# Gestor de tipos de dispositivos de comunicación de Modbus TCP

## Manual de usuario

02/2019

EIO0000000369.06

www.schneider-electric.com

La información que se ofrece en esta documentación contiene descripciones de carácter general y/o características técnicas sobre el rendimiento de los productos incluidos en ella. La presente documentación no tiene como objeto sustituir dichos productos para aplicaciones de usuario específicas, ni debe emplearse para determinar su idoneidad o fiabilidad. Los usuarios o integradores tienen la responsabilidad de llevar a cabo un análisis de riesgos adecuado y completo, así como la evaluación y las pruebas de los productos en relación con la aplicación o el uso de dichos productos en cuestión. Ni Schneider Electric ni ninguna de sus filiales o asociados asumirán responsabilidad alguna por el uso inapropiado de la información contenida en este documento. Si tiene sugerencias de mejoras o modificaciones o ha hallado errores en esta publicación, le rogamos que nos lo notifique.

Usted se compromete a no reproducir, salvo para su propio uso personal, no comercial, la totalidad o parte de este documento en ningún soporte sin el permiso de Schneider Electric, por escrito. También se compromete a no establecer ningún vínculo de hipertexto a este documento o su contenido. Schneider Electric no otorga ningún derecho o licencia para el uso personal y no comercial del documento o de su contenido, salvo para una licencia no exclusiva para consultarla "tal cual", bajo su propia responsabilidad. Todos los demás derechos están reservados.

Al instalar y utilizar este producto es necesario tener en cuenta todas las regulaciones sobre seguridad correspondientes, ya sean regionales, locales o estatales. Por razones de seguridad y para garantizar que se siguen los consejos de la documentación del sistema, las reparaciones solo podrá realizarlas el fabricante.

Cuando se utilicen dispositivos para aplicaciones con requisitos técnicos de seguridad, siga las instrucciones pertinentes.

Si con nuestros productos de hardware no se utiliza el software de Schneider Electric u otro software aprobado, pueden producirse lesiones, daños o un funcionamiento incorrecto del equipo.

Si no se tiene en cuenta esta información, se pueden causar daños personales o en el equipo.

© 2019 Schneider Electric. Reservados todos los derechos.

# Tabla de materias


| | | |
|---|---|---|
| | **Información de seguridad** | 5 |
| | **Acerca de este libro** | 7 |
| Capítulo 1 | **Requisitos de hardware y software** | 9 |
| | Requisitos del sistema | 10 |
| | Compatibilidad | 11 |
| | Instalación y desinstalación | 12 |
| Capítulo 2 | **Tipos de conexión y modelos de comunicación** | 13 |
| | Tipo de conexión | 14 |
| | Modelo de comunicación | 15 |
| Capítulo 3 | **Interfaz Gráfica de Usuario** | 17 |
| | Interfaz gráfica de usuario | 17 |
| Capítulo 4 | **Configuración** | 21 |
| | Ficha Configuración | 22 |
| | Ficha de tiempo de ejecución | 24 |
| | Tabla de direcciones | 28 |
| | Configuración de la exploración | 30 |
| Capítulo 5 | **Ciberseguridad** | 33 |
| | ¿Qué es la ciberseguridad? | 34 |
| | Directrices de Schneider Electric | 36 |
| **Glosario** | | 39 |
| **Índice** | | 43 |

# Información de seguridad

## Información importante

### AVISO

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 LO SIGUIENTE:

La instalación, el manejo, las revisiones y el 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 de este libro

## Presentación

### Objeto

Este manual de usuario tiene como objetivo describir la utilización del gestor de tipos de dispositivos de comunicación (Comm DTM) para Modbus.

### Campo de aplicación

Este documento se ha actualizado con la publicación de la Modbus Communication Library V2.6.9.

### Información relativa al producto

**⚠ ADVERTENCIA**

**PÉRDIDA DE CONTROL**

- El diseñador del esquema de control debe tener en cuenta las posibles modalidades de fallo de rutas de control y, para ciertas funciones de control críticas, proporcionar los medios para lograr un estado seguro durante y después de un fallo de ruta. Algunas funciones de control críticas son, por ejemplo, la parada de emergencia y la parada de sobrecarrera, un corte de alimentación o un reinicio.
- Para las funciones críticas de control deben proporcionarse rutas de control separadas o redundantes.
- Las rutas de control del sistema pueden incluir enlaces de comunicación. Deben tenerse en cuenta las implicaciones de retardos de transmisión imprevistos o fallos del enlace.
- Tenga en cuenta todas las reglamentaciones para la prevención de accidentes y las normativas de seguridad locales.[1]
- Cada instalación de este equipo debe probarse de forma individual y exhaustiva antes de entrar en servicio.

**El incumplimiento de estas instrucciones puede causar la muerte, lesiones serias o daño al equipo.**

[1] Para obtener información adicional, consulte NEMA ICS 1.1 (última edición), "Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control" (Directrices de seguridad para la aplicación, la instalación y el mantenimiento del control de estado estático) y NEMA ICS 7.1 (última edición), "Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems" (Estándares de seguridad para la construcción y guía para la selección, instalación y utilización de sistemas de unidades de velocidad ajustable) o su equivalente aplicable a la ubicación específica.

