



# SECURITHOR V 1.0

## Guía de inicio.



## Desbloqueando SECURITHOR.

Las versiones completa y de prueba de SECURITHOR son exactamente iguales. La única diferencia radica en que hay que desbloquear esta última después de 30 días. Para utilizar SECURITHOR después de los 30 días se requiere la compra de una licencia de parte de MCDI o cualquiera de nuestros distribuidores. Después de la compra, debe crearse un código de SECURITHOR en la PC donde se utilizará el componente de STnet.

Al utilizar la versión de prueba, el número de días restantes se desplegará en la barra superior del componente STnet. Asegúrese de contactar a MCDI por lo menos un día hábil antes de la fecha de expiración para asegurarse de que SECURITHOR no se bloquee. Incluso en esa situación, la recepción y procesamiento de alarmas continuara trabajando y sera accesible. Las demás funciones no lo estarán.

Durante la instalación, SECURITHOR crea un ID de hardware único diseñado específicamente para su PC. Este ID de hardware no es válido en otra PC. El ID de hardware es creado y almacenado en un archivo en ...MCDI\SECURITHOR\HIDnw.txt. Este archivo es creado al iniciar por primera vez STnet.

HIDnw es común a ambos ST1 y ST Edición de red. El número de estaciones permitidas en ST Edición de red es computado por MCDI y parte de su número de serie.

HIDnw.txt debe ser enviado a MCDI para el desbloqueo final de SECURITHOR. Es preferible tener acceso a Internet para el proceso de desbloqueo ya que HIDnw.txt es un archivo que contiene una cadena larga de dígitos de MCDI. Los errores de transmisión son minimizados enormemente al transmitir el HID por vía electrónica.

Diríjase a STnet> Ayuda>Activar para abrir el formulario Web de aplicación de número de serie (securithor.com/desbloquear). Se requiere acceso a Internet. Al usar esta opción se insertará el ID de hardware en el formulario Web automáticamente. Llene tantos detalles sobre su compra como sea posible. MCDI le enviará la licencia inmediatamente.

También puede contactar directamente a MCDI. Transmita esta clave HIDnw a MCDI usando el correo electrónico [support@mcdi.com](mailto:support@mcdi.com).

MCDI calculará un archivo de licencia para su computadora y lo regresara por correo electrónico. Deberá copiar este archivo en el directorio MCDI>SECURITHOR.

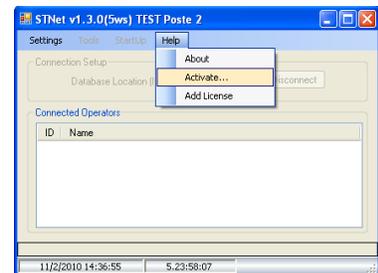
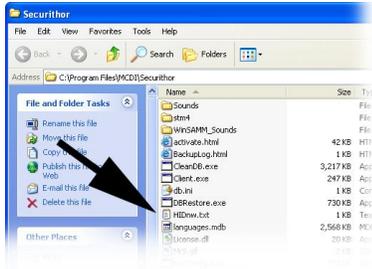
Otra opción consiste en conectarse directamente a [securithor.com/desbloquear](http://securithor.com/desbloquear). Llene tantos detalles como sea posible acerca de su compra. MCDI regresara la licencia tan pronto como sea [posible].

También puede utilizar STnet>Ayuda>Agregar licencia para copiar automáticamente el archivo de licencia en el directorio indicado.

Es posible migrar SECURITHOR a otra PC pero se requiere la desactivación del código en la primera y volver a desbloquearlo en la segunda.

Los desbloques se hacen en horario de oficina de MCDI. Fuera de este horario, los desbloques se proveen a aquellos que posean un contrato de soporte las 24 horas. SECURITHOR está diseñado para mantener siempre la VENTANA DE PROCESAMIENTO DE ALARMAS desbloqueada INCLUSO si todas las demás secciones están bloqueadas. Otras funciones podrían estar inactivas en tanto no se contacte a MCDI.

ADVERTENCIA: sólo un archivo de licencia deberá estar presente en el directorio MCDI>SECURITHOR afín de desbloquear SECURITHOR. Elimine cualquier archivo con la terminación .license



### **OPCIONES Y CARACTERÍSTICAS ADICIONALES**

El nivel de bloqueo es determinado por MCDI de acuerdo con el tipo de licencia adquirida. Para la Edición de red, el número de estaciones se fija en el archivo de licencia.

Algunos archivos de licencia tienen límite de tiempo y trabajarán durante cierto periodo. Deberá renovar su archivo de licencia con MCDI afín de continuar utilizando SECURITHOR. Se muestra el número de días restantes en la barra superior de STnet y la fecha de expiración en el cuadro de dialogo "Acerca de" de SECURITHOR. Permita por lo menos un día hábil para contactar MCDI para obtener una nueva licencia.

Algunas opciones tales como STM son de pago en ST1 y se requiere un nuevo archivo de licencia para su activación.

La licencia puede restringir el uso o añadidura de algunos idiomas.

**EN CASO DE EMERGENCIA LLAME A MCDI AL +514.481.1067 O CONTACTE SUPPORT@MCDI.COM**  
EL SOPORTE FUERA DE HORAS DE OFICINA FORMA PARTE DE CONTRATOS DE SOPORTE PREPAGADOS.

