.
- Mantener el área cerrada en todo momento.
- Facilitar la llave o el código de acceso únicamente a personal autorizado.

Para obtener información adicional sobre cómo proteger el acceso al interruptor automático, consulte Implementación de una política de acceso restringido, página 34.

# Bloqueo de los ajustes de protección

Se pueden bloquear físicamente los ajustes de protección del interruptor automático siguientes para impedir que se cambien localmente en la HMI:

- Interruptores automáticos MasterPacT MTZ con unidades de control MicroLogic X
- Interruptores automáticos MasterPacT NT/NW con unidades de disparo remoto MicroLogic
- Interruptores automáticos ComPacT
- Interruptores automáticos PowerPacT

De forma predeterminada, estos interruptores automáticos permiten cambiar la configuración de protección de la HMI. Si no desea utilizar esta función, le recomendamos bloquear los ajustes de protección. Para obtener más información, consulte las Guías del usuario de MicroLogic, página 8

# Recomendaciones para proteger el acceso a través de NFC (MasterPacT MTZ)

## Funciones accesibles a través de NFC

Por medio de la comunicación de campo cercano (NFC) inalámbrica, se pueden descargar datos de diagnóstico de la unidad de control MicroLogic X o MicroLogic Active a un smartphone, aunque la unidad de control no esté encendida. No es posible cambiar ningún ajuste en la unidad de control, ni abrir, cerrar o reiniciar el interruptor automático MasterPacT MTZ.

## Requisitos previos para establecer una conexión NFC

Para establecer una conexión inalámbrica NFC con la unidad de control MicroLogic X o MicroLogic Active, los requisitos previos son los siguientes:

- Debe tener acceso físico a la sala en la que está el interruptor automático MasterPacT MTZ y a la carcasa del equipo.
- Aplicación EcoStruxure Power Device debe estar instalada en el smartphone.
- El smartphone debe ser compatible con la NFC.

Cualquier persona que cumpla estas condiciones puede descargar datos que pueden ser confidenciales para las operaciones. En la unidad de control MicroLogic X o MicroLogic Active, no se registran las conexiones establecidas a través de NFC.

Para conocer el procedimientodetallado para establecer una conexión NFC, consulte la Guía del usuario de MicroLogic X o MicroLogic Active, página 8.

## Recomendaciones generales para proteger el acceso a través de NFC

Para proteger el acceso a datos a los que se puede llegar mediante NFC inalámbrica, se recomienda lo siguiente:

- Instalar el interruptor automático MasterPacT MTZ en un área cerrada para que solo el personal autorizado pueda acceder a la unidad de control MicroLogic X o MicroLogic Active.
- Mantener el área cerrada en todo momento.
- Facilitar la llave o el código de acceso únicamente a personal autorizado.

Para obtener más información, consulte las recomendaciones para restringir el acceso local al interruptor automático MasterPacT MTZ, página 34.

## Recomendaciones para la comunicación NFC

Para proteger el acceso a funciones a las que se puede llegar mediante NFC inalámbrica, se recomienda lo siguiente:

- Desconectar el smartphone de Internet (por ejemplo, colocarlo en modo avión) durante una conexión NFC con la unidad de control MicroLogic X o MicroLogic Active.
- No introducir un código de emparejamiento si se le solicita, porque no es necesario para una conexión NFC.

# Recomendaciones para el uso de EcoStruxure Power Device

Para restringir el acceso a la unidad de control MicroLogic X o MicroLogic Active desde un smartphone en el que se ejecute Aplicación EcoStruxure Power Device, se recomienda utilizar únicamente la oficial de Schneider Electric Aplicación EcoStruxure Power Device para conectarse al interruptor automático MasterPacT MTZ.

# Recomendaciones para el uso de smartphones

Para restringir el acceso a la unidad de control MicroLogic X o MicroLogic Active desde un smartphone, se recomienda:

- Asegurarse de que los smartphones que dispongan de Aplicación EcoStruxure Power Device estén protegidos con contraseña y se utilicen solo para el trabajo.
- Proteger los smartphones en los que se haya instalado Aplicación EcoStruxure Power Device implementando todas las funciones de seguridad recomendadas por el proveedor o el fabricante del smartphone.
- Mantener actualizadas las aplicaciones antivirus para smartphones.
- No facilitar información acerca del smartphone (número de teléfono, dirección MAC) a menos que sea estrictamente necesario.
- Desconectar el smartphone de Internet (por ejemplo, colocarlo en modo avión) durante una conexión NFC con la unidad de control MicroLogic X o MicroLogic Active.
- No almacenar información confidencial en un smartphone.

# Recomendaciones para proteger el acceso a través de la tecnología inalámbrica Bluetooth® (MasterPacT MTZ)

## Funciones accesibles a través de la tecnología inalámbrica Bluetooth

**AVISO**

**RIESGO DE FUNCIONAMIENTO IMPREVISTO**

- Solo personal cualificado debe ser el encargado de configurar y preparar el aparato, usando los resultados del estudio del sistema de protección de la instalación.
- Durante la puesta en marcha de la instalación y después de cualquier modificación, compruebe que la configuración de MicroLogic X y los ajustes de las funciones de protección sean acordes con los resultados de este estudio.
- Las funciones de protección de MicroLogic X están establecidas de manera predeterminada en su valor mínimo, a excepción de la función de protección de largo retardo, que se establece de manera predeterminada en su valor máximo.

**Si no se siguen estas instrucciones, pueden producirse daños en el equipo.**

Mediante la tecnología inalámbrica Bluetooth Low Energy, puede acceder a la unidad de control MicroLogic X desde un smartphone que esté ejecutando la Aplicación EcoStruxure Power Device. Esta aplicación ofrece una interfaz orientada a tareas con la unidad de control. Los datos transferidos a través de la tecnología inalámbrica Bluetooth se cifran utilizando el algoritmo de cifrado AES de 128 bits.

**NOTA:** La tecnología inalámbrica Bluetooth no está disponible en las unidades de control MicroLogic Active.

## Requisitos previos para establecer una conexión Bluetooth

Para establecer una conexión inalámbrica Bluetooth con la unidad de control MicroLogic X, los requisitos previos son los siguientes:

- La unidad de control MicroLogic X debe estar encendida.
- La función Bluetooth de la unidad de control MicroLogic X debe estar activada.
- Solo se puede conectar un smartphone a una unidad de control a la vez.
- Debe tener un smartphone con Aplicación EcoStruxure Power Device instalada.
- El smartphone debe admitir la tecnología inalámbrica Bluetooth Low Energy (4.0 o versiones superiores).
- Debe tener acceso a la unidad de control MicroLogic X para activar la función Bluetooth (pulsando el pulsador de activación correspondiente) y encontrarse físicamente en la zona de cobertura durante la conexión (normalmente, de 20 a 30 metros o yardas).
- Debe introducir el código de emparejamiento de 6 cifras generado aleatoriamente por la unidad de control MicroLogic X y mostrado en la HMI MicroLogic X.

Cualquier persona que cumpla estas condiciones y establezca una conexión tendrá acceso a funciones que pueden afectar a la instalación.

Para conocer los procedimientos detallados para establecer una conexión Bluetooth, consulte *MasterPacT MTZ - MicroLogic X* , página 8.

# Recomendaciones generales para proteger el acceso a través de la tecnología inalámbrica Bluetooth

Para proteger el acceso a las funciones a las que se puede acceder a través de la tecnología inalámbrica Bluetooth, se recomienda:

- Instalar el interruptor automático MasterPacT MTZ en un área cerrada para que solo el personal autorizado pueda acceder a la unidad de control MicroLogic X.
- Mantener el área cerrada en todo momento.
- Facilitar la llave o el código de acceso únicamente a personal autorizado.

Para obtener información adicional sobre cómo proteger el acceso al interruptor automático MasterPacT MTZ, consulte Implementación de una política de acceso restringido, página 34.

# Recomendaciones para utilizar la tecnología inalámbrica Bluetooth

La implementación de la función Bluetooth cumple con lo estipulado en la publicación especial NIST 800-121 Revisión 1. No obstante, para proteger el acceso a las funciones a las que se puede acceder a través de la tecnología inalámbrica Bluetooth, se recomienda:

- Desactivar la función Bluetooth en la unidad de control MicroLogic X y activarla solo cuando esté listo para establecer una conexión.

  Para obtener los procedimientos detallados sobre cómo desactivar la función Bluetooth Bluetooth, consulte *MasterPacT MTZ - MicroLogic X* , página 8.
- Ajustar el temporizador de desconexión de la función Bluetooth en 5 minutos.
- Excepto cuando inicie una conexión Bluetooth, la función Bluetooth no debe activarse por medio del pulsador de activación de la parte frontal de la unidad de control MicroLogic X. La función Bluetooth debe permanecer desconectada cuando no se utilice.
- Pulse el pulsador Bluetooth para finalizar la comunicación cuando haya terminado.
- El emparejamiento solo debe realizarse cuando sea necesario y en una zona segura.
- No introduzca un código de emparejamiento si se le pide de forma inesperada.
- Durante el emparejamiento de Bluetooth, mantenga el smartphone lo más cerca posible de la unidad de control MicroLogic X.

# Recomendaciones para el uso de EcoStruxure Power Device

Para restringir el acceso a la unidad de control MicroLogic X desde un smartphone en el que se ejecute Aplicación EcoStruxure Power Device, se recomienda utilizar únicamente la oficial de Schneider Electric Aplicación EcoStruxure Power Device para conectarse al interruptor automático MasterPacT MTZ.

# Recomendaciones para el uso de smartphones

Para restringir el acceso a la unidad de control MicroLogic X desde un smartphone, se recomienda:

- Asegurarse de que los smartphones que dispongan de Aplicación EcoStruxure Power Device estén protegidos con contraseña y se utilicen solo para el trabajo.
- Proteger los smartphones en los que se haya instalado Aplicación EcoStruxure Power Device implementando todas las funciones de seguridad recomendadas por el proveedor o el fabricante del smartphone.
- Mantener actualizadas las aplicaciones antivirus para smartphones.
- No facilitar información acerca del smartphone (número de teléfono, dirección MAC) a menos que sea estrictamente necesario.
- Desconectar el smartphone de Internet durante la conexión Bluetooth con la unidad de control MicroLogic X.
- No almacenar información confidencial en un smartphone.

# Recomendaciones para proteger el acceso a la unidad de control MicroLogic a través del puerto USB (MasterPacT MTZ)

## Funciones accesibles a través del puerto USB

Es posible acceder a las funciones de la unidad de control MicroLogic X o MicroLogic Active al:

- Conectar un PC en el que se ejecute el software EcoStruxure Power Commission al puerto USB de la unidad de control.
- Conectar un smartphone en el que se ejecute Aplicación EcoStruxure Power Device al puerto USB de la unidad de control a través de un adaptador USB OTG.

Tenga en cuenta que la función de almacenamiento masivo no se implementa en la unidad de control. Por lo tanto, no es posible atacar el sistema descargando malware desde una memoria USB u otro dispositivo de almacenamiento masivo.

## Requisitos para establecer una conexión USB o USB OTG con la unidad de control MicroLogic X

Para establecer una conexión USB con la unidad de control MicroLogic X, los requisitos previos son los siguientes:

- Debe disponer de acceso físico a la sala en la que se encuentra el interruptor automático MasterPacT MTZ con la unidad de control MicroLogic X.
- Para una conexión desde un PC:
  - Debe disponer de un cable USB con un conector mini USB para conectar su PC al puerto mini USB de la unidad de control MicroLogic X.
  - Debe disponer de un PC en el que se ejecute el software EcoStruxure Power Commission.
- Para una conexión desde un smartphone:
  - Debe disponer de un adaptador OTG con un cable USB y un conector mini USB para conectar su PC al puerto mini USB de la unidad de control MicroLogic X.
  - Debe disponer de un smartphone en el que se ejecute Aplicación EcoStruxure Power Device.

## Requisitos para establecer una conexión USB o USB OTG con la unidad de control MicroLogic Active

Para establecer una conexión USB con la unidad de control MicroLogic Active, los requisitos previos son los siguientes:

- Debe disponer de acceso físico a la sala en la que se encuentra el interruptor automático MasterPacT MTZ con MicroLogic Active.
- Para una conexión desde un PC:
  - Debe disponer de un cable USB con un conector USB-C para conectar su PC al puerto USB-C de la unidad de control MicroLogic Active.
  - Debe disponer de un PC en el que se ejecute el software EcoStruxure Power Commission.

- Para una conexión desde un smartphone:
  - Debe disponer de un adaptador OTG con un cable USB y un conector USB-C para conectar su PC al puerto USB-C de la unidad de control MicroLogic Active.

    **NOTA:** Puede usar un cable USB-C a USB-C en lugar de un adaptador OTG para conectar su smartphone a la unidad de control MicroLogic Active.
  - Debe disponer de un smartphone en el que se ejecute Aplicación EcoStruxure Power Device.

# Recomendaciones generales para proteger el acceso a través del puerto USB

Para proteger el acceso a las funciones a las que se puede acceder a través del puerto USB de la unidad de control MicroLogic X o MicroLogic Active, se recomienda:

- Instalar el interruptor automático MasterPacT MTZ en un área cerrada para que solo el personal autorizado pueda acceder a la unidad de control MicroLogic X o MicroLogic Active.
- Mantener el área cerrada en todo momento.
- Facilitar la llave o el código de acceso únicamente a personal autorizado.

Para obtener más información, consulte las recomendaciones para restringir el acceso local al interruptor automático MasterPacT MTZ, página 34.