# Capítulo 1
# Requisitos de hardware y software

## Contenido de este capítulo

Este capítulo contiene los siguientes apartados:


| Apartado | Página |
|---|---|
| Requisitos del sistema | 10 |
| Compatibilidad | 11 |
| Instalación y desinstalación | 12 |

# Requisitos del sistema

## Requisitos de hardware

| Requisito | Mínimo | Recomendado |
|---|---|---|
| Ordenador | Pentium 4 o equivalente | |
| RAM | 1 GB | 2 GB |
| Espacio libre en el disco duro de la unidad del sistema | 100 MB | |
| Espacio libre en el disco duro de la unidad de instalación | 100 MB | |
| Archivo de intercambio | 1024 MB | 2048 MB |
| Monitor | 256 colores SVGA con resolución de 800x600 | Color verdadero XGA con resolución de 1.024 x 768 |

## Requisitos de software

Sistemas operativos de software

| Sistema operativo | Edición/Service Pack | Consideraciones especiales |
|---|---|---|
| Windows 7 32 bits | SP1 | Necesita derechos de acceso de administrador para instalar Modbus TCP Comm DTM |
| Windows 7 64 bits | SP1 | |
| Windows 8.1, 10 Professional | – | |

Software instalado en el PC

| Software | Edición | Consideraciones especiales |
|---|---|---|
| Microsoft.NET Framework | V2.0 SP2 | – |
| Aplicación de trama de FDT | FDT 1.2 o FDT 1.2.1 | Modbus TCP Comm DTM requiere una aplicación de trama de FDT compatible con el estándar FDT. La aplicación de trama de FDT debe ser compatible con Microsoft.NET Framework 2.0. |

# Compatibilidad

## Compatibilidad con FDT

Modbus Comm DTM es compatible con los estándares FDT 1.2 y FDT 1.2.1. Se basa en FDT Modbus anexo 1.0.

## Compatibilidad de Modbus

Modbus Comm DTM es compatible con los servicios de Modbus especificados en el protocolo de aplicación Modbus especificación V1.1b.

# Instalación y desinstalación

## Instalación

Haga doble clic en el archivo *setup.exe* y siga las instrucciones del asistente de instalación.

## Eliminación

Para desinstalar el DTM del equipo, seleccione **Inicio → Configuración → Panel de control → Agregar o quitar programas**.

# Capítulo 2
# Tipos de conexión y modelos de comunicación

## Introducción

En este capítulo se ofrece una descripción general de las diversas configuraciones que pueden utilizarse para establecer las comunicaciones con Modbus.

## Contenido de este capítulo

Este capítulo contiene los siguientes apartados:


| Apartado | Página |
|---|---|
| Tipo de conexión | 14 |
| Modelo de comunicación | 15 |

# Tipo de conexión

## Introducción

Modbus TCP Comm DTM permite establecer una comunicación Modbus basada en el tipo de conexión siguiente.

## Conexión TCP

Modbus TCP Comm DTM ofrece la posibilidad de establecer una comunicación Modbus por TCP. La conexión se establecerá mediante el adaptador de red Ethernet del PC.

# Modelo de comunicación

## Introducción

En este capítulo se describe el modelo de comunicación compatible con Modbus TCP Comm DTM.

**NOTA:** La tecnología FDT no se ha diseñado para la transferencia de datos en tiempo real. En función del sistema y del modelo de comunicación que utilice, puede que los datos no reflejen el estado real del dispositivo en tiempo real.

**⚠ ADVERTENCIA**

**INFORMACIÓN SOBRE EL ESTADO DEL DISPOSITIVO NO VÁLIDA**

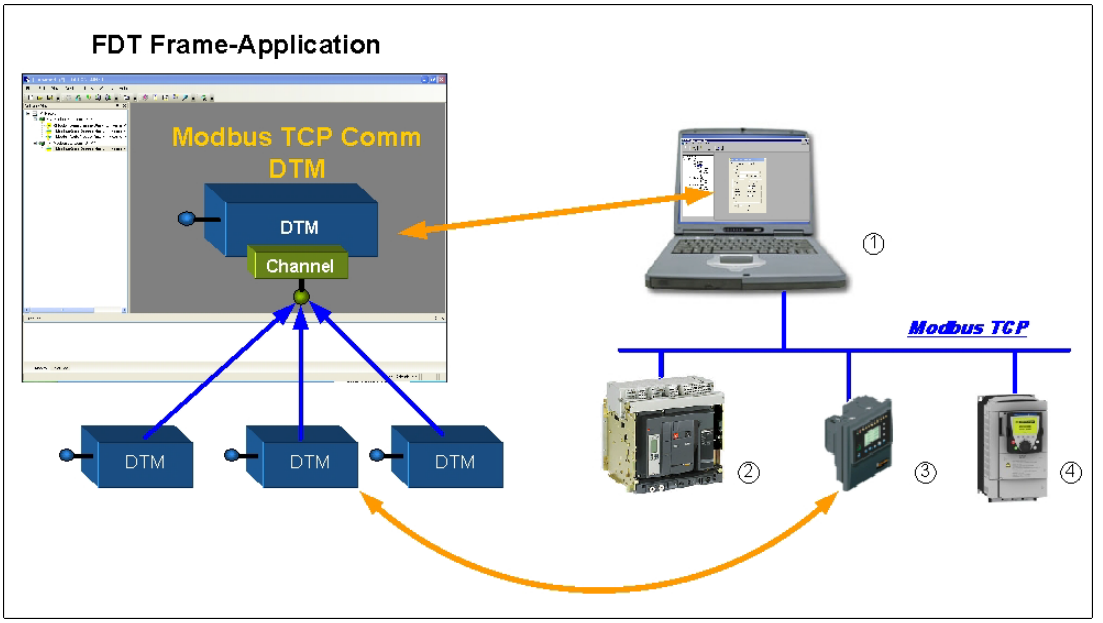
No utilice Modbus Comm DTM para tareas de control o supervisión dependientes del tiempo, porque es posible que los datos transferidos no reflejen el estado real del dispositivo. La tecnología FDT no se ha diseñado para este fin.

**El incumplimiento de estas instrucciones puede causar la muerte, lesiones serias o daño al equipo.**

## Conexión de red

Modbus TCP Comm DTM se puede utilizar para establecer una comunicación Modbus entre el PC y el dispositivo de destino mediante una red Ethernet.

En esta configuración, Modbus TCP Comm DTM actúa como un cliente Modbus.