### **LICENCIAS DE EMERGENCIA**

A pesar de que la sección de Procesamiento de Alarmas nunca se desactiva, SECURITHOR está provisto con 3 licencias de emergencia para efectuar desbloques temporalmente. Deben utilizarse con precaución y en caso de extrema necesidad cuando no se tenga acceso al soporte de MCDI. Cada una es válida durante 5 días y sólo funciona UNA VEZ.

Instalar una segunda o tercera licencia de emergencia anulará la anterior, incluso si el término de 5 días aún no ha finalizado. Una vez que son utilizadas las 3 licencias de emergencia, SECURITHOR no aceptará más a menos de que la PC sea formateada y SECURITHOR reinstalado con una base de datos. Reinstalar SECURITHOR solamente no permitirá el uso de más licencias de emergencia.

Para utilizar la Licencia de Emergencia (versión >1.1.0.5) :

- Cierre SECURITHOR y STnet.exe.
- Ubique y copie en alguna otra parte cualquier archivo .license presente en el directorio de MCDI>SECURITHOR .
- Ubique Emergency1.license en la carpeta MCDI>SECURITHOR>EMERGENCIA
- Mueva y copie al directorio MCDI >SECURITHOR.
- Reinicie STnet.exe.
- Reinicie SECURITHOR.
- Contacte a MCDI. El Desbloqueo de SECURITHOR se hace tan pronto como podamos identificar el pago de SECURITHOR. Y tengamos listo el nombre de su compañía, nota de compra o número de serie. El desbloqueo se hace en horas de oficina de MCDI a menos que tenga un contrato de soporte las 24 horas.

Para utilizar la segunda o tercera Licencia de Emergencia :

- Elimine cualquier archivo.license del directorio MCDI>SECURITHOR.
- Sólo debería haber un archivo .license en el directorio MCDI>SECURITHOR.
- Repita el procedimiento previo con Emergency2.license o Emergency3.license.
- Contacte a MCDI. El desbloqueo de SECURITHOR se hace tan pronto como identifiquemos su pago. Tenga a la mano el nombre de su compañía, nota de compra o número de serie. El desbloqueo se hace en horas de oficina de MCDI a menos de que tenga un contrato de soporte las 24 horas.

**Actualizando SECURITHOR.**

Actualizando de versiones anteriores a 1.0.8.0.

Cambios en la base de datos y compatibilidad con versiones precedentes.

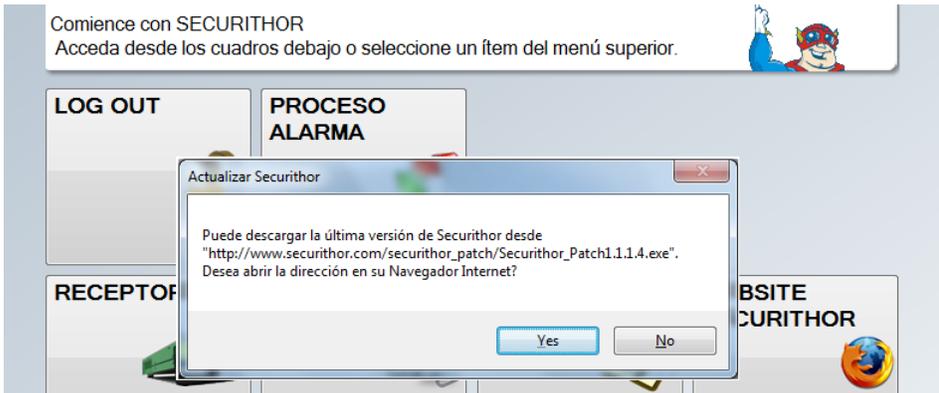
Cliente Teamviewer .

Licencias de Emergencia.

Contacto con MCDI .

**ACTUALIZANDO SECURITHOR.**

**ADVERTENCIA:** ES NECESARIO Y OBLIGATORIO CERRAR SECURITHOR, STNET Y STRECEIVER AL ACTUALIZAR. PLANIFIQUE CON ANTERIORIDAD ESTE TIEMPO SIN ACTIVIDAD. YA QUE SERÁN REQUERIDOS HASTA 15 MINUTOS. HAGA UN RESPALDO TOTAL ANTES DE CUALQUIER ACTUALIZACIÓN.



**ADVERTENCIA:** SERÁN NECESARIAS ALGUNAS REESTRUCTURACIONES EN LA BASE DE DATOS DESPUÉS DE LA ACTUALIZACIÓN. ESTO PODRÍA RALENTIZAR SECURITHOR AL REINICIAR. PLANEE LA ACTUALIZACIÓN EN HORAS DE POCA ACTIVIDAD O TRÁFICO.

Las actualizaciones están disponibles en forma de parches que contienen sólo los cambios necesarios. No hay necesidad de descargar y reinstalar SECURITHOR a menos de que MCDI se lo indique.

Si no cuenta con conexión a Internet en la máquina que contiene SECURITHOR, contacte a MCDI en [securithor@mcdi.com](mailto:securithor@mcdi.com) para obtener la última actualización. Por favor especifique su número de serie y versión actual de SECURITHOR.

Si su máquina con SECURITHOR está conectada a Internet haga un respaldo total y dirijase a Ayuda>Actualizar SECURITHOR. SECURITHOR verificará la última actualización en el servidor y le avisará si su versión de SECURITHOR debería ser actualizada. Si tiene una versión anterior a la que está en el servidor, SECURITHOR le pedirá descargar el último parche y abrirá un explorador Web con un enlace para descarga. Descárguelo y siga las instrucciones del instalador.