# Recomendaciones para PC que en los que se ejecuta el software EcoStruxure Power Commission

Para proteger el acceso a la unidad de control MicroLogic X o MicroLogic Active desde un PC conectado localmente al puerto USB de la parte frontal de la unidad de control, se recomienda:

- Mantener los PC bloqueados mientras no se utilicen.
- Asegurarse de que los PC en los que se ejecute el software EcoStruxure Power Commission requieran un nombre de usuario y una contraseña.
- Aplicar el uso de contraseñas seguras, página 25.
- Asegurarse de que las contraseñas de usuario se cambien periódicamente.
- Prohibir la reutilización de contraseñas antiguas.
- Ajustar un temporizador para bloquear la pantalla del PC tras un periodo de inactividad.
- Proteger los PC siguiendo las directrices más recientes del proveedor para el sistema operativo que se ejecute en el PC.
- Limitar el número de usuarios a los que se permite utilizar el software EcoStruxure Power Commission.
- Mantener actualizadas las aplicaciones antivirus para PC.

# Recomendaciones para smartphones en los que se ejecute EcoStruxure Power Device

Para proteger el acceso a la unidad de control MicroLogic X o MicroLogic Active desde un smartphone conectado localmente al puerto USB de la parte frontal de la unidad de control, se recomienda:

- Asegurarse de que los smartphones en los que se ejecuta Aplicación EcoStruxure Power Device estén protegidos con contraseña y se utilicen solo para el trabajo.
- Proteger los smartphones en los que se haya instalado Aplicación EcoStruxure Power Device implementando todas las funciones de seguridad recomendadas por el proveedor o el fabricante del smartphone.
- Mantener actualizadas las aplicaciones antivirus para smartphones.
- No facilitar información sobre el smartphone (número de teléfono, dirección MAC) a menos que sea estrictamente necesario.
- Desconectar el smartphone de Internet durante la conexión USB OTG con la unidad de control MicroLogic X o MicroLogic Active.
- No almacenar información confidencial en un smartphone.

# Recomendaciones para la configuración de IEC 61850

Para la unidad de control MicroLogic X, utilice el protocolo FTPS para cargar el archivo de configuración IEC 61850 en la interfaz IFE o EIFE, o el servidor IFE.

# Recomendaciones para proteger el acceso a la unidad de disparo remoto MicroLogic a través del puerto de prueba

## Funciones accesibles a través del puerto de prueba mediante una interfaz de mantenimiento USB

Es posible acceder a las funciones de la unidad de disparo remoto MicroLogic conectando un PC con el software EcoStruxure Power Commission al puerto de prueba de la unidad de disparo remoto a través de la interfaz de mantenimiento USB.

La interfaz de mantenimiento USB permite conectar un PC con el software EcoStruxure Power Commission al puerto de prueba de la unidad de disparo remoto para llevar a cabo todo tipo de comprobaciones, pruebas y ajustes en la unidad de disparo MicroLogic.

La interfaz de mantenimiento USB es compatible con los siguientes dispositivos:

- Interruptores automáticos ComPacT NSX
- Interruptores automáticos PowerPacT de marcos H, J y L

## Funciones accesibles a través del puerto de prueba mediante una interfaz de servicio

Es posible acceder a las funciones de la unidad de disparo remoto MicroLogic conectando un PC con el software EcoStruxure Power Commission al puerto de prueba de la unidad de disparo remoto a través de la interfaz de servicio.

La interfaz de servicio permite conectar un PC con el software EcoStruxure Power Commission al puerto de prueba de la unidad de disparo remoto para llevar a cabo todo tipo de comprobaciones, pruebas y ajustes en la unidad de disparo remoto MicroLogic.

La interfaz de servicio es compatible con los siguientes dispositivos:

- Interruptores automáticos MasterPacT NT/NW
- Interruptores automáticos EasyPact™ MVS
- Interruptores automáticos ComPacT NS
- Interruptores automáticos PowerPacT de marcos P y R
- Interruptores automáticos ComPacT NSX
- Interruptores automáticos PowerPacT con marcos H, J y L

## Recomendaciones generales para proteger el acceso a través del puerto de prueba

Para proteger el acceso a las funciones a las que se puede acceder a través del puerto de prueba en la unidad de disparo remoto MicroLogic, se recomienda:

- Instalar el interruptor automático MasterPacT NT/NW, ComPacT o PowerPacT en un área cerrada para que solo el personal autorizado pueda acceder a la unidad de disparo MicroLogic.
- Mantener el área cerrada en todo momento.
- Facilitar la llave o el código de acceso únicamente a personal autorizado.

Para obtener más información, consulte las recomendaciones para restringir el acceso local al interruptor automático MasterPacT, ComPacT y PowerPacT, página 34.

# Recomendaciones para PC que en los que se ejecuta el software EcoStruxure Power Commission

Para proteger el acceso a la unidad de disparo remoto MicroLogic desde un PC conectado localmente al puerto de prueba de la parte frontal de la unidad de disparo remoto, se recomienda:

- Mantener los PC bloqueados mientras no se utilicen.
- Asegurarse de que los PC en los que se ejecute el software EcoStruxure Power Commission requieran un nombre de usuario y una contraseña.
- Aplicar el uso de contraseñas seguras, página 25.
- Asegurarse de que las contraseñas de usuario se cambien periódicamente.
- Prohibir la reutilización de contraseñas antiguas.
- Ajustar un temporizador para bloquear la pantalla del PC tras un periodo de inactividad.
- Proteger los PC siguiendo las directrices más recientes del proveedor para el sistema operativo que se ejecute en el PC.
- Limitar el número de usuarios a los que se permite utilizar el software EcoStruxure Power Commission.
- Mantener actualizadas las aplicaciones antivirus para PC.

# Recomendaciones para proteger el acceso a la unidad de control o disparo MicroLogic a través del Unidad de visualización FDM121

## Funciones accesibles a través de Unidad de visualización FDM121

Es posible acceder a las funciones de la unidad de control o disparo remoto MicroLogic desde el Unidad de visualización FDM121 conectado a la IMU.

En la Unidad de visualización FDM121 se muestran las mediciones, alarmas y datos de ayuda para el funcionamiento de la IMU. La Unidad de visualización FDM121 se puede utilizar para controlar los siguientes elementos:

- Un interruptor automático provisto de un mecanismo de motor
- La aplicación predefinida que ejecuta el módulo IO

La Unidad de visualización FDM121 es compatible con los siguientes dispositivos:

- Interruptores automáticos MasterPacT MTZ con unidades de control MicroLogic X
- Interruptores automáticos MasterPacT MTZ con unidades de control MicroLogic Active
- Interruptores automáticos MasterPacT NT/NW
- Interruptores automáticos ComPacT NS
- Interruptores automáticos PowerPacT de marcos P y R
- Interruptores automáticos ComPacT NSX
- Interruptores automáticos PowerPacT de marcos H, J y L

## Recomendaciones generales para proteger el acceso a través de la Unidad de visualización FDM121

Para proteger el acceso a las funciones a las que se puede acceder en la Unidad de visualización FDM121, se recomienda:

- Instalar el interruptor automático MasterPacT MTZ, ComPacT o PowerPacT y el Unidad de visualización FDM121 asociado en un área cerrada para que solo el personal autorizado pueda acceder al Unidad de visualización FDM121.
- Mantener el área cerrada en todo momento.
- Facilitar la llave o el código de acceso únicamente a personal autorizado.

Para obtener más información, consulte las recomendaciones para restringir el acceso local al interruptor automático MasterPacT MTZ, ComPacT o PowerPacT, página 34.

## Recomendaciones para proteger el acceso a la unidad de control MicroLogic Active a través del Unidad de visualización FDM121

El acceso a las unidades de control de MicroLogic Active a través de Unidad de visualización FDM121 solo está permitido en Auto Local control mode. Se recomienda ajustar el modo de control a Manual para evitar comandos intrusivos.

# Recomendaciones de ciberseguridad para el acceso remoto

## Contenido de esta parte



# Descripción general

El acceso remoto está disponible con los siguientes interruptores automáticos:

- Interruptores automáticos MasterPacT MTZ con unidades de control MicroLogic X
- Interruptores automáticos MasterPacT MTZ con unidades de control MicroLogic Active
- Interruptores automáticos MasterPacT NT/NW con unidades de disparo remoto MicroLogic
- Interruptores automáticos ComPacT
- Interruptores automáticos PowerPacT

Esta parte enumera las rutas de acceso remoto a dichos interruptores automáticos. También proporciona recomendaciones para asegurar estas rutas de acceso. Son cuestiones importantes que tener en cuenta para el funcionamiento.

# Restricción del acceso remoto al interruptor automático MasterPacT, ComPacT y PowerPacT

## Descripción general

La unidad funcional inteligente (IMU) MasterPacT, ComPacT y PowerPacT ofrece posibilidades de acceso local y remoto. Debe asegurarse de que solo se otorgue acceso a usuarios autorizados.

## Acceso remoto al interruptor automático MasterPacT, ComPacT y PowerPacT

Según la arquitectura de su sistema, probablemente haya varios modos de obtener acceso remoto al interruptor automático MasterPacT, ComPacT y PowerPacT.

Es sumamente importante controlar el acceso remoto a su sistema, pues el acceso remoto a través de las siguientes rutas de comunicación puede otorgar control total sobre su instalación:

- Software EcoStruxure Power Commission mediante una conexión Ethernet con IFE, EIFE, una interfaz IFM, un servidor IFE o un módulo BSCM Modbus SL/ULP
- Software EcoStruxure Power Commission mediante Modbus-SL con una interfaz IFM o un módulo BSCM Modbus SL/ULP
- Páginas web IFE o EIFE mediante una conexión Ethernet con una interfaz IFE o EIFE, o un servidor IFE

Concretamente, debe tener en cuenta lo siguiente:

- Cómo se puede acceder al sistema utilizando las distintas rutas de comunicación disponibles, página 14
- La información y los controles disponibles a través de cada ruta de acceso, página 23

## Protocolos compatibles

Las interfaces IFE y EIFE, y el servidor IFE, son compatibles con los siguientes protocolos de comunicación:

- HTTPS para la configuración a través de páginas web incorporadas
- Modbus TCP/IP para la comunicación con otros dispositivos de OT
- Modbus TCP por encima de TLS
- DHCP para el direccionamiento IP en la red
- DNS para la resolución de nombres de red
- SNTP para la sincronización horaria
- DPWS para la entrega de red
- SMTPS para el envío de correo electrónico
- FTPS para la configuración y notificación de eventos IEC 61850
- IEC 61850 para la comunicación con dispositivos y sistemas de subestaciones

La interfaz IFM es compatible con el protocolo de comunicación Modbus-SL.

El módulo BSCM Modbus SL/ULP es compatible con el protocolo de comunicación Modbus-SL.

Las aplicaciones MasterPacT MTZ son compatibles con los siguientes protocolos de comunicación:

- Tecnología inalámbrica Bluetooth para la comunicación con Aplicación EcoStruxure Power Device
- NFC para descargar datos de diagnóstico

# Activación y desactivación del control remoto del interruptor automático MasterPacT, ComPacT y PowerPacT

El control remoto del interruptor automático MasterPacT, ComPacT y PowerPacT hace referencia a las operaciones siguientes:

- Apertura, cierre y restablecimiento del interruptor automático
- Modificación de los ajustes del interruptor automático

Si el control remoto del interruptor automático MasterPacT, ComPacT y PowerPacT no es un requisito, es muy recomendable desactivar el control remoto utilizando las interfaces de IFE o EIFE, el servidor IFE o la interfaz de IFM. El control remoto está activado de forma predeterminada.

Si el control remoto del interruptor automático MasterPacT MTZ con la unidad de control MicroLogic Active no es un requisito, se recomienda encarecidamente ajustar el modo de control a Manual. De forma predeterminada, el modo de control del MicroLogic Active es Manual.

En la interfaz de IFE o el servidor IFE, utilice el conmutador de bloqueo del panel frontal para activar o desactivar los comandos de control remoto enviados mediante la red Ethernet.

En la interfaz de EIFE, conecte un PC en el que se ejecute el software EcoStruxure Power Commission al puerto mini MicroLogic X de la parte frontal de la unidad de control USB para activar o desactivar el control remoto del interruptor automático MasterPacT MTZ a través de la red Ethernet.

En la interfaz de IFM, utilice el conmutador de bloqueo del panel frontal para activar o desactivar los controles remotos enviados mediante la red Modbus-SL.

Para el módulo BSCM Modbus SL/ULP, conecte un PC que ejecute el software EcoStruxure Power Commission al concentrador Modbus SL y utilice el parámetro de bloqueo remoto para habilitar o deshabilitar el control remoto enviado a través de la red Modbus-SL.

# Bloqueo de los ajustes de protección (MasterPacT MTZ)

Puede bloquear los ajustes de protección del interruptor automático MasterPacT MTZ con una unidad de control MicroLogic X para evitar que se cambien remotamente. De forma predeterminada, se permite el cambio remoto de los ajustes de protección.

Se recomienda desactivar la modificación remota de los ajustes de protección si no utiliza esta función. Para obtener más información, consulte *MasterPacT MTZ - MicroLogic X* , página 8.

**NOTA:** La modificación remota de los ajustes de protección no está disponible con los interruptores automáticos MasterPacT MTZ con unidades de control MicroLogic Active.

# Desactivación de los servicios de redes IP no utilizados

Los puertos de comunicación en la interfaz IFE o EIFE, o el servidor IFE, se pueden desactivar desde las páginas web de la interfaz IFE o EIFE, o del servidor IFE.

Se recomienda:

- Deshabilitar los puertos de comunicación que no se utilicen de la interfaz IFE o EIFE.
- Acceder a las páginas web de la interfaz IFE o EIFE mediante el servicio HTTPS en lugar de HTTP.
- Acceder al software EPC mediante una puesta en marcha segura (disponible en las páginas web de la interfaz IFE o EIFE) para unidades de control MicroLogic MasterPacT MTZ y unidades de disparo ComPacT NSX MicroLogic 5, 6 o 7.

# Utilización de la lista de control de acceso (ACL)

Si se debe usar el control remoto, recomendamos utilizar la capacidad de filtrado IP de las interfaces IFE y EIFE, o del servidor IFE, para enumerar las direcciones IP de las aplicaciones (por ejemplo, SCADA) que estén autorizadas a comunicarse con la IMU. La lista de aplicaciones con autorización constituye la lista de control de acceso (ACL).

# Separación de la red OT y la red corporativa

## Descripción general

En el diseño y la implementación de su red de tecnología operativa, debe utilizar mecanismos de segregación para mantenerla separada de su red corporativa. Esto ayuda a limitar el acceso a la unidad funcional inteligente MasterPacT, ComPacT y PowerPacT.

Concretamente, debe tener en cuenta lo siguiente:

- Uso de cortafuegos
- Creación de zonas desmilitarizadas
- Uso de soluciones de sistema de detección de intrusiones (IDS) o sistema de prevención de intrusiones (IPS)
- Implementación de políticas de seguridad y programas de formación
- Definición de procedimientos de respuesta frente a incidentes

Diversas organizaciones especializadas (por ejemplo, NIST) y organismos de normalización (por ejemplo, ISO, IEC/IEEE) publican y actualizan directrices para diseñar una red de tecnología operativa y mantenerla separada de la intranet corporativa. Consulte estas publicaciones para abordar los puntos indicados anteriormente.

Además de las precauciones anteriores, debe seguir las directrices generales y las recomendaciones para la segregación de las redes que se indican en *How Can I Reduce Vulnerability to Cyber Attacks?*.

# Recomendaciones para proteger el acceso a la unidad de control o disparo MicroLogic a través de Ethernet

## Funciones accesibles a través de Ethernet

Cuando un PC en el que se ejecuta el software de supervisión y control (software SCADA, EcoStruxure Power Commission) está conectado a la red Ethernet (Modbus/TCP), se puede acceder a las funciones de la unidad de control o disparo MicroLogic en las siguientes situaciones:

- El interruptor automático MasterPacT, ComPacT y PowerPacT está conectado a través de una interfaz IFE o un servidor IFE.
- El interruptor automático MasterPacT MTZ está conectado a través de la interfaz EIFE.
- El interruptor automático MasterPacT, ComPacT y PowerPacT está conectado a través de una interfaz IFM apilada en un servidor IFE.
- El interruptor automático ComPacT NSX y PowerPacT con marcos H, J y L se conecta con un módulo BSCM Modbus SL/ULP en el modo Modbus a través de un concentrador Modbus SL al servidor IFE.

## Requisitos previos para establecer una conexión Ethernet

Para establecer una conexión Ethernet con la unidad de control o disparo MicroLogic, los requisitos previos son los siguientes:

- La unidad de control o disparo remoto MicroLogic debe estar encendida.
- La unidad de control o disparo remoto MicroLogic debe estar conectada a una red Ethernet a través de uno de los elementos siguientes:
  - Un IFE o una interfaz EIFE
  - Un servidor IFE
  - Una interfaz IFM apilada en un servidor IFE
  - Un módulo BSCM Modbus SL/ULP en modo Modbus conectado a través de un concentrador Modbus SL al servidor IFE
- Debe disponer de un PC u otro dispositivo (por ejemplo, pantalla FDM128 o PLC) en el que se ejecute el software de control y supervisión (SCADA, EcoStruxure Power Commission) conectado a la red Ethernet, que ofrezca acceso remoto
- Debe tener un PC con un navegador conectado a la red Ethernet, que ofrezca acceso a las páginas web de IFE o EIFE
- Debe disponer de un ID de usuario y una contraseña con los permisos de acceso adecuados para iniciar sesión en:
  - Páginas web de la interfaz IFE y EIFE
  - Páginas web del servidor IFE
  - Servidor FTPS para interfaces IFE y EIFE, y servidor IFE
  - El software EcoStruxure Power Commission conectado mediante interfaz IFE y EIFE, y servidor IFE
- Debe disponer de un ID de usuario y una contraseña con los permisos de acceso adecuados para iniciar sesión en el software EcoStruxure Power Commission

# Recomendaciones para PC conectados a Ethernet

Para proteger el acceso a la unidad de control o disparo remoto MicroLogic desde un PC conectado en red, se recomienda:

- Mantener los PC bloqueados mientras no se utilicen.
- Asegurarse de que el PC que ofrece acceso a la unidad de control o disparo MicroLogic mediante Ethernet (por ejemplo, a través de las páginas web de las interfaces IFE o EIFE, las páginas web del servidor IFE o SCADA) requiera un nombre de usuario y una contraseña.
- Aplicar el uso de contraseñas seguras, página 27.
- Utilice la funcionalidad de filtrado IP de las interfaces IFE y EIFE y del servidor IFE para permitir la comunicación únicamente con direcciones IP remotas seleccionadas.
- Asegurarse de que las contraseñas de usuario se cambien periódicamente.
- Prohibir la reutilización de contraseñas antiguas.
- Ajustar un temporizador para bloquear la pantalla del PC tras un periodo de inactividad.
- Proteger el PC siguiendo las directrices más recientes del proveedor para el sistema operativo que se ejecute en el PC.
- Limitar el número de usuarios a los que se permite acceder a la unidad de control o disparo remoto MicroLogic desde un PC en red.
- Mantener actualizadas las aplicaciones antivirus para PC.

Además de las precauciones anteriores, debe seguir las directrices generales y las recomendaciones para proteger la instalación que se indican en *How Can I Reduce Vulnerability to Cyber Attacks?*.

# Recomendaciones para la comunicación entre máquinas

Para sistemas compatibles con Modbus TCP TLS, active el modo de seguridad de conexión TLS en las páginas web de la interfaz IFE o EIFE, o del servidor IFE.

La comunicación segura máquina a máquina requiere componentes que se conecten a la interfaz IFE o EIFE, o al servidor IFE, para ser compatibles con la comunicación Modbus Secure.

# Recomendaciones para los registros de seguridad

Para asegurarse de que los registros de seguridad se descarguen regularmente, utilice:

- La función de exportación automática de registros a través del servicio Syslog desde la interfaz IFE o EIFE, o el servidor IFE.
- Exportación manual del registro en formato CSV desde la interfaz IFE o EIFE, o el servidor IFE.

# Recomendaciones para proteger el acceso a la unidad de control o disparo MicroLogic a través de Modbus-SL

## Funciones accesibles a través de Modbus-SL

Cuando un PC que ejecuta un software de supervisión y control (SCADA) está conectado a la red Modbus-SL, se puede acceder a las funciones de la unidad de disparo o la unidad de control MicroLogic en los siguientes casos:

- El interruptor automático MasterPacT, ComPacT y PowerPacT está conectado a una interfaz IFM.
- Los interruptores automáticos ComPacT NSX y PowerPacT con marcos H-, J- o L- están conectados al módulo BSCM Modbus SL/ULP en el modo Modbus.

## Requisitos previos para establecer una conexión Modbus-SL

Para establecer una conexión Modbus-SL con la unidad de control o disparo MicroLogic, los requisitos previos son los siguientes:

- La unidad de control o disparo remoto MicroLogic debe estar encendida.
- La unidad de disparo o la unidad de control MicroLogic debe estar conectada a una interfaz IFM o un módulo BSCM Modbus SL/ULP en el modo Modbus.
- Debe disponer de un PC u otro dispositivo (por ejemplo, PLC) en el que se ejecute el software de control y supervisión (SCADA) conectado a la red Modbus-SL, que ofrezca acceso remoto.
- Debe disponer de un ID de usuario y una contraseña con los permisos de acceso adecuados para iniciar sesión en el software EcoStruxure Power Commission.

## Recomendaciones para PC conectados a Modbus-SL

Para proteger el acceso a la unidad de control o disparo remoto MicroLogic desde un PC conectado en red, se recomienda:

- Mantener los PC bloqueados mientras no se utilicen.
- Asegurarse de que el PC que ofrece acceso a la unidad de control o disparo MicroLogic mediante Modbus-SL (por ejemplo, a través de SCADA) requiera un nombre de usuario y una contraseña.
- Aplicar el uso de contraseñas seguras, página 27.
- Asegurarse de que las contraseñas de usuario se cambien periódicamente.
- Prohibir la reutilización de contraseñas antiguas.
- Ajustar un temporizador para bloquear la pantalla del PC tras un periodo de inactividad.
- Proteger el PC siguiendo las directrices más recientes del proveedor para el sistema operativo que se ejecute en el PC.
- Limitar el número de usuarios a los que se permite acceder a la unidad de control o disparo remoto MicroLogic desde un PC en red.
- Mantener actualizadas las aplicaciones antivirus para PC.

Además de las precauciones anteriores, debe seguir las directrices generales y las recomendaciones para proteger la instalación que se indican en *How Can I Reduce Vulnerability to Cyber Attacks?*.

# Recomendaciones para proteger el acceso a través de la tecnología inalámbrica Zigbee (MasterPacT MTZ)

## Versión Zigbee

Las unidades de control MicroLogic Active AP/EP están certificadas para Zigbee 3.0.

## Funciones accesibles a través de la tecnología inalámbrica Zigbee

Con la comunicación Zigbee puede supervisar los datos desde la unidad de control MicroLogic Active AP/EP desde un Panel Server Advanced (PAS800), Panel Server Universal (PAS600) o Panel Server Entry (PAS400).

Los datos transferidos a través de la tecnología inalámbrica Zigbee se cifran utilizando el algoritmo de cifrado AES de 128 bits.

**NOTA:** La tecnología inalámbrica Zigbee no está disponible en las unidades de control MicroLogic X.

## Requisitos previos para establecer una conexión Zigbee

Los requisitos previos para establecer una conexión Zigbee son los siguientes:

- El Panel Server debe estar encendido.
- La unidad de control MicroLogic Active AP/EP y el Panel Server deben estar muy cerca.
- Para el emparejamiento selectivo, debe proporcionar el ID de Zigbee, que se muestra en la página de destino de Go2SE o en la pantalla de visualización del MicroLogic Active.

Para saber el procedimiento detallado de cómo establecer una conexión Zigbee, consulte el capítulo Puesta en marcha de las Guías del usuario del interruptor automático *MasterPacT MTZ con unidad de control MicroLogic Active*, página 8.

## Recomendaciones generales para proteger el acceso a través de la tecnología inalámbrica Zigbee

Para proteger el acceso a las funciones a las que se puede acceder a través de la tecnología inalámbrica Zigbee, se recomienda:

- Instalar el interruptor automático MasterPacT MTZ en un área cerrada para que solo el personal autorizado pueda acceder a la unidad de control MicroLogic Active.
- Mantener el área cerrada en todo momento.
- Facilitar la llave o el código de acceso únicamente a personal autorizado.

Para obtener información adicional sobre cómo proteger el acceso al interruptor automático MasterPacT MTZ, consulte Implementación de una política de acceso restringido, página 34.

# Recomendaciones para utilizar la tecnología inalámbrica Zigbee

La comunicación inalámbrica Zigbee es vulnerable a interrupciones por emisiones de radio no autorizadas en el entorno operativo. Para proteger el acceso a funciones accesibles mediante la comunicación inalámbrica Zigbee, se recomienda que:

- La unidad de control MicroLogic Active AP/EP no esté conectada a redes malintencionadas.
- La red de Zigbee se revise periódicamente para asegurarse de que todos los dispositivos sean válidos.
- La red de Zigbee se repare si algún dispositivo no es válido.
- La puesta en marcha de los dispositivos inalámbricos Zigbee se realiza en un lugar protegido de los transmisores de radio no autorizados, como una sala de administración.
- El emparejamiento solo debe realizarse cuando sea necesario y en una zona segura.

# Recomendaciones para el uso de Panel Server

Consulte el capítulo Recomendaciones de ciberseguridad de DOCA0172•• *EcoStruxure Panel Server - Guía del usuario*, página 8.

# Recomendaciones de ciberseguridad para actualizaciones de firmware y Digital Module

## Contenido de esta parte

# Instalación de actualizaciones de firmware

## Descripción general

Un ciberataque cada vez más común consiste en la distribución de paquetes de software manipulados o ilegítimos que pueden contener aplicaciones modificadas o adicionales. Estas aplicaciones pueden poner en peligro la integridad del software original y su uso previsto.

Para garantizar la integridad y autenticidad de los componentes de la MasterPacT, ComPacT y PowerPacT IMU (es decir, la unidad de control MicroLogic X o MicroLogic Active; el servidor IFE, IFE, EIFE; la interfaz IFM; el módulo BSCM Modbus SL/ULP, BCIM, IO, y Unidad de visualización FDM121), el firmware original Schneider Electric está firmado digitalmente.

Actualice el firmware con el software EcoStruxure Power Commission. Debe tener la última versión del software EcoStruxure Power Commission. Utilice el software EcoStruxure Power Commission para actualizar el firmware a través del menú del firmware.

## Recomendaciones de ciberseguridad referentes a actualizaciones de firmware

**⚠ADVERTENCIA**

**RIESGO DE FUNCIONAMIENTO IMPREVISTO**

- Actualice la versión del software EcoStruxure Power Commission en cuanto reciba una notificación que le indique que hay una actualización disponible.
- Utilice esta última versión del software EcoStruxure Power Commission para actualizar el firmware de todos sus productos.
- Consulte de forma periódica la lista de revocación de certificados que se publica en el sitio web oficial de Schneider Electric. Si hay un certificado revocado para uno de sus productos, no instale firmware de una fecha anterior a la de la revocación.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

Cuando se instalen actualizaciones de firmware de los componentes de la IMU MasterPacT, ComPacT y PowerPacT, se recomienda lo siguiente:

- Solo use la última versión del software EcoStruxure Power Commission para descargar e instalar las actualizaciones del firmware.
- Proteja el PC en el que se ejecuta el software EcoStruxure Power Commission siguiendo las directrices más recientes del proveedor para el sistema operativo.
- Instale las actualizaciones aplicando prácticas de tecnología operativa (TO) aceptadas, como realizar pruebas en un entorno que no sea de producción (si está disponible) para garantizar la validación antes de instalar e implementar las actualizaciones en su sistema de producción.

Consulte las notas de la versión del firmware, página 8 correspondientes para comprobar si la actualización más reciente ofrece mejoras de ciberseguridad. Si es así, le recomendamos que se actualice a esta versión.

# Firmware firmado

El firmware diseñado para la unidad de control MicroLogic X, la unidad de control MicroLogic Active y los módulos ULP se firma mediante la infraestructura de clave pública (PKI) de Schneider Electric. Las firmas digitales se autentican mediante el certificado público incluido en el software EcoStruxure Power Commission.

Cuando se carga el firmware en un dispositivo mediante el software EcoStruxure Power Commission, también se verifica automáticamente la firma digital del paquete de actualización. Esta verificación se realiza con el certificado público presente en cada dispositivo.

Por motivos de seguridad, los certificados públicos están sujetos a cambios. Por lo tanto, deberá comprobar que la versión del software EcoStruxure Power Commission que utiliza para descargar e instalar las actualizaciones del firmware sea la más reciente. Si cuenta con la última versión del software EcoStruxure Power Commission, los certificados públicos utilizados para firmar el firmware están actualizados.

Los certificados que ya no son válidos se publican en la lista de revocación de certificados (CRL) disponible en el sitio web oficial de Schneider Electric.

# Ventajas del uso del software EcoStruxure Power Commission para las actualizaciones de firmware

El software EcoStruxure Power Commission desempeña una función importante para ayudar a garantizar la integridad de su red de tecnología operativa durante las actualizaciones de firmware. Utilice solo la última versión del software EcoStruxure Power Commission para descargar e instalar el firmware, ya que es el único software que puede ofrecer las siguientes ventajas:

- Al descargar los paquetes de firmware en la unidad de control MicroLogic X, la unidad de control MicroLogic Active o el módulo ULP desde el centro de descargas oficial de Schneider Electric mediante el software EcoStruxure Power Commission, se verifica automáticamente la firma digital de los paquetes.
- Al cargar el firmware en la unidad de control MicroLogic X, la unidad de control MicroLogic Active o el módulo ULP mediante el software EcoStruxure Power Commission a través de una conexión USB o Ethernet, la firma digital del paquete de actualización se verifica automáticamente.

Las verificaciones automáticas realizadas por el software EcoStruxure Power Commission dependen completamente de la validez del certificado público que utiliza.

Consulte *MicroLogic Trip Units and Control Units - Firmware History*, página 8 para obtener los procedimientos detallados en los que se explica cómo actualizar el firmware de MicroLogic.

# Compra e instalación de Digital Modules (MasterPacT MTZ)

## Descripción general

Digital Modules son módulos opcionales que amplían las funciones disponibles a través de la gama de unidades de control MicroLogic X. Se pueden comprar junto con el interruptor automático MasterPacT MTZ en el pedido inicial o posteriormente contactando con el Centro de Atención al Cliente.

Los Digital Modules diseñados para la unidad de control Schneider Electric están firmados digitalmente para aumentar la seguridad utilizando la infraestructura de clave pública (PKI) de MicroLogic X. La PKI ayuda a garantizar tanto la autenticidad como la integridad de estas descargas. Los Digital Modules se deben instalar utilizando el software EcoStruxure Power Commission.

**NOTA:** Los Digital Modules no son compatibles con unidades de control MicroLogic Active.

## Recomendaciones de ciberseguridad para la instalación de Digital Modules

**⚠ADVERTENCIA**

**RIESGO DE FUNCIONAMIENTO IMPREVISTO**

- Actualice la versión del software EcoStruxure Power Commission en cuanto reciba una notificación que le indique que hay una actualización disponible.
- Utilice esta última versión del software EcoStruxure Power Commission para actualizar el firmware de todos sus productos.
- Consulte de forma periódica la lista de revocación de certificados que se publica en el sitio web oficial de Schneider Electric. Si hay un certificado revocado para uno de sus productos, no instale firmware de una fecha anterior a la de la revocación.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

Cuando instale Digital Modules para la unidad de control MicroLogic X, se recomienda:

- Instalar Digital Modules que se ciñan a las prácticas de tecnología operativa (OT) aceptadas, como la prueba en un entorno que no sea de producción, para su validación antes de instalarlos e implementarlos en el sistema de producción.
- Usar solo la última versión del software EcoStruxure Power Commission para descargar e instalar Digital Modules.
- Proteger los PC utilizados para descargar e instalar Digital Modules siguiendo las directrices más recientes del proveedor para el sistema operativo.

Solo debe usar el software EcoStruxure Power Commission para instalar Digital Modules en la unidad de control MicroLogic X.

El software EcoStruxure Power Commission desempeña una función importante para ayudar a garantizar la integridad de la red de tecnología operativa. Utilice solo la última versión del software EcoStruxure Power Commission para instalar Digital Modules, ya que es el único software que puede ofrecer las siguientes ventajas:

- Cuando actualice el firmware de un dispositivo de IMU usando el software EcoStruxure Power Commission con una conexión USB o Ethernet, la firma digital de la actualización del firmware se verifica automáticamente.
- Cuando se carga un Digital Module en la unidad de control MicroLogic X mediante el software EcoStruxure Power Commission a través de una conexión USB, la firma digital del Digital Module se verifica automáticamente.

Las verificaciones automáticas realizadas por el software EcoStruxure Power Commission dependen completamente de la validez del certificado público utilizado.

Consulte DOCA0144EN *MasterPacT MTZ - MicroLogic X Control Unit - Firmware Release Notes* para ver los procedimientos detallados que explican cómo descargar e instalar Digital Modules.

# Cybersecurity Support Portal de Schneider Electric

## Descripción general

El Schneider Electric de cybersecurity support portal describe la política de gestión de vulnerabilidad de Schneider Electric.

El objetivo de la política de gestión de vulnerabilidad de Schneider Electric es abordar las vulnerabilidades en la ciberseguridad que afectan productos y sistemas de Schneider Electric para proteger las soluciones instaladas, los clientes y el entorno.

Schneider Electric trabaja junto a investigadores, equipos de CERT (del inglés Cyber Emergency Response Team, equipo de respuesta ante ciberemergencias) y propietarios de equipos para asegurar que se proporcione información precisa de manera oportuna para proteger correctamente las instalaciones.

Schneider ElectricEl equipo CPCERT (del inglés Corporate Product Cyber Emergency Response Team, equipo de respuesta ante ciberemergencias para productos corporativos) de es responsable de administrar y emitir alertas sobre vulnerabilidades y mitigaciones que afectan a productos y soluciones.

El CPCERT coordina las comunicaciones entre los CERT pertinentes, los investigadores independientes, los gerentes de productos y todos los clientes afectados.

## Información disponible en Cybersecurity Support Portal de Schneider Electric

Cybersecurity Support Portal brinda lo siguiente:

- Información sobre vulnerabilidades de ciberseguridad de los productos
- Información sobre incidentes de ciberseguridad
- Una interfaz que permite a los usuarios declarar incidentes o vulnerabilidades de ciberseguridad

# Recomendaciones de ciberseguridad para la eliminación o retiro

Las interfaces EIFE e IFE y el servidor IFE contienen información confidencial configurada durante la puesta en marcha, valores de datos recientes y registros. Por ejemplo, esta información puede incluir contraseñas o consumos de energía medidos.

Es necesario realizar un restablecimiento de fábrica antes de desechar el equipo EIFE o la IFE interfaz, o el IFE servidor. Para obtener más información, consulte la guía del usuario correspondiente a su interfaz.

# Glosario

## B

**BCIM:**

El módulo BCIM permite la comunicación entre la unidad de control MicroLogic Active y otros módulos ULP en un sistema ULP.

**Bluetooth Low Energy:**

Una tecnología de red de área personal inalámbrica que reduce el consumo de energía.

## C

**Código de emparejamiento:**

Código formado por números que se utiliza para verificar la identidad de la persona en cuestión al establecer una conexión Bluetooth.

**Conectividad ULP:**

ULP es un enlace rápido de comunicación dedicado a la supervisión y el control de interruptores automáticos. Conecta el interruptor automático a una interfaz de Ethernet o a un módulo IO. ULP funciona a una velocidad de 1 Mb/s y es plug and play.

## F

**FTP: protocolo de transferencia de archivos:**

Protocolo de red que proporciona la capacidad para transferir archivos de un equipo a otro a través de Internet.

**FTPS - Protocolo seguro de transferencia de archivos:**

Variante de la versión estándar del protocolo de transferencia de archivos (FTP) que añade una capa de seguridad a los datos en tránsito mediante una conexión de protocolo de capa de sockets seguros (SSL) o seguridad de la capa de transporte (TLS).
.

## H

**HMI: interfaz hombre-máquina:**

Hace referencia a las pantallas de la parte frontal de un dispositivo que un operador puede utilizar para leer información o configurar el dispositivo.

**HTTP: protocolo de transferencia de hipertexto:**

Protocolo de red que gestiona la entrega de archivos y datos en la World Wide Web.

**HTTPS: protocolo seguro de transferencia de hipertexto:**

Variante del protocolo de transferencia web estándar (HTTP) que añade una capa de seguridad a los datos que se transportan a través de una conexión de protocolo de capa de sockets seguros (SSL) o seguridad de la capa de transporte (TLS).

## I

**IMU: unidad funcional modular inteligente:**

El interruptor automático con sus componentes de comunicación internos (unidad de control o disparo remoto MicroLogic) y los módulos ULP externos (módulo IO) conectados a una interfaz de comunicación recibe el nombre de unidad funcional modular inteligente (IMU).

**Interfaz de IFM:**

La interfaz Modbus-SL de IFM permite que una IMU se conecte a una red Modbus de línea serie RS 485 de dos hilos. Cada IMU tiene su propia interfaz IFM y dirección Modbus correspondiente.

**Interfaz EIFE:**

Interfaz de Ethernet integrada que es un módulo opcional del interruptor automático seccionable MasterPacT MTZ. Este módulo permite acceder al interruptor automático a través de una red Ethernet. El acceso a las páginas web de la interfaz EIFE y al servidor FTPS EIFE se autoriza en función del mecanismo de control de acceso basado en roles (RBAC).

**Interfaz IFE:**

Interfaz de IFE Ethernet para un interruptor automático que se puede conectar al interruptor automático MasterPacT, ComPacT o PowerPacT. Este módulo permite acceder al interruptor automático a través de una red Ethernet. El acceso a las páginas web de la interfaz IFE y al servidor FTPS IFE se autoriza en función del mecanismo de control de acceso basado en roles (RBAC).

**IP : protocolo de Internet:**

Las direcciones IP se utilizan para identificar dispositivos conectados a la intranet de la empresa o a Internet.

## L

**LAN: red de área local:**

Hace referencia a la intranet o la red de TI de la empresa.

## M

**Modbus TCP/IP:**

Protocolo que proporciona comunicación cliente/servidor entre dispositivos y TCP/IP que proporciona comunicaciones a través de una conexión Ethernet.

**Módulo BSCM Modbus SL/ULP:**

El módulo BSCM Modbus SL/ULP con referencia comercial LV434220 es un módulo de control de estado de los interruptores que puede utilizarse para comunicar datos mediante la red de comunicación de línea serie Modbus o la red de comunicación ULP.

## N

**NFC - Near field communication:**

Hace referencia a un protocolo de comunicación inalámbrica.

## O

**OT: tecnología operativa:**

Hace referencia a los sistemas de hardware y software que la empresa utiliza para supervisar y controlar directamente los procesos y equipos de producción, lo que también se conoce como red de control industrial (IC). OT se suele utilizar para hacer referencia a la red operativa de la empresa, en contraposición a su red de TI.

## P

**PKI: infraestructura de clave pública:**

Define un conjunto de servicios que se utilizan para generar y autenticar firmas digitales. Una infraestructura de clave pública está diseñada para garantizar la confidencialidad, la integridad y la autenticidad de la información.

**Política de seguridad:**

La política de seguridad de un sistema es la configuración de seguridad aplicada en todo el sistema protegido. Las políticas de seguridad suelen hacer referencia al uso de normas. Se usan para definir la configuración de seguridad compartida por todos los dispositivos.

**Protocolo IEC 61850:**

Estándar para redes de comunicaciones y sistemas de subestaciones. Basado en el protocolo Ethernet, se trata de un método de comunicación estandarizado, desarrollado para dar soporte a sistemas integrados compuestos por dispositivos electrónicos inteligentes (IED) autodescriptivos multifabricante. Estos sistemas están conectados entre sí a través de una red para llevar a cabo funciones de protección en tiempo real, control, medición y supervisión.

## R

**RBAC: control de acceso basado en funciones:**

Método para asignar diferentes niveles de acceso según los elementos a los que da acceso la función definida por el usuario.

## S

**SCADA - Supervisory control and data acquisition:**

Hace referencia a los sistemas diseñados para obtener datos en tiempo real sobre los procesos y equipos de producción para supervisarlos y controlarlos remotamente.

**Servidor IFE:**

Servidor de panel IFE Ethernet que se puede conectar a más de un interruptor automático MasterPacT MTZ. Este módulo permite acceder a los interruptores automáticos a través de una red Ethernet.

## T

**TCP/IP - Transmission control protocol/Internet protocol:**

Hace referencia al conjunto de protocolos que se utilizan para las comunicaciones por Internet.

**TI: tecnologías de la información:**

Hace referencia a los sistemas de información y a la red de información de la empresa en contraposición a su red de OT (tecnología operativa).

## V

**VPN: red privada virtual:**

Las VPN se utilizan para establecer un "túnel" protegido o privado entre un punto de acceso externo autenticado y la red empresarial de confianza.

## Z

**Zigbee:**

Un protocolo de comunicación inalámbrica que cumple el estándar Zigbee.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

Debido a que las normas, especificaciones y diseños cambian periódicamente, solicite la confirmación de la información dada en esta publicación.



DOCA0122ES-11