**1** PC con Modbus TCP Comm DTM
**2 - 4** dispositivos de destino

# Capítulo 3
# Interfaz Gráfica de Usuario

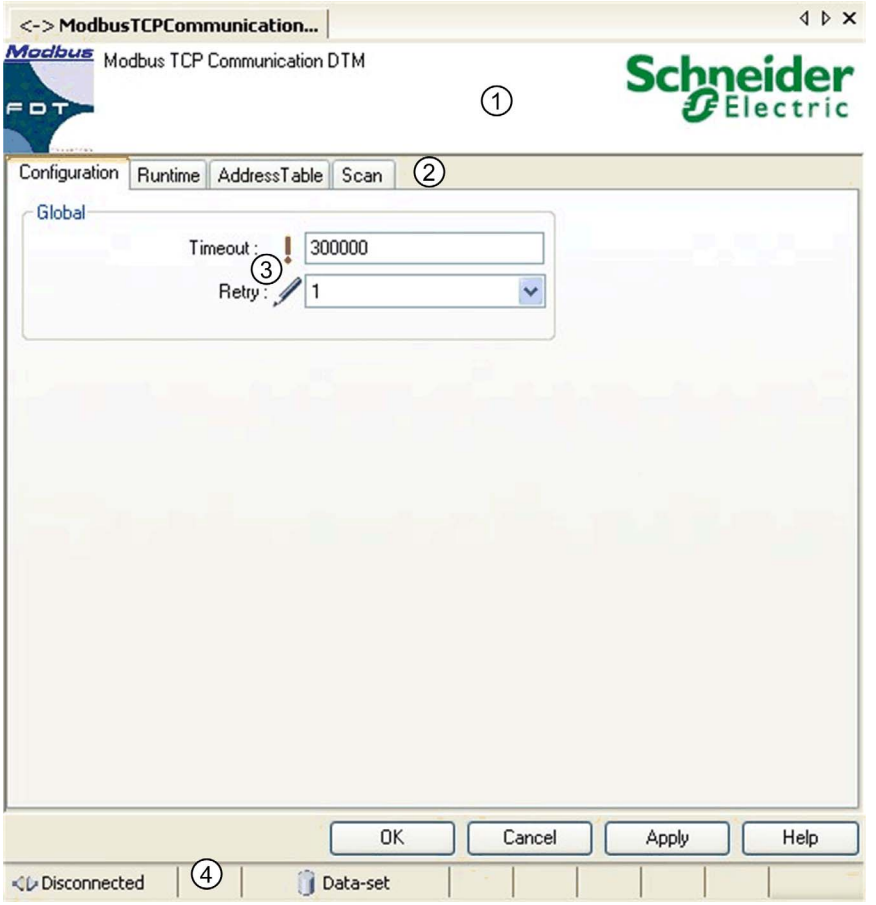
## Interfaz gráfica de usuario

### Descripción general

En este capítulo se describe la interfaz gráfica de usuario (GUI) de Modbus TCP Comm DTM.

## Introducción

En la figura siguiente se muestra la GUI (interfaz gráfica de usuario) de DTM.




1 Área de identificación
2 Menú de fichas
3 Iconos de estado de parámetros
4 Barra de estado

## Área de identificación

El área de identificación muestra el nombre y la versión del DTM.

## Menú de fichas

Utilice el menú Ficha para acceder a las diversas funciones del DTM.

## Iconos de estado de parámetros

Los iconos de estado de los parámetros proporcionan información sobre el estado actual del parámetro

Posibles estados de parámetros

| Icono | Significado |
|---|---|
|  | El parámetro se ha modificado y tiene un valor no válido. |
|  | El parámetro se ha modificado y tiene un valor válido. |

## Barra de estado

La barra de estado ofrece información sobre el estado actual del DTM.

Posibles estados de conexión

| Icono | Texto | Significado | Estado del DTM |
|---|---|---|---|
|  | Conectando | conectando | pasando a online |
|  | Conectado | conectado | online |
|  | Desconectando | desconectando | pasando a offline |
|  | Interrumpido | interrumpido | interrupción de comunicación detectada |
|  | Desconectado | desconectado | el resto de estados |

Posibles estados de origen de datos

| Icono | Texto | Funcionamiento |
|---|---|---|
|  | Conjunto de datos | Los valores visualizados se cargan del conjunto de datos de la instancia. Los valores modificados afectan sólo en el conjunto de datos de la instancia. |
|  | Conjunto de datos bloqueado. | Los valores visualizados se cargan del conjunto de datos de la instancia. El conjunto de datos está bloqueado. |

# Capítulo 4
# Configuración

## Contenido de este capítulo

Este capítulo contiene los siguientes apartados:


| Apartado | Página |
|---|---|
| Ficha Configuración | 22 |
| Ficha de tiempo de ejecución | 24 |
| Tabla de direcciones | 28 |
| Configuración de la exploración | 30 |

# Ficha Configuración

## Introducción

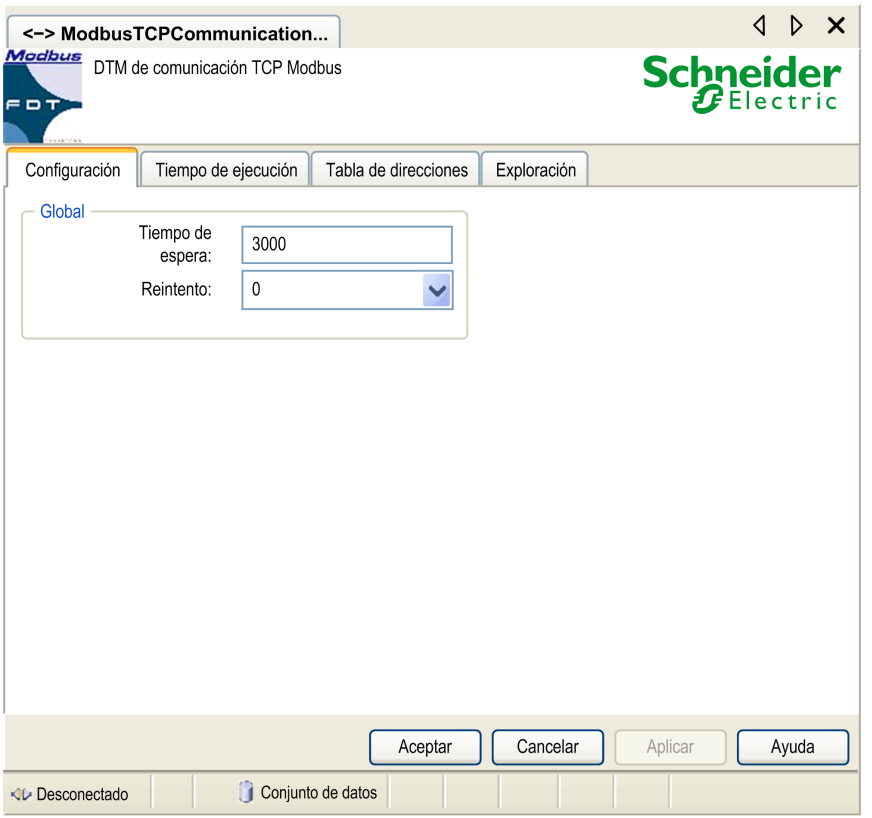
La ficha **Configuración** de Modbus TCP Comm DTM contiene los parámetros de comunicación.

## Ficha Configuración

Existen varias posibilidades para acceder a la ficha **Configuración** de Modbus TCP Comm DTM:

- En la vista de la red de la aplicación de trama de FDT, haga doble clic en el icono Modbus TCP Comm DTM.
- En la vista de la red de la aplicación de trama de FDT, haga doble clic en el icono Modbus TCP Comm DTM y luego haga clic en **Configuración**.

En la figura siguiente se muestra la ficha **Configuración** del cuadro de diálogo de Modbus TCP Comm DTM:



## Parámetros de comunicación

La tabla contiene una descripción de los parámetros de comunicación para una conexión Modbus TCP.

| Parámetro | Descripción | Valor predeterminado |
|---|---|---|
| **Timeout global** | Timeout de respuesta del servidor Modbus. | 3.000 ms |
| **Número de reintentos** | Número de veces que Modbus TCP Comm DTM reenviará la petición Modbus en la conexión TCP si se ha producido un timeout en la comunicación. | 0 |

## Comandos de configuración

Comandos de configuración disponibles en la ficha **Configuración**

| Comando | Descripción |
|---|---|
| **Aceptar** | Se guardarán los parámetros y la ventana Modbus TCP Comm DTM se cerrará. Los nuevos valores de parámetros se aplicarán en la conexión siguiente. |
| **Cancelar** | Se cancelarán las modificaciones de parámetros y la ventana Modbus TCP Comm DTM se cerrará. Los valores originales se aplicarán en la conexión siguiente. |
| **Aplicar** | Almacena los parámetros pero la ventana Modbus TCP Comm DTM permanece abierta. Los nuevos valores de parámetros se aplicarán en la conexión siguiente. |

# Ficha de tiempo de ejecución

## Introducción

Modbus TCP Comm DTM facilita varios tipos de información de tiempo de ejecución. En este capítulo se describe la información proporcionada por Modbus TCP Comm DTM y la configuración de la función de registro.

## Ficha de tiempo de ejecución

Modbus TCP Comm DTM facilita varios tipos de información de tiempo de ejecución, que se puede utilizar para supervisar las comunicaciones establecidas.

La información del tiempo de ejecución está disponible en la ficha **Tiempo de ejecución** de Modbus TCP Comm DTM, a la cual se puede acceder de la forma siguiente:

- En la vista de red de la aplicación de trama de FDT, haga doble clic en el icono de Modbus TCP Comm DTM. Ahora seleccione la ficha **Tiempo de ejecución**.
- En la vista de red de la aplicación de trama de FDT, haga doble clic en el icono de Modbus TCP Comm DTM y luego en **Configuración**. Ahora seleccione la ficha **Tiempo de ejecución**.

En la figura siguiente se muestra la ficha **Tiempo de ejecución** del cuadro de diálogo de Modbus TCP Comm DTM:




## Comandos de configuración

La tabla siguiente contiene una descripción de los comandos de configuración disponibles en la ficha **Tiempo de ejecución**.

| Comando | Descripción |
|---|---|
| **Aceptar** | Se guardan los parámetros y se cierra la ventana Modbus TCP Comm DTM. Los nuevos valores de los parámetros se aplicarán en la siguiente conexión. |

| Comando | Descripción |
|---|---|
| **Cancelar** | Se cancelan las modificaciones de los parámetros y se cierra la ventana Modbus TCP Comm DTM. Los valores originales se aplicarán en la siguiente conexión. |
| **Examinar** | Abre un explorador de archivos para especificar la ruta del archivo de registro. |
| **Resetear** | Restablece a cero todos los parámetros de tiempo de ejecución. |
| **Aplicar** | Guarda los parámetros, pero la ventana Modbus TCP Comm DTM permanece abierta. Los nuevos valores de los parámetros se aplicarán en la siguiente conexión. |

## Parámetros de tiempo de ejecución

La tabla siguiente contiene una descripción de los parámetros de tiempo de ejecución disponibles en la ficha **Tiempo de ejecución** de Modbus TCP Comm DTM:

| Comando | Descripción |
|---|---|
| **Conexiones** | Número de conexiones activas con Modbus TCP Comm DTM. |
| **Mensajes enviados** | Número de mensajes enviados por Modbus TCP Comm DTM. |
| **Mensajes recibidos** | Número de mensajes recibidos por Modbus TCP Comm DTM. |
| **Excepciones** | Número de mensajes de excepción de Modbus recibidos por Modbus TCP Comm DTM. |
| **Tiempos de espera excedidos** | Número de errores de tiempo de espera excedido detectados durante la recepción. |

## Archivo de registro

Modbus TCP Comm DTM permite crear un archivo de registro. En el cuadro **Archivo de registro** debe especificar la ruta en la que se almacenará el archivo de registro.