Para informarse de actualizaciones, lista de cambios o nuevas características de la última versión de SECURITHOR, contacte a MCDI en [securithor@mcdi.com](mailto:securithor@mcdi.com). Por favor especifique su actual versión de SECURITHOR y número de serie en Ayuda>Acerca de SECURITHOR.

Algunas restricciones se aplican para utilizar ciertas características disponibles en las actualizaciones. Algunas características pueden no estar disponibles en todas las versiones de SECURITHOR a pesar de ser parte de la descarga. Podría requerirse un pago por la activación de nuevas funcionalidades.

Podría ser necesario desbloquear nuevamente SECURITHOR al actualizarlo. Contacte a MCDI de ser este el caso.

**ACTUALIZACIÓN MEDIANTE LA REINSTALACIÓN COMPLETA DE SECURITHOR.**

Nota: El procedimiento siguiente debería realizarse sólo si MCDI se lo indica:

En caso de completa reinstalación, primero haga un respaldo de la base de datos ya sea copiando completamente el directorio de SECURITHOR o usando la función de respaldo incluida en el mismo programa(ver sección NN).

La actualización mediante reinstalación requerirá la restauración de la base de datos. Si este respaldo de la BD no se efectúa, se perderán datos y la restauración de

SECURITHOR podría no ser realizada adecuadamente. Contacte a MCDI antes de hacer una reinstalación completa.

**Actualizando desde versiones <1.0.8.0.**

La versión 1.0.8.0. marca un giro en el desarrollo de SECURITHOR, La Edición de red se introdujo junto con varios componentes clave de forma que los usuarios de ST1 pudieran beneficiarse de la estabilidad y velocidad encontradas en STnet.

Por lo tanto un nuevo componente llamado STnet ahora es común a ambos ST1 y ST Edición de red. El componente STnet actúa como un enlace entre las estaciones de trabajo y la base de datos. Incluso Al utilizar ST1, STnet es todavía obligatorio ya que actúa como una puerta de conexión ente la interfaz gráfica de usuario y la base de datos. Por favor siga las instrucciones del archivo Léame de STnet. Podría requerirse desbloquear nuevamente el programa y otro HID sería generado por SECURITHOR. Ahora es llamado HIDnw.

### Cambios en la base de datos

Varios cambios y adiciones a la base de datos podrían producirse a la hora de actualizar. Por lo tanto MCDI sugiere enérgicamente hacer un respaldo completo antes de actualizar. La compatibilidad de la BD de SECURITHOR va hacia adelante y podría no ser posible recuperarla de querer instalar una versión anterior del programa. Infórmese con el equipo de soporte de MCDI en support@mcdi.com si desea ir a una versión anterior.

### SOPORTE A SECURITHOR - TEAMVIEWER

Comenzando con la versión 1.1.0.5, Teamviewer fue añadido al instalador de SECURITHOR. Es de esta forma fácil de comenzar una sesión de Teamviewer con MCDI. Se requiere acceso a Internet. Vaya a Menú>Todos los programas >Securithor>TeamviewerQS.

Una ventana de Teamviewer será desplegada con número de usuario y contraseña.

Si cuenta con un contrato de soporte o todavía esta cubierto con su período de soporte inicial, el equipo de soporte de MCDI lo conectará tan pronto como sea posible. Envíe un correo electrónico a support@mcdi.com con el número de usuario y contraseña de Teamviewer generados en el cuadro de diálogo azul de la izquierda.

Teamviewer permite al equipo de soporte de MCDI conectarse remotamente a su SECURITHOR a través de una conexión segura. Por favor prepárese para describir y reproducir su problema.

Una vez que MCDI se conecte, será alertado por Teamviewer. En algunos puntos, MCDI podría mover ventanas y formularios en el escritorio de su computadora para tener acceso a SECURITHOR. Esto es completamente normal.

Por favor tenga en cuenta que Teamviewer y los contratos de soporte no deben ser usados para capacitación. Son sólo para solución de problemas. Puede adquirir sesiones de capacitación de forma separada. Contacte a securithor@mcdi.com para adquirir dichas sesiones.

### LICENCIAS DE EMERGENCIA.

A pesar de que la sección de Procesamiento de Alarmas nunca se bloquea, SECURITHOR está provisto con 3 licencias de emergencia para desbloques temporales. Deberían ser utilizados con precaución y sólo en caso de extrema necesidad cuando no tenga acceso al soporte de MCDI. Cada una es válida durante 5 días y sólo puede ser usada UNA VEZ.

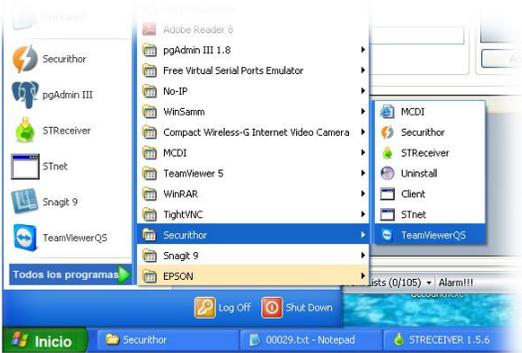
La instalación de una segunda o tercera licencia de emergencia invalidará a la anterior, incluso si el término de los 5 días no ha finalizado. Una vez que las 3 licencias de emergencia han sido usadas, SECURITHOR no aceptará más a menos de que formatee su computadora y reinstale SECURITHOR con una base de datos vacía. La reinstalación únicamente de SECURITHOR no le permitirá usar más licencias de emergencia.

Para utilizar la Licencia de Emergencia (versión >1.1.0.5) :

- Cierre SECURITHOR y STnet.exe.
- Ubique y copie en alguna otra parte cualquier archivo .license presente en el directorio de MCDI>SECURITHOR .
- Ubique Emergency1.license en la carpeta MCDI>SECURITHOR>EMERGENCIA.
- Mueva y copie al directorio MCDI >SECURITHOR.
- Reinicie STnet.exe.
- Reinicie SECURITHOR.
- Contacte a MCDI. El Desbloqueo de SECURITHOR se hace tan pronto como podamos identificar el pago de SECURITHOR. Y tengamos listo el nombre de su compañía, nota de compra o número de serie. El desbloqueo se hace en horas de oficina de MCDI a menos que tenga un contrato de soporte las 24 horas.

Para utilizar la segunda o tercera Licencia de Emergencia

- -Elimine cualquier archivo.license del directorio MCDI>SECURITHOR.



- Sólo debería haber un archivo .license en el directorio MCDI>SECURITHOR.
- Repita el procedimiento previo con Emergency2.license o Emergency3.license.
- Contacte a MCDI. El desbloqueo de SECURITHOR se hace tan pronto como identifiquemos su pago. Tenga a la mano el nombre de su compañía, nota de compra o número de serie. El desbloqueo se hace en horas de oficina de MCDI a menos de que tenga un contrato de soporte las 24 horas.

**Contacto con MCDI.**

Respecto a noviembre del 2010, los contactos de MCDI SECURITHOR son:

Inglés y Francés: 514-481-1067 support@mcdi.com.

Español e Inglés: 514-487-0441 soporte@mcdi.com.

Portugués: +55 (54)221-1727 (by MCDI Do Brasil) suporte@mcdidobrasil.com.br

Ruso: Grupo Navigator info@navigatorgrp.ru.

Los poseedores de contratos de soporte las 24 horas cuentan con correos electrónicos y números telefónicos especialmente dedicados.

## VERIFICACIÓN DE CONFIGURACIÓN DEAD MAN Y VERIFICACIÓN DE ALERTAS A OPERADOR.

Verificación de configuración Dead Man se refiere al concepto de conmutador hombre-muerto (traducción al español), un dispositivo especial de seguridad que desactiva una máquina cuando el operador suelta los controles. En SECURITHOR Dead Man verifica si el operador se encuentra alerta. ST mide el tiempo sin actividad de teclado en la estación de trabajo. Si no se detecta teclado en un espacio de tiempo predefinido, ST presenta un formulario al operador con 4 números al azar. El operador debe introducir la secuencia correcta en un tiempo determinado. Si el operador no responde, ST creará un evento de alarma y/o enviará correos electrónicos a direcciones predefinidas.



Nota: La función Dead Man trabaja sólo si hay alarmas que necesiten ser procesadas. Cuando no existen alarmas a procesar (en tráfico o pendientes), la verificación se pospone.

Habilitando verificación de Dead Man.

Primer paso: Para habilitar la función de Dead Man por operador en administración de operadores.

Vaya a operadores y seleccione operador.

Haga clic en el cuadro de diálogo Dead Man para habilitarlo para este operador.

Segundo paso: Para habilitar la función Dead Man de manera global vaya a Configuración >Otra configuración y modifique los parámetros de verificación de Dead Man.

Salga de SECURITHOR y entre de nuevo para habilitar los parámetros Dead Man o activar cambios de configuraciones por operador.

### Parámetros.

Habilitar.

Haga clic para habilitar, o deseccione para deshabilitar la función globalmente.

Demora Activación AutoGen seleccionado: NN segundos o minutos (mínimo 1 máximo: ilimitado).

AutoGen activado se refiere al botón icono AUTO cuando se le hace clic se presenta un cuadro emergente con eventos de alarma. Los eventos entrantes se presentan a los operadores por medio de ventanas emergentes.

Demora Activación AutoGen NO seleccionado: NN segundos o minutos (mínimo 1 máximo: ilimitado).

AutoGen NO seleccionado se refiere a al botón icono AUTO cuando no se le ha hecho clic par ver las ventanas emergentes con eventos de alarmas. En este caso los eventos no se presentan a los operadores.

Demora por fuera de tiempo.

Retardo en segundos (de 1 a N) para introducir la respuesta correcta del test. Si el operador introduce una respuesta incorrecta, se enviará la alarma correspondiente al tiempo de demora.

Códigos de alarma.

Nótese que los códigos de alarma no son obligatorios. Puede dejar estos espacios en blanco si no desea crear eventos de alarma. De cualquier forma un correo electrónico puede ser enviado si esta definido en configuración de Dead Man. Para ver los eventos de alarma vaya a Cuenta 0 Partición 0.

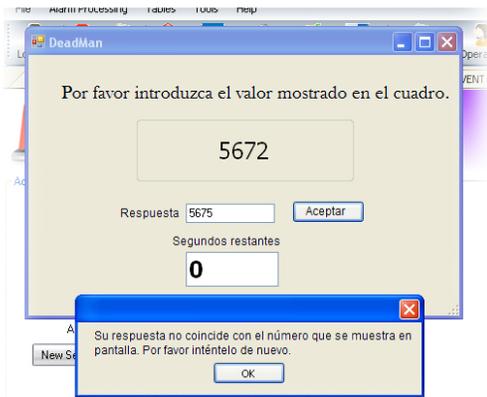
Para activar los códigos de alarma, deberá definir los códigos de alarma correspondientes en Cuenta 0 Partición 0. Como ejemplo puede definir los siguientes códigos de alarma correspondientes en "Otras configuraciones" y Cuenta 0:

Código 'AA' Descripción: Operador no introdujo código Dead Man.

Código 'BB' Descripción: Operador no introdujo código Dead Man después del tiempo de espera.

Código 'CC' Descripción: Operador introdujo una respuesta incorrecta a la pregunta Dead Man.

Seleccione enviar correo electrónico si desea activar direcciones de correo globales para un código.



Varias direcciones de correo electrónico o direcciones SMS pueden definirse y asignarse a estos códigos de alarma en Cuenta 0. Refiérase a la sección Enviando correos electrónicos y SMS para configurarlas correctamente, recuerde que un campo de dirección de correo electrónico global en configuración de Dead Man es una dirección de correo para todos los operadores que tengan activada dicha función. Si desea agregar más de una dirección de correo electrónico sepárelas con comas.

#### Respondiendo a verificación de Dead Man.

Al momento de habilitar y volver a entrar a SECURITHOR, El operador será sometido a una verificación de alerta. Después del tiempo de espera seleccionado, SECURITHOR abrirá un formulario de prueba al operador. El operador deberá introducir los 4 dígitos generados al azar desplegados en el formulario para cancelar la generación de códigos/correos electrónicos. El no responder correctamente dentro del tiempo límite establecido generará acciones predefinidas.

## Agregando receptores de alarma . El componente STreceiver.

A partir de la versión 1.5.5, todos los receptores de MCDI que se comuniquen con la PC en formato, Surgard MLR2, Ademco 685 y SK9000/9500 por medio de puertos seriales también pueden hacerlo por medio de USB. La comunicación está bien establecida con los receptores de MCDI pero necesita ser validada con receptores de otra marca. El uso de un puerto en serie virtual es requerido. Existe cierta compatibilidad IP con receptores Extrium de MCDI.

El módulo de comunicación de SECURITHOR se llama STReceiver. Está ubicado en el directorio MCDI>STReceiver. Ejecute STReceiver para configurar la comunicación entre los receptores y SECURITHOR. Vea la figura descriptiva al final de la sección.

### Receptores de alarma soportados en la versión de STreceiver 1.5.5:

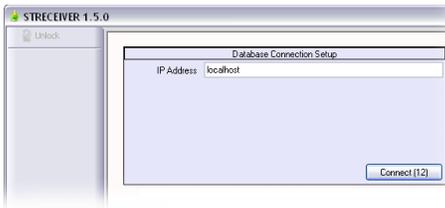
MCDI's TLR, TLR+, SA-TLR+, EXSA, Decrypta 1, Decrypta 2, Decrypta 3.  
MCDI's Exprecium 1, 2.  
MCDI 's Exprecium 3 y 3r.  
MCDI's Exprecium D.  
MCDI'S RACK16 .  
Decrypta 5, Decrypta 6 (sobre IP, USB o puertos seriales).  
Formato Ademco 685 .  
Formato Surgard MLR2, MLR2000 .  
Surgard System 3 (parcial).  
Radionics 6500 .  
Silent Knight 9000 (bajo lista SK9500).  
Silent Knight 9500 (sólo mediante contacto ID).  
SMS - formato SMS definido por MCDI.

Otros receptores son considerados en la versión 2.0. Los receptores Legacy presentes en WinSAMM pueden ser agregados dependiendo de las condiciones del mercado.

### CONTRASEÑA.

Se requiere una contraseña para abrir STReceiver. La contraseña por omisión es 'securithor'. Puede cambiarse haciendo clic en el botón cambiar en la columna izquierda de STr después de desbloquear la configuración.

STr fue diseñado para no salirse de el cuando está bloqueado. Para salir primero desbloquee e introduzca la contraseña, entonces haga clic en el botón X. Un formulario le pedirá salir. Responda Si par salir de STreceiver o No para continuar ejecutándolo. Vea la figura descriptiva al final de la sección.



### Conexión a base de datos.

Al arranque, STreceiver pide una dirección IP afín de conectar la base de datos de PostgreSQL a SECURITHOR. Para cambiar la dirección de conexión, salga de STreceiver y reinicie para conectarse a otra dirección IP.

Por omisión se selecciona 'localhost' en STreceiver afín de conectarse a la maquina en la cual esta ubicada la base de datos. Si esta corriendo en una maquina diferente a la del núcleo de SECURITHOR, introduzca la dirección IP de la máquina en la que se encuentra la base de datos de PostgreSQL. El formato de la dirección IP es IP V4 xxx.xxx.xxx.xxx . La información del puerto no es necesaria.

Con ST1 o STnet, puede instalar STreceiver en una máquina separada de aquella en la que corre la base de datos de SECURITHOR.

Es posible instalar varios STreceiver (uno por máquina) y conectarse a SECURITHOR ST1 o STnet.

Refiérase a la instalación de SECURITHOR Edición de red afín de conectar SECURITHOR a la base de datos de PostgreSQL.

### AÑADIENDO UN RECEPTOR.

Los receptores disponibles se muestran en la columna izquierda como COM 1 a COMn. El número COM no indica el número de puerto de una computadora sino el número de canal de comunicación N en STreceiver.

Para asignar un nombre o alias, haga clic en el COM deseado para abrir el formulario de opciones. Cambie el nombre en Configuración de puerto>Alias.

Seleccione tipo de receptor y después parámetros específicos de receptor. La mayoría de los receptores se comunican con software de automatización a 1200 baudios. Refiérase a la guía de usuario de su receptor para configuraciones más avanzadas.

Incluso si no reconoce su receptor seleccione uno con un formato de reporte equivalente para el suyo. Si tiene dudas contacte el equipo de soporte de MCDI support@mcdi.com con detalles específicos de su receptor.

ABRIR COMn/específicos de receptor.

Tipo de receptor.

Seleccione el tipo de receptor de acuerdo con el nombre o formato compatible.

Selección de color (botón superior derecho).

Asignará este color al tráfico entrante de este receptor.

Prefijo.

Seleccione un número de 1 a F para ser agregado a un evento de alarma frontal. Típicamente usado para agrupar cuentas, para mover alarmas de un receptor específico a un rango de cuentas.

Agregar número de receptor como prefijo.

No relacionado a prefijos de configuración previos. Número provisto por el receptor.

Agregar número de línea como prefijo.

Número provisto por el receptor para identificar la línea.

Usar hora del receptor de alarma.

Utiliza el huso horario del receptor en vez de la hora de STreceiver's. Al desactivarlo, La hora de STreceiver (y el huso horario) reemplaza la hora del receptor. Se recomienda verificar la configuración de hora regularmente al comienzo de cada turno de trabajo.

Usar ID de contacto comprimido.

Cambia la definición de ID de contacto a la forma comprimida.

Mostrar Latidos.

Al seleccionar esta opción, se mostrará el caracter de latido durante el tráfico.

La mayoría de los receptores seriales o USB enviarán el caracter '@'.

El número de receptor y número de línea también son enviados por el receptor.

El nombre de Alias y número COM son agregados por STr.

Los receptores Silent Knight muestran latidos como eventos.

El receptor IP de MCDI's envía un paquete de latidos. Todo esto es transparente para el usuario y es mostrado como un latido de corazón en la ventana de trafico.

**Configuración de puerto.**

Alias.

Introduzca el nombre de su elección para identificar fácilmente un receptor.

Velocidad en baudios.

Seleccione e iguale la velocidad del receptor. Típicamente 1200 baudios.

Este dato no es requerido para los receptores IP o USB.

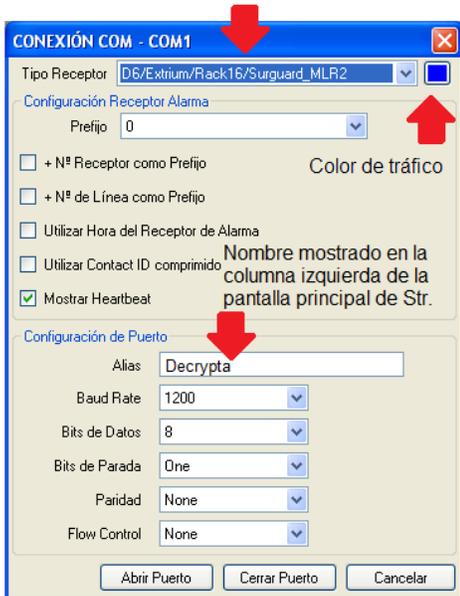
Bits de datos.

Usualmente se fija en 8, que es la longitud de un byte.

Bits de paro.

Número de bits de parada, se deja normalmente en 7.

Seleccione receptor por tipo/descripción. Si el nombre del receptor no aparece, seleccione uno con formato de reporte equivalente.



Añadiendo un receptor – configuración de conexión COM.

**Paridad.**

Normalmente se deja en uno cuando se usan 7 bits de paro = 1 byte.

**Control de flujo.**

Se deja en ninguno. Esta opción está disponible para fijar la petición de envío del próximo byte.

**Abrir puerto /Cerrar puerto/Cancelar.**

Abrir creará un Puerto en la columna izquierda y la ventana de tráfico. También úselo para aplicar cambios.

Cerrar eliminará el receptor de la columna izquierda y de la pantalla de tráfico.

Cancelar cancelará cambios y regresará el formulario a la configuración previa sin cerrar el formulario de conexión.

**Nuevo TCP/IP / Añadiendo un receptor IP MCDIs.**

Seleccione para establecer comunicación IP usando el formato IP de MCDI o el formato ROF para la familia Extrium o los receptores, D5 o D6. La comunicación establecida por medio de un dispositivo IP de MCDI se mostrará bajo TCP/IP. El tráfico será amalgamado en la ventana de tráfico. El panel de configuración de conexión TCP permite la personalización de:

**Tipo de receptor.**

Seleccione tipo de receptor Decrypta 5 o 6. Este formato es común para todos los receptores IP de MCDI.

**Selección de color (botón superior derecho).**

Asignará este color al tráfico entrante desde este receptor.

**Prefijo.**

Seleccione un número de 1 a F para ser agregado a un evento de alarma frontal. Típicamente usado para agrupar cuentas, para mover alarmas de un receptor específico a un rango de cuentas.

**Agregar número de receptor como prefijo.**

No relacionado a prefijos de configuración previos. Número provisto por el receptor.

**Agregar número de línea como prefijo.**

Número provisto por el receptor para identificar la línea.

**Usar hora del receptor de alarma.**

Utiliza el huso horario del receptor en vez de la hora de STreceiver's. Al desactivarlo, La hora de STreceiver (y el huso horario) reemplaza la hora del receptor. Se recomienda verificar la configuración de hora regularmente al comienzo de cada turno de trabajo.

**Usar ID de contacto comprimido.**

Cambia la definición de ID de contacto a la forma comprimida.

**Mostrar Latidos.**

Al seleccionar esta opción, se mostrará el caracter de latido durante el tráfico.

**CONFIGURACIÓN DE CONEXIÓN TCP.****Alias.**

El nombre seleccionado se mostrará en la columna izquierda bajo TCP/IP.

**Dirección IP.**

Introduzca la dirección IP del receptor. En formato IPV4.

**Puerto.**

Introduzca el Puerto IP del receptor. Máximo 5 dígitos. Asegúrese de que el puerto no esté bloqueado por el firewall de su computadora.

**Contraseña.**

Introduzca la contraseña de su receptor IP de MCDI.

**Abrir puerto.**

Agregaré este receptor a STreceiver o actualizaré las configuraciones.

**Cerrar Puerto.**

Eliminaré este receptor de STreceiver.

**Cancelar.**

Regresará a la configuración guardada previamente.

**Mensajes de STreceiver.**

Algunas veces STR desplegará los mensajes en una ventana de tráfico. Los siguientes mensajes son desplegados en la ventana de tráfico pero no son registrados en archivos LOG:

- Puerto abierto.
- El Puerto no ha respondido durante más de un minuto.
- Escuchando al puerto.
- ACOMX (denota ausencia del puerto COM donde X es el número de puerto)
- RCOMX (denota puerto COM restaurado donde X es el número de puerto).
- Contraseña errónea.

**Usar STreceiver sin utilizar SECURITHOR (crear archivos de registro solamente).**

Es posible utilizar STreceiver sin SECURITHOR afín de usar archivos de registro (Log) solamente. De cualquier manera, SECURITHOR debe instalarse primero. Abriendo únicamente STreceiver, los archivos Log se crearan y actualizaran continuamente sin tener que hacer uso de SECURITHOR. STreceiver es independiente de SECURITHOR y por consiguiente no necesita ser desbloqueado después del periodo de prueba de SECURITHOR.

**DIRECTORIO DE REGISTRO.**

Durante la instalación, STreceiver crea una carpeta 'Logs' en el directorio MCDI>STreceiver.

Se crean subdirectorios por cada mes y por cada año. Archivos por cada día y por cada receptor.

**Formato (típico).**

HH:MM:SS.millisegundos [tab.] Alarma [DC4].

Los eventos de alarma incluyen ID de llamadas cuando parte del evento CR es cambiado por DC4 en modo Sur-Gard.

Esta función no está incluida sin contrato de soporte ni durante el periodo de garantía de SECURITHOR. Es distribuida como shareware sin garantía.

Las funciones descritas existen a partir de Noviembre del 2010, en la versión STR 1.5.0.



## Programación de respaldos.

Frecuentemente deben respaldarse todos los datos. La recuperación de datos o del disco duro es muchas veces costosa o imposible. Por esta razón, SECURITHOR incluye un programador de respaldos automático. En versiones anteriores a la 1.0.8.0, el programador de respaldos estaba disponible desde un icono en la barra superior de SECURITHOR en la ventana principal. En versiones posteriores a la 1.0.8.1., El programador de respaldos se colocó en STnet.exe. Acceda al programador de respaldos mediante STnet>Herramientas>Respaldo. La presente sección cubrirá las versiones que preceden a la 1.0.8.1.

Puede definir la ubicación del respaldo de su base de datos y el programa de respaldos. La función explorar esta disponible desde el botón con el mismo nombre. SECURITHOR se apoya en el sistema operativo Windows para acceder a dispositivos externos, ubicaciones de red o sitios FTP fuera de su red.

Se pueden especificar la ubicación y puerto de la base de datos. De cualquier forma SECURITHOR introducirá la información especificada por STnet.exe y usualmente no necesita ser cambiada.

Se pueden programar respaldos cada día, cada fin de semana, un día del mes o un día de la semana específico. Por naturaleza algunas selecciones efectuarán respaldos en forma repetitiva.

El respaldo podría ralentizar su computadora y SECURITHOR. Es preferible programar el respaldo en un periodo de inactividad o de ser possible de noche.

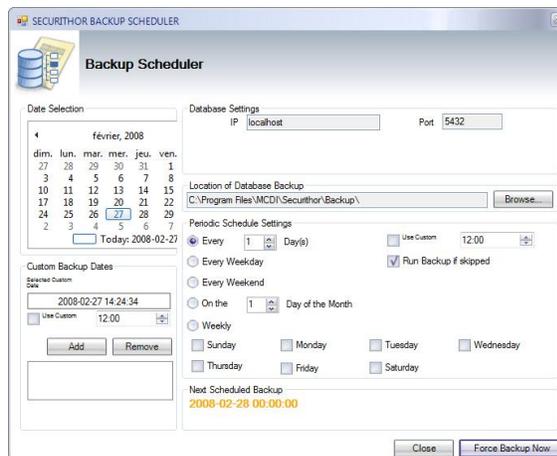
### Podría forzar un respaldo en cualquier momento mediante 'FORZAR RESPALDO AHORA'.

Para minimizar la exposición a subidas de voltaje, su unidad removible no deberá estar conectada a la PC a menos de que esté realizando un respaldo. También será bueno mantener siempre un respaldo reciente.

La integridad del respaldo deberá ser revisada periódicamente.

Se recomienda también una configuración de disco RAID. Debería verificar la compatibilidad de su arreglo RAID contra SECURITHOR ANTES de comenzar un monitoreo en tiempo real. Tener un arreglo RAID no deberá verse como un sustituto de un respaldo de seguridad.

SECURITHOR indica la hora del último respaldo en la esquina inferior izquierda y la hora de la próxima copia de respaldo programada en caso de existir.



- 6. STM SECURITHOR MÓVIL.
- 6.1 Propósito y descripción.
- 6.2 Velocidad de actualización.
- 6.3 Dispositivos en la mira.
- 6.4 Configuración y actualización a FTP.
- 6.5 Personalización.
- 6.6 Desbloqueo/Condiciones de operación.

**Propósito.**

STM es una interfaz Web diseñada para propietarios y supervisores de estaciones centrales. Hecha para dispositivos de mano tales como iPhone o iPad, STM es un formulario Web que muestra algunos de los elementos clave de SECURITHOR. También puede ver contenido de STM en otros dispositivos de mano y tabletas o exploradores Web compatibles.

Estado de la clave, lista de operadores inscritos, lista de los últimos eventos y los primeros 10 códigos de alarma recibidos en las últimas 24 horas son desplegados en 320 pixeles (mínimo) a 480 pixeles de ancho (máximo).

STM está incluido en ST Edición de red y como una opción de pago de SECURITHOR ST1. Requerirá un código especial para desbloquear y usar STM con ST1 (SECURITHOR estación sencilla). Pregunte al personal de MCDI en securithor@mcdi.com sobre la adquisición de STM.

**DESCRIPCIÓN.**

Para alternar entre temas, toque o haga clic en el tabulador correspondiente.

Accese a su STM introduciendo el URL.

Vuelva a cargar para actualizar o espere la actualización automática, la cual ocurre en intervalos de 30 a 60 segundos (configurables).

Desplácese hacia arriba o hacia abajo para ver más información.



Cargue de nuevo para ver la última actualización

Nombre de su CMS

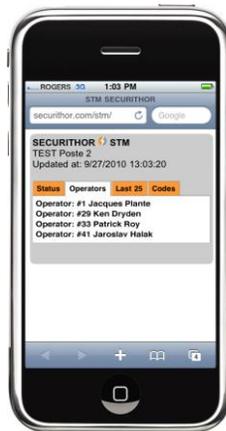
Última actualización de Script

Seleccione una pestaña para ver el contenido. La pestaña blanca está seleccionada, desplácese hacia arriba o hacia abajo para ver el contenido completo

iPhone o iPad> OS4  
Presione el botón Inicio y Encendido/apagado para capturar la pantalla. Vea la captura de pantalla en el icono rollo de camera



Estado



Operadores



Últimos 25

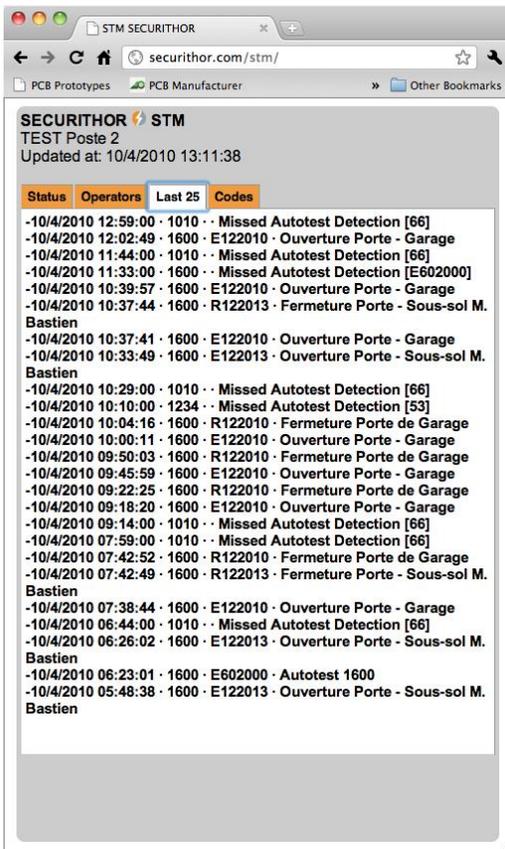


Primeros 10 códigos

**Estado.**

La ventana de estado muestra:

- Tiempo de actividad desde la última vez que se inició la computadora o SECURITHOR.
- Correos electrónicos: Si está activo significa que el componente está listo para enviar correos. Indica también el número de correos electrónicos enviados contra el número de correos que faltan por ser enviados en la última hora.
- Si muestra inactivo significa ya sea que el componente de correos electrónicos no fue configurado correctamente, que el servidor de correo saliente no está respondiendo o bien que no se encuentra habilitado.



- Fallo en prueba de alerta: se muestra sólo cuando uno o más operadores fallan la prueba de alerta.
- Recibido en la última hora
- Guardado automático: número de eventos guardados en archivo sin la intervención del operador vs. número total de eventos recibidos durante la última hora.
- Operador guardado: número de eventos procesados directamente por operadores vs. número total de eventos recibidos durante la última hora.
- Correos enviados: número de eventos enviados vs. total a enviar, ya sea por correo electrónico o SMS.

#### OPERADORES.

Lista los números de operador y nombres de todos los operadores inscritos actualmente.

#### ÚLTIMOS NN EVENTOS.

Lista los últimos eventos NN recibidos por SECURITHOR. En formato: MM/DD/YYYY\_HH\_MM\_SS\_-\_AAAA\_-\_CCCCC\_-\_Descripción del código de alarma.

Puede seleccionar entre 10,25,50,75,100 eventos.

MM: mes.  
 DD: día.  
 YYYY: año.  
 HH: horas.  
 MM: minutos.  
 SS: segundos.

Nota: