



Ordene este documento
como UM-90925
Rev. A

UM-90925

Dto. de Ingeniería

SISTEMA AUTONOMO CON PATROL IP

Manual de Usuario

VERSION 1.0
PRELIMINAR

1. Descripción General.

El sistema autónomo es una alternativa para utilizar los equipos Celletech (RVA400, RVA600, IIP100) sin hacer uso del servicio que Celletech brinda a sus clientes (comunicaciones, Gateway, acceso a monitoreo o configuración desde la web, etc.), dejando al cliente a cargo de la administración de las líneas de sus equipos y funcionamiento de las comunicaciones que intervienen en el sistema.

La implementación de un sistema autónomo se puede dividir en dos etapas:

- Instalación y configuración del Patrol IP y elementos que intervienen en la estación de monitoreo.
- Configuración e instalación de los equipos remotos, que serán instalados en los distintos abonados de la estación de monitoreo.

En la figura 1 se pueden ver los distintos elementos que intervienen en el sistema.

[UM-90925 – Rev. A](#)

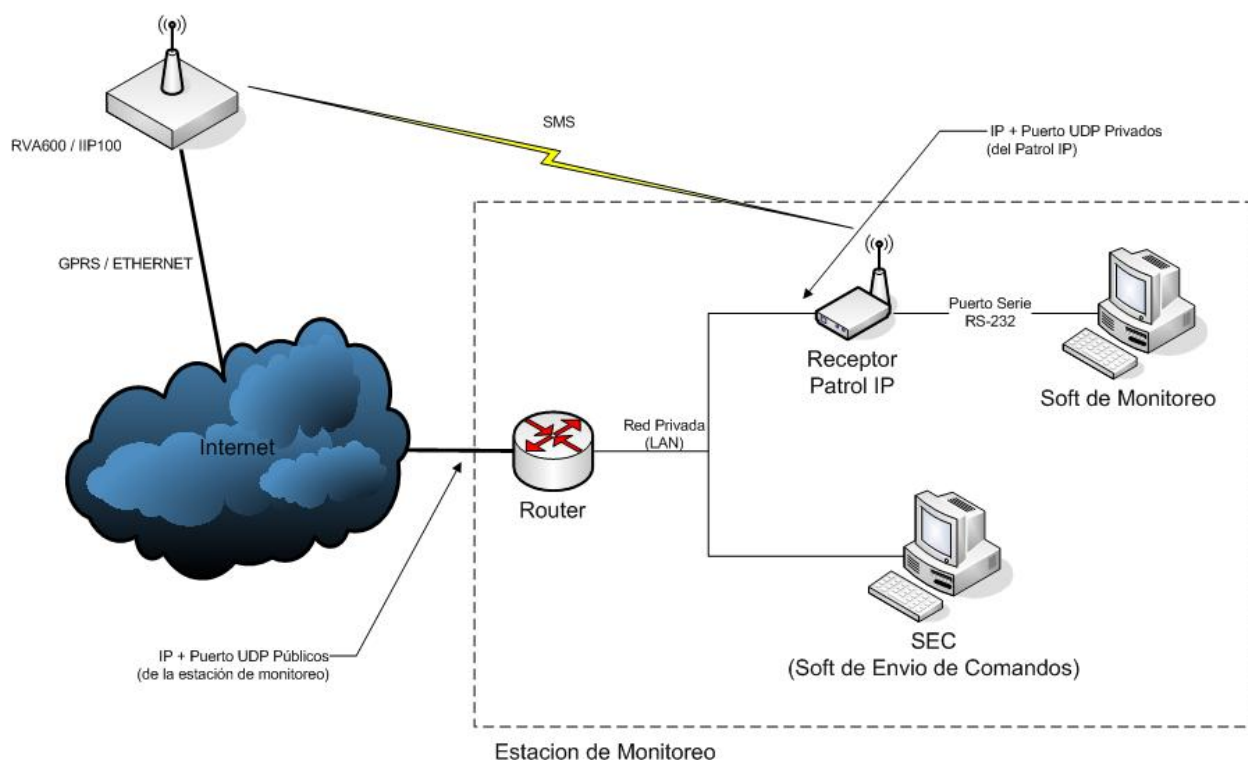


Figura 1. Esquema del Sistema Autónomo.

2. Configuración del Patrol IP.

La implementación del sistema autónomo requiere que se disponga de dos servicios fundamentales:

- **Conexión a Internet con una IP fija** en la estación de monitoreo.
- **Línea celular con servicio SMS habilitado**, para asignar al Patrol IP.

Estos requisitos son necesarios, para poder luego configurar a los distintos equipos para que transmitan por GPRS a la IP pública de la estación de monitoreo, o por SMS directo a la línea cargada en el Patrol IP.

Antes de continuar con la guía, se recomienda leer atentamente el **manual de usuario del Patrol IP (UM-90620)**, donde se detalla su instalación y configuración, y se explica como debe conectarse a la PC para ser configurado por el puerto serie utilizando algún programa de comunicaciones, como por ejemplo el Hyperterminal de Windows (se recuerda que la configuración por defecto es 9600-8-N-1, sin control de flujo).

Luego de encender el Patrol IP se debe entrar al modo programación como se detalla en su manual, y configurar los distintos parámetros del mismo. A continuación se indican los parámetros más importantes que deben ser configurados (para una descripción completa recuerde ver el manual del Patrol IP, punto 4):

- “**Modo de Protocolo**”: para configurar la comunicación con el software de monitoreo, puede ser conectado a Monitor II (Modo 1) o a cualquier otro software emulando un receptor genérico (Modo 2).
- “**IP Local**”: el Patrol IP estará conectado en la red privada de la estación de monitoreo. Se deberá asignar una IP estática disponible, perteneciente a la red privada para el Patrol IP (Ej.: 192.168.0.100).
- “**Mascara de Subred**”: este parámetro dependerá de la configuración de la red privada de la estación de monitoreo (por lo general es 255.255.255.0).
- “**Default Gateway**”: puerta de enlace predeterminada, que dependerá de la configuración de la red privada de la estación de monitoreo (Ej.: 192.168.0.1).
- “**Local Port**”: es el puerto UDP del Patrol IP por el cual recibirá los mensajes entrantes de los distintos equipos remotos (valor por defecto: 11500).

Una vez configurado el Patrol IP, y habiendo conectado ya el cable de red y la antena, el mismo quedará listo para recibir los mensajes provenientes desde los equipos remotos, solo resta configurar el router o firewall que exista en la red local. Para ello, **debe redireccionar un puerto UDP público a la IP y puerto local configurados en el Patrol IP**, para permitirle recibir los mensajes provenientes de Internet. Se recomienda utilizar el mismo puerto para evitar confusiones. Es decir, si se configuró el “Local Port” del Patrol IP con el valor “11500”, utilizar ese mismo puerto como el puerto público.

3. Configuración de los equipos.

Mediante la herramienta de configuración “Config Manager”, se pueden configurar todos los parámetros propios de los distintos modelos de equipo de Celletech, antes de ser instalados. Este software se puede ejecutar en cualquier PC que tenga un puerto serie disponible, para conectar a través del mismo el equipo a configurar, utilizando el cable de conexión accesorio que viene incluido con el Patrol IP (conector DB9 hembra y RJ45/RJ11 en sus extremos).

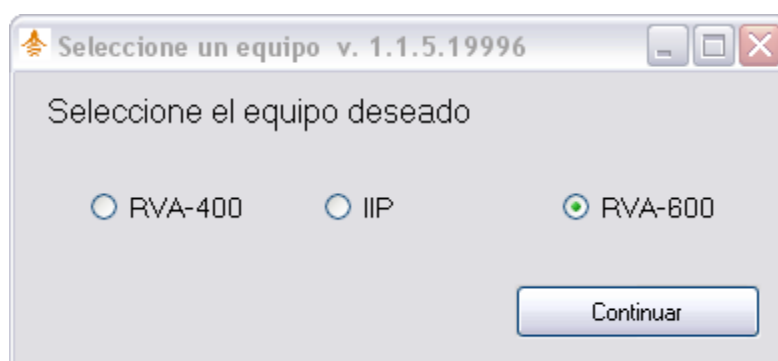


Figura 2. Selección del tipo de equipo a configurar.

En la figura 2 se ve la ventana de selección del modelo de equipo que se desea configurar, en nuestro caso, daremos el ejemplo con un equipo RVA600.

A continuación, se abrirá la ventana principal del Config Manager, que se muestra en la figura 3. Los datos que aparecen en los distintos campos de configuración, son los almacenados en una plantilla por defecto, que puede ser cambiada por el usuario, que podrá crear una plantilla nueva o cargar una existente desde el menú principal (“Archivo”).

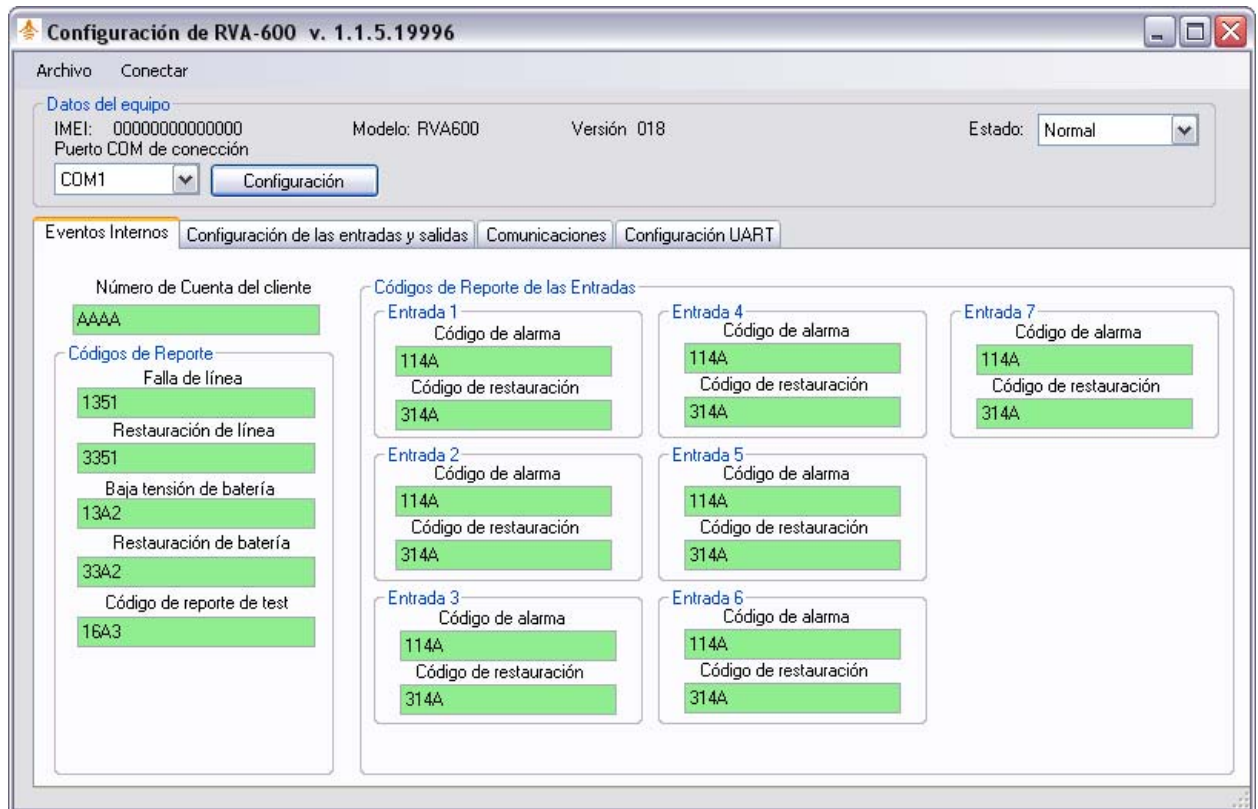


Figura 3. Ventana principal del Config Manager.

Deberá seleccionar el puerto serie a utilizar para la conexión (puerto COM), y de ser necesario, modificar los parámetros del mismo (botón “Configuración”).

Luego, podrá leer los datos almacenados en el RVA600, o directamente guardar en el equipo los datos ingresados en todos los campos de las distintas solapas de la ventana principal. Estas acciones se ejecutan desde el menú principal, dentro del submenú “Conectar”. Las opciones que aparecen en este submenú son:

- “Traer datos desde el equipo”: sirve para leer todos los parámetros de configuración internos del equipo. Para conocer su estado y permitir modificaciones sobre la base actual de su configuración.
- “Guardar datos en el equipo”: permite guardar todos los datos ingresados en el Config Manager en la memoria interna del equipo.

Como se observa en la figura 3, en la solapa “Eventos Internos” aparecen todos los campos que permiten modificar los códigos de reporte a utilizar cuando se generan eventos propios del equipo, y el número de abonado a utilizar en los

reportes de dichos eventos. Si un código de evento es ingresado con 4 caracteres "hexa", cuando este evento ocurra generará un reporte en formato "Contact ID". Mientras que si se utiliza un código con solo 2 caracteres, o con 4 caracteres cuyo inicio sean dos ceros ("00??"), el evento en cuestión generará un reporte en formato "Ademco Express". Si el código se carga con "0000", el evento no generará ningún reporte hacia la central de monitoreo.

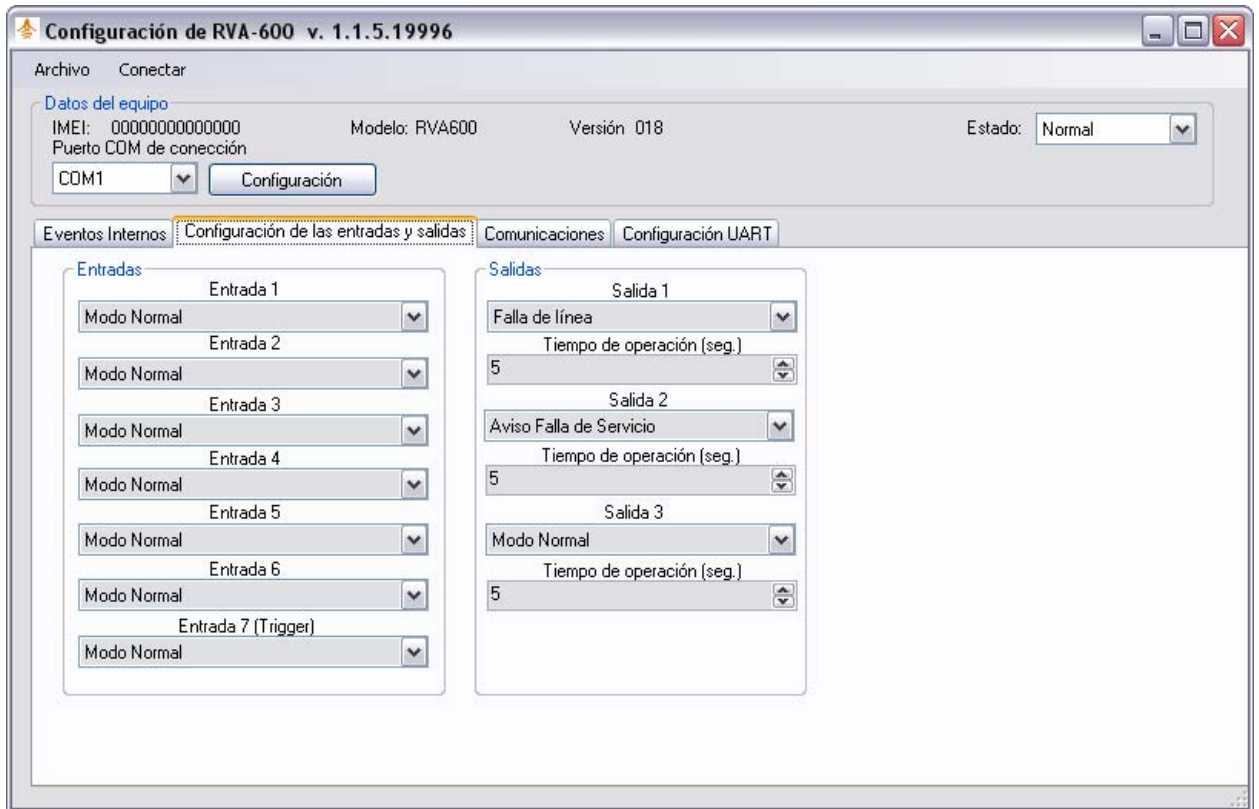


Figura 4. Configuración de entradas y salidas.

En la figura 4 se ven los parámetros de configuración para el funcionamiento de las entradas y salidas del RVA600. Se pueden cambiar los modos de operación de las salidas, como también los tiempos de operación si se usan en modo normal como temporizadas. Si el tiempo de operación de una salida en modo normal se configura en "0", la misma podrá ser activada o desactivada en forma remota por medio de un comando, quedando en ese estado hasta que sea cambiado por una nueva ejecución del comando.

La figura 5 muestra la solapa "Comunicaciones", que es la más importante al momento de configurar el equipo antes de instalarlo, ya que en la misma figuran todos los campos referidos a la comunicación del equipo con la estación de monitoreo, y si no se configuran correctamente, la comunicación entre la estación de monitoreo y el equipo una vez instalado no podrá realizarse.

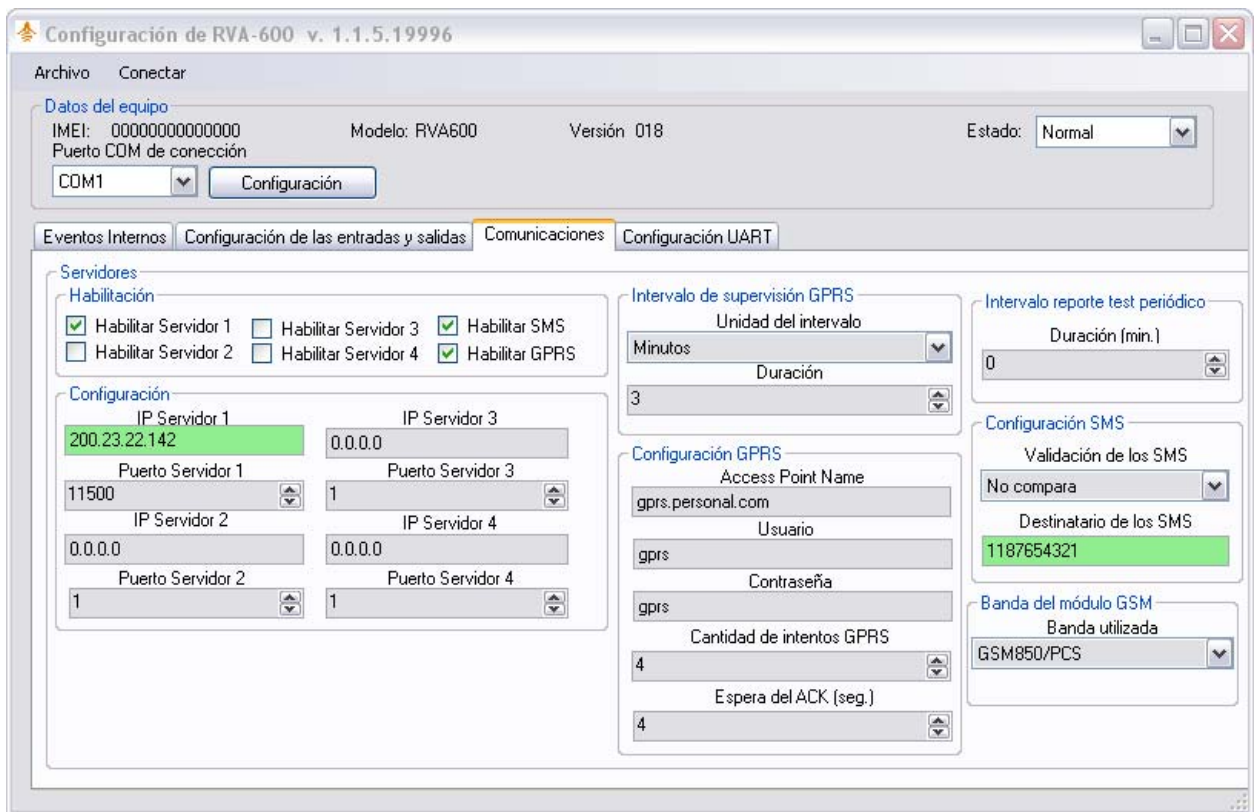


Figura 5. Configuración de las comunicaciones.

En la figura 5 se muestra como ejemplo la configuración para que el RVA600 envíe sus reportes a la IP 200.23.22.142 / Puerto 11500, siendo esta IP la IP pública y fija de la estación de monitoreo. Por lo tanto, en la configuración del router o firewall de la red privada de la estación, deberá existir una regla de redireccionamiento que redirija el puerto UDP público 11500 a la IP y Puerto privados del Patrol IP (Ej.: a la IP 192.168.0.100 / Puerto 11500, siendo estos valores los que se dieron como ejemplo en el punto 2 de este manual).

La posibilidad de configurar múltiples servidores no está orientada a permitir el monitoreo en forma simultánea por más de una estación de monitoreo, si no que se usa para hacer una redundancia secuencial en caso de no tener conectividad con un servidor. Ejemplo: si se configuran y se habilitan los servidores 1 y 2, el RVA600 enviará sus reportes solo al servidor 1, en caso de que no logre establecer conexión con el servidor 1, intentará reenviar sus reportes a la dirección IP y puerto del servidor 2, que funcionará como respaldo del servidor 1. La cantidad de reintentos se puede definir en el campo "Cantidad de intentos por GPRS", como también el tiempo de espera de respuesta del servidor por medio del campo "Espera del ACK (seg.)", pero se recomienda no alterar esos campos y usar ambos parámetros con valor "4".

En los campos "Access Point Name", "Usuario" y "Contraseña" deberán cargarse los datos de conexión al servicio GPRS del proveedor celular que vaya a utilizar en la línea asignada al RVA600 (SIMCARD). En el ejemplo, se pueden ver los datos para la conexión mediante una línea de Personal.

Cuando el RVA600 no logre enviar un reporte utilizando la conexión GRPS, intentará enviarlo por SMS, siempre y cuando esté habilitado (opción “Habilitar SMS”). El destinatario de estos reportes será el ingresado en el campo “Destinatario de los SMS”, que deberá ser cargado con el número de línea asignado al Patrol IP. Como opción adicional, se puede restringir que el RVA600 solo se comunique con una línea en particular mediante SMS, a través del campo “Validación de los SMS”, que permite al RVA600 comparar o no el número de línea de los mensajes que le llegan, con el que tiene configurado como destinatario de los SMS.

Cuando se utiliza la conexión GPRS, el RVA600 envía periódicamente un reporte de supervisión al Patrol IP. Si el Patrol IP deja de recibir estos reportes desde un determinado RVA600, generará un evento de alarma al software de monitoreo, para saber que la conexión GPRS con determinado equipo se ha caído. En esta situación, cuando el Patrol IP vuelva a recibir un reporte de supervisión, generará un evento de restauración al software de monitoreo, indicando que se ha reestablecido la comunicación por GPRS con ese equipo. Además, estos reportes periódicos de supervisión, permiten al Patrol IP conocer la IP y puerto asignados al RVA600, que pueden ser utilizados para enviarle algún comando en forma remota (por medio del SEC).

En esta misma solapa se puede configurar el intervalo para generar el evento de test periódico, que es un reporte interno del RVA600, como el que tienen la mayoría de paneles de alarma. Si este valor se carga con “0”, el intervalo del test periódico dependerá de la configuración del dipswitch del RVA600, como se describe en su manual de instalación.

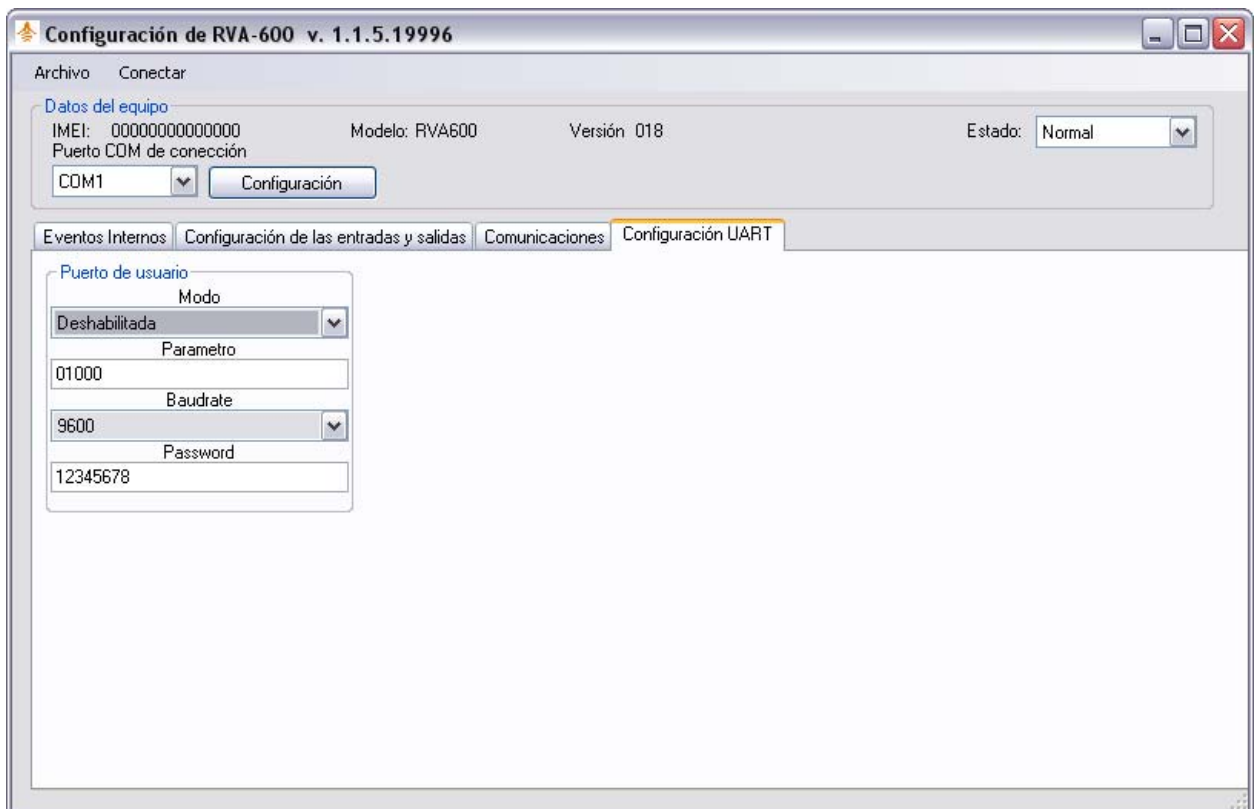


Figura 6. Configuración del puerto serie de usuario.

En la figura 6 se ven los datos para configurar el puerto serie en aplicaciones donde el usuario quiera utilizar el RVA600 como un conversor RS-232 a Ethernet y viceversa. Habilitando esta funcionalidad, el RVA600 capturará lo que recibe por su puerto serie para enviarlo en un paquete UDP a la dirección del servidor 4 configurado previamente en la solapa de “Comunicaciones”. Es el usuario quien deberá tener una aplicación escuchando en esa dirección, encargada de manejar el protocolo que requiera implementar su aplicación. A su vez, el RVA600 transmitirá al puerto serie todo lo que reciba por UDP desde el servidor 4.

Una vez cargados los campos, se puede guardar la plantilla de datos para no tener que volver a ingresar los campos cuando se quiera configurar otro RVA600 (menú principal: “Archivo” + “Guardar Como...”).

Con los campos cargados, se procede a la escritura de los mismos en el RVA600, utilizando la opción “Guardar datos en el equipo” como se dijo anteriormente.

Una vez finalizada la configuración del equipo, el RVA600 se encuentra listo para ser instalado, y reportara a las direcciones especificadas en su configuración.

Cuando el RVA600 se encuentre instalado y operativo, podrá cambiar cualquiera de sus parámetros en forma remota utilizando el SEC (**ver manual de usuario del SEC: UM-90722**). Los eventos generados por el RVA600, sean internos o provenientes del panel de alarmas al que esta conectado, serán recibidos por el Patrol IP, quien los transmitirá al software de monitoreo.