En la tabla siguiente se describe la información que se escribirá en el archivo de registro según la **modalidad de registro** seleccionada:

| Modalidad de registro | Descripción |
|---|---|
| **Desactivado** | Deshabilita la función de archivo de registro. |
| **Registro de errores** | En el archivo de registro se escribirá sólo información sobre errores de tiempo de espera excedido y excepciones de Modbusrecibidas. |

| Modalidad de registro | Descripción |
|---|---|
| **Registro general** | Además de la información sobre los errores de tiempo de espera excedido y las excepciones de Modbus recibidas, en el archivo de registro también se escribe la información sobre las peticiones Modbus enviadas y las respuestas de Modbus recibidas, así como las peticiones recibidas del DTM de dispositivo. |

## Recomendación para mejorar la ciberseguridad

El archivo de registro suele contener datos sensibles tales como
- Direcciones de dispositivos
- Nombres de dispositivos
- Detalles de la tipología de red
- Detalles de la configuración de red

Se almacena en el disco duro del PC. Se elimina el archivo de registro en cuanto ya no es necesario o se almacena en un lugar seguro, en el que no es posible el acceso sin autorización.

# Tabla de direcciones

## Introducción

Modbus Comm DTM facilita una tabla de direcciones que muestra los DTM de dispositivo conectados y sus direcciones de destino. En este capítulo se describe la información proporcionada en la tabla de direcciones y la configuración de las direcciones de destino de los dispositivos.

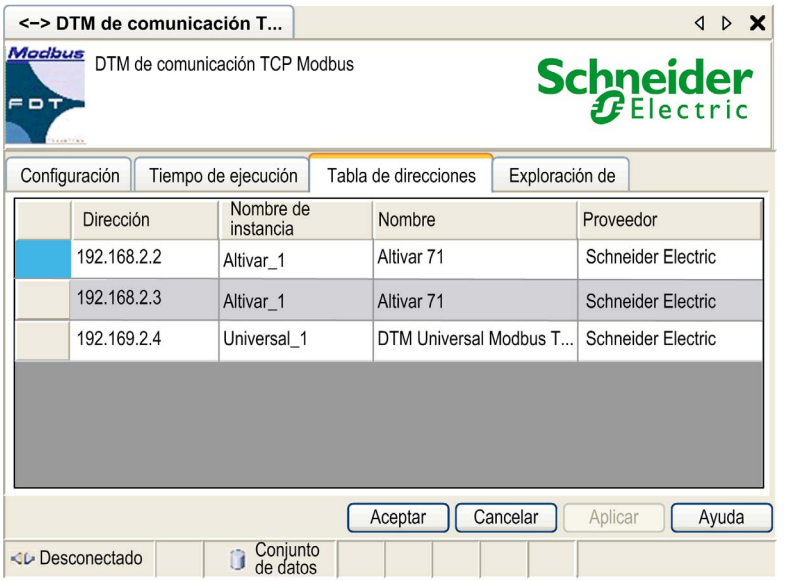
## Tabla de direcciones

Modbus TCP Comm DTM facilita una tabla de direcciones que muestra los DTM de dispositivo conectados y sus direcciones de destino. En esta tabla de direcciones se pueden especificar las direcciones de destino de los DTM de dispositivo conectados.

Se puede acceder a la ficha **Tabla de direcciones** de la manera siguiente:

- En la vista de la red de la aplicación de trama de FDT, haga doble clic en el icono Modbus TCP Common DTM. Ahora seleccione la ficha **Tabla de direcciones**.
- En la **vista de red** de la aplicación de trama de FDT, haga clic con el botón derecho del ratón en el icono Modbus TCP Comm DTM y luego haga clic en **Configuración**. Ahora seleccione la ficha **Tabla de direcciones**.

En la figura siguiente se muestra la ficha **Tabla de direcciones** del cuadro de diálogo de Modbus TCP Comm DTM:



## Comandos de configuración

La tabla contiene una descripción de los comandos de configuración disponibles en la ficha **Tabla de direcciones**

| Comando | Descripción |
|---|---|
| **Aceptar** | Se guardarán las modificaciones y la ventana Modbus TCP Comm DTM se cerrará. Los valores nuevos se aplicarán en la conexión siguiente. |
| **Cancelar** | Se cancelan las modificaciones y la ventana Modbus TCP Comm DTM se cerrará. Los valores originales se aplicarán en la conexión siguiente. |
| **Aplicar** | Almacena las modificaciones pero la ventana Modbus TCP Comm DTM permanece abierta. Los valores nuevos se aplicarán en la conexión siguiente. |

## Información de dirección

La tabla contiene una descripción de la información de dirección disponible en la ficha **Tabla de direcciones** de Modbus TCP Comm DTM:

| Parámetro | Descripción |
|---|---|
| **Dirección** | Dirección de destino del dispositivo de hardware, que se configurará con el DTM conectado |
| **Nombre de instancia** | Nombre de la instancia del DTM |
| **Nombre** | Nombre específico del DTM |
| **Proveedor** | Nombre del proveedor de DTM |

## Asignación de dirección

Se puede utilizar la tabla de direcciones de Modbus TCP Comm DTM para especificar la dirección de destino del dispositivo de hardware, que se configurará con un DTM específico. Para especificar la dirección de destino debe escribir la nueva dirección en el campo **Dirección** correspondiente de este DTM y validar esta modificación haciendo clic en el botón **Aplicar** o **Aceptar**.

# Configuración de la exploración

## Introducción

Modbus Comm DTM facilita la posibilidad de especificar el rango de las direcciones exploradas para la exploración de FDT. En este capítulo se describe la configuración de los parámetros de exploración para la exploración de FDT.

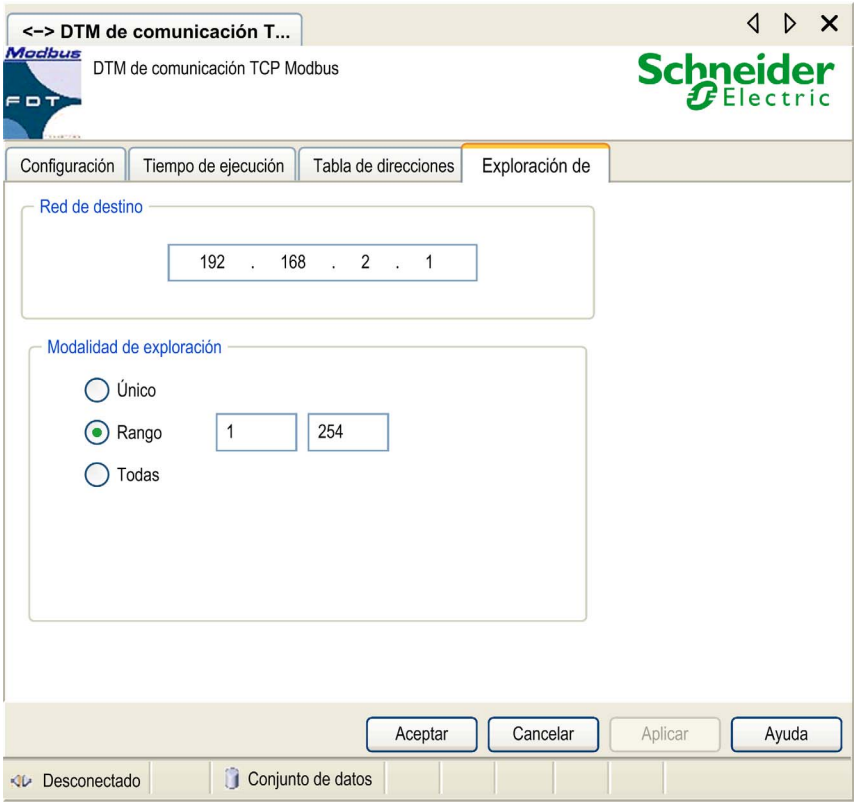
## Ficha de exploración

Modbus TCP Comm DTM es compatible con la función de exploración tal como se define en la especificación FDT V1.2.1. La exploración permite generar de forma automática la topología de la red de comunicaciones subyacente. Modbus TCP Comm DTM facilita la posibilidad de especificar el rango de las direcciones exploradas.

Los parámetros de exploración están disponibles en la ficha **Exploración** de Modbus TCP Comm DTM, a la cual se puede acceder de la forma siguiente:

- En la **vista de red** de la aplicación de trama de FDT, haga doble clic en el icono Modbus TCP Comm DTM. Ahora seleccione la ficha **Exploración**.
- En la **vista de red** de la aplicación de trama de FDT, haga clic con el botón derecho del ratón en el icono Modbus TCP Comm DTM y luego haga clic en **Configuración**. Ahora seleccione la ficha **Exploración**.

En la figura se muestra la ficha **Explorar** del cuadro de diálogo de Modbus TCP Comm DTM:




## Comandos de configuración

La tabla contiene una descripción de los comandos de configuración disponibles en la ficha **Explorar**:

| Comando | Descripción |
|---|---|
| **Aceptar** | Se guardarán las modificaciones y la ventana Modbus Comm DTM se cerrará. Los valores nuevos se aplicarán en la exploración siguiente. |
| **Cancelar** | Se cancelarán las modificaciones y la ventana Modbus Comm DTM se cerrará. Los valores originales se aplicarán en la exploración siguiente. |
| **Aplicar** | Almacena las modificaciones pero la ventana Modbus Comm DTM permanece abierta. Los valores nuevos se aplicarán en la exploración siguiente. |

## Parámetros de exploración para Modbus TCP

La tabla contiene una descripción de los parámetros de exploración disponibles en la ficha **Explorar** de Modbus TCP Comm DTM Comm DTM:

| Comando | Descripción | |
|---|---|---|
| **Red de destino** | Especifica el rango de red que se va a explorar. | |
| **Modalidad de exploración** | **Única** | Explora solo una dirección de un dispositivo de destino del rango 0 a 255 del rango de red especificado. |
| | **Rango** | Explora un rango de direcciones especificado entre 0 y 255 en el rango de red definido. |
| | **Todo** | Explora el rango de direcciones completo del rango de red (todas la direcciones entre 0 y 255). |

# Capítulo 5
# Ciberseguridad

## Introducción

La ciberseguridad es una rama de la administración de redes que se ocupa de los ataques en o desde sistemas informáticos que pueden causar interrupciones accidentales o intencionadas. El objetivo de la ciberseguridad es contribuir a aumentar los niveles de protección de la información y los activos físicos ante el robo, la corrupción, el uso inapropiado o los accidentes, al tiempo que se mantiene el acceso para sus usuarios previstos.

Ningún método de ciberseguridad es apropiado por sí solo. Schneider Electric recomienda un método de defensa exhaustivo. Concebido por la National Security Agency (NSA), este método protege la red en varias capas con funciones de seguridad, dispositivos y procesos. Los componentes básicos de este método son:

- evaluación del riesgo
- un plan de seguridad elaborado según los resultados de la evaluación de riesgo
- una campaña de formación en varias fases
- separación física de las redes industriales y las redes de empresa utilizadas en una zona desmilitarizada (DMZ) y rutas de acceso para establecer otras zonas de seguridad
- control de acceso al sistema
- endurecimiento del dispositivo
- seguimiento y mantenimiento de la red

En este capítulo se definen los elementos que le ayudan a configurar un sistema menos susceptible a sufrir ciberataques. Para mayor información acerca del método de defensa exhaustivo, consulte *TVDA: How Can I Reduce Vulnerability to Cyber Attacks in the Control Room* en *Schneider Electric website*.

## Contenido de este capítulo

Este capítulo contiene los siguientes apartados:


| Apartado | Página |
|---|---|
| ¿Qué es la ciberseguridad? | 34 |
| Directrices de Schneider Electric | 36 |

# ¿Qué es la ciberseguridad?

## Introducción

Las ciberamenazas son acciones deliberadas o accidentes que pueden interrumpir el funcionamiento normal de redes y sistemas informáticos. Estas acciones pueden iniciarse desde dentro del sitio físico o desde una localización externa. Los desafíos a la seguridad para el entorno de control incluyen:

- diversos límites físicos y lógicos
- múltiples sitios y grandes áreas geográficas
- efectos adversos de la implementación de seguridad en la disponibilidad de procesos
- mayor exposición a gusanos y virus al migrar de los sistemas empresariales a los sistemas de control, a medida que las comunicaciones de control empresarial se vuelven más abiertas
- mayor exposición a software malintencionado desde dispositivos USB, ordenadores portátiles de proveedores y servicio técnico, y red empresarial
- impacto directo de los sistemas de control en sistemas mecánicos y físicos

## Fuentes de ciberataques

Implemente un plan de ciberseguridad que pueda contrarrestar varias fuentes potenciales de ciberataques e incidentes, incluyendo:

| Origen | Descripción |
|---|---|
| interno | ● comportamiento inapropiado del empleado o contratista<br>● empleado o contratista insatisfecho |
| oportunista externo (no dirigido) | ● script kiddies*<br>● hackers aficionados<br>● programadores de virus |
| deliberado externo (dirigido) | ● grupos criminales<br>● activistas<br>● terroristas<br>● agencias de estados extranjeros |
| accidental | |
| * término anglófono en jerga para designar a hackers que utilizan scripts malintencionados programados por otros sin poseer un conocimiento exhaustivo de su funcionamiento o su impacto potencial en un sistema. | |

Un ciberataque deliberado sobre un sistema de control puede ser ejecutado para conseguir una serie de resultados maliciosos, entre ellos:

- perturbar el proceso productivo bloqueando o retrasando el flujo de información.
- dañar, deshabilitar o apagar el equipo para que la producción tenga un impacto negativo en el entorno
- modificar o deshabilitar los sistemas de seguridad para causar un daño intencionado

## ¿Cómo consiguen acceder los atacantes?

Un ciberatacante elude las defensas del perímetro para obtener acceso a la red del sistema de control. Los puntos de acceso comunes incluyen:

- acceso de marcación a los dispositivos de la unidad de terminal remoto (RTU)
- puntos de acceso del proveedor (como los puntos de acceso del soporte técnico)
- productos de red controlados informáticamente
- red privada virtual de empresa (VPN)
- vínculos de la base de datos
- cortafuegos mal configurados
- servicios compartidos

## Certificaciones de ciberseguridad

Schneider Electric ha desarrollado unas directrices de ciberseguridad según las siguientes recomendaciones:

- Achilles
- ISA Secure

## Preguntas

Para hacernos llegar cualquier pregunta sobre ciberseguridad, informar de cualquier problema de seguridad o obtener información actualizada de Schneider Electric, visite nuestro *website*.

# Directrices de Schneider Electric

## Introducción

El sistema de su PC puede ejecutar varias aplicaciones para mejorar la seguridad en su entorno de control. El sistema viene con una configuración predeterminada de fábrica que debe reconfigurarse para que coincida con la recomendación de Schneider Electric de emplear un método de defensa exhaustivo para el endurecimiento de los dispositivos.

En las siguientes directrices se describen procedimientos llevados a cabo en un sistema operativo Windows 7. Solamente se recogen a modo de ejemplo. Su sistema operativo y aplicación podrían necesitar procedimientos o requisitos diferentes.

## Deshabilitar tarjetas de interfaz de red no utilizadas

Verifique que las tarjetas de interfaz de red que no necesite la aplicación estén deshabilitadas. Por ejemplo, si su sistema tiene 2 tarjetas y la aplicación utiliza solo una, verifique que la otra tarjeta de red (conexión de área local 2) está deshabilitada.

Para deshabilitar una tarjeta de red en Windows 7:

| Paso | Acción |
|---|---|
| 1 | Abra **Panel de control → Redes e Internet → Centro de redes y recursos compartidos → Cambiar configuración del adaptador**. |
| 2 | Haga clic con el botón derecho en la conexión no utilizada. Seleccione **Deshabilitar**. |

## Configurar la conexión de área local

Varias configuraciones de red de Windows proporcionan una mayor seguridad de acuerdo con el método de defensa exhaustivo que recomienda Schneider Electric.

En los sistemas Windows 7, acceda a estos ajustes abriendo **Panel de control → Redes e Internet → Centro de redes y recursos compartidos → Cambiar configuración del adaptador → Conexión de área local (x).**

Esta lista es un ejemplo de los cambios en la configuración que podría realizar en su sistema en la pantalla **Propiedades de conexión de área local**:

- Deshabilite todas las pilas IPv6 en sus respectivas tarjetas de red. (Este ejemplo de sistema no requiere el rango de direcciones de IPv6, y si se deshabilitan las pilas IPV6 se limita la vulnerabilidad a los posibles riesgos de seguridad para el IPv6).
- Deshabilite **Uso compartido de archivos e impresoras para la red de Microsoft**.

Las recomendaciones de Schneider Electric para una defensa exhaustiva incluyen:

- Definir solo direcciones IPv4, máscaras de subred y pasarelas estáticas.
- No utilice DHCP ni DNS en la sala de control.

### Administrar el cortafuegos de Windows

El método de defensa exhaustivo de Schneider Electric recomienda entre otras cosas habilitar el cortafuegos principal de Windows en cada uno de los PC del sistema. Habilite los cortafuegos para cualquier perfil público o privado de la lista.

Se recomienda que el usuario defina las reglas de cortafuegos que rechacen las conexiones desde o hacia cualquier host externo desconocido/no seguro.

### Deshabilitar el protocolo de escritorio remoto

El método de defensa exhaustivo de Schneider Electric recomienda deshabilitar el protocolo de escritorio remoto (RDP) a menos que su aplicación requiera el uso del RDP. En los siguientes pasos se explica cómo deshabilitar el protocolo:

| Paso | Acción |
|---|---|
| 1 | En Windows 2008R2 o Windows 7, deshabilite RDP a través de **Equipo → Propiedades del sistema → Configuración avanzada del sistema**. |
| 2 | En la ficha **Acceso remoto**, deseleccione la casilla de verificación **Permitir conexiones de Asistencia remota a este equipo**. |
| 3 | Seleccione la casilla de verificación **No permitir las conexiones a este equipo**. |

### Actualizar las directivas de seguridad

Actualice las directivas de seguridad de los PC en su sistema escribiendo `gpupdate` en una ventana de comando. Para obtener más información, consulte la documentación de Microsoft sobre `gpupdate`.

### Deshabilitar LANMAN y NTLM

El protocolo Microsoft LAN Manager (LANMAN o LM) y su sucesor NT LAN Manager (NTLM) presentan vulnerabilidades que hacen desaconsejable su uso en aplicaciones de control.

En los siguientes pasos se describe cómo deshabilitar LM y NTLM en un sistema Windows 7 o Windows 2008R2:

| Paso | Acción |
|---|---|
| 1 | En una ventana de comandos, ejecute `secpol.msc` para abrir la ventana **Directiva de seguridad local**. |
| 2 | Abra **Configuración de seguridad → Directivas locales → Opciones de seguridad**. |
| 3 | Seleccione **Enviar sólo respuesta NTLMv2 y rechazar LM y NTLM** en el campo **Seguridad de red: nivel de autenticación de LAN manager**. |
| 4 | Seleccione la casilla **Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña**. |
| 5 | En una ventana de comando, escriba `gpupdate` para realizar el cambio de directivas de seguridad. |

## Administrar actualizaciones

Antes de la implementación, actualice todos los sistemas operativos del PC utilizando las herramientas de la página web **Windows Update** de Microsoft. Para acceder a esta herramienta en Windows 2008R2, Windows 7 o Windows XP, seleccione **Inicio** → **Todos los programas** → **Windows Update**.

# Glosario

## C

**código de función**

Conjunto de instrucciones que ordenan a uno o varios dispositivos esclavo de una o varias direcciones especificadas que realicen un tipo de acción, por ejemplo, leer un conjunto de registros de datos y responder con el contenido de estos.

**configuración**

Organización e interconexión de los componentes de hardware en un sistema y la selección de hardware y software que determina las características operativas del sistema.

**CRC**

comprobación de redundancia cíclica (del inglés, Cyclic Redundancy Check)

Los mensajes que aplican este mecanismo de comprobación de error disponen de un campo CRC que se calcula mediante el transmisor según el contenido del mensaje. Los nodos receptores recalculan el campo. Una falta de coincidencia entre los dos códigos indica una diferencia entre el mensaje transmitido y el recibido.

## D

**DTM**

Un DTM (gestor de tipos de dispositivo, en inglés "Device Type Manager") es un tipo de controlador de dispositivo proporcionado por el proveedor del dispositivo de campo. El DTM contiene la información específica del dispositivo y facilita una interfaz gráfica de usuario. El DTM puede utilizarse para realizar tareas de supervisión y tareas de configuración en el dispositivo específico. Un DTM no es una aplicación autónoma. Requiere una aplicación de trama FDT para ejecutarse.

## E

**Ethernet**

Especificación de señalización y cableado de LAN utilizada para conectar dispositivos dentro de un área definida como, por ejemplo, un edificio. Ethernet utiliza un bus o una topología en estrella para conectar diferentes nodos en una red.

# F

**FDT**

La tecnología FDT (herramienta para dispositivos de campo, en inglés "Field Device Tool") estandariza la interfaz de comunicaciones entre los dispositivos de campo y los sistemas (*www.fdtgroup.org*).

# I

**interfaz**

La interfaz representa la conexión física a la red, por ejemplo, una tarjeta de red o un convertidor de USB a RS 232.

**IP**

Protocolo de Internet.

Parte de la familia de protocolos TCP/IP que realiza el seguimiento de las direcciones de Internet de los nodos, encamina los mensajes salientes y reconoce los mensajes entrantes.

# L

**LAN**

Siglas del inglés Local Area Network (red de área local).

Red de comunicaciones de datos de corta distancia.

# M

**MB**

Abreviatura de Modbus

**Modbus**

Modbus es un protocolo de mensajes de la capa de aplicación. Modbus ofrece numerosos servicios especificados por códigos de función.

**modelo maestro/esclavo**

La dirección de control en una red que aplica el modelo maestro/esclavo va del maestro a los dispositivos esclavos.

# P

**pasarela**

Programa o hardware que transmite datos entre redes

## S

**SL**

Abreviatura de línea serie

## T

**TCP**

Acrónimo del inglés Transmission Control Protocol (protocolo de control de transmisión).

Protocolo de capa de transporte orientado a la conexión que proporciona una transmisión fiable de datos de dúplex completo. TCP es una parte del conjunto de protocolos TCP/IP.

**telegrama**

Paquete de datos utilizado en comunicaciones en serie.

# Índice


## C

ciberseguridad, *33*
- certificaciones, *34*
- conexión de área local, *36*
- cortafuegos, *37*
- directrices, *36*
- escritorio remoto, *37*
- introducción, *34*
- LANMAN/NTLM, *37*
- tarjetas de interfaz de red, *36*

compatibilidad, *11*
conexión
- red, *15*
- TCP, *14*
- tipo, *14*

configuración de la exploración, *30*

## F

ficha configuración, *22*
ficha de tiempo de ejecución, *24*

## I

instalación, *12*
interfaz de usuario, *17*
interfaz gráfica de usuario, *17*

## M

modalidad de exploración, *30*
modelo de comunicación, *15*

## N

número de reintentos, *23*

## R

requisitos
- hardware, *10*
- software, *10*

## T

tabla de direcciones, *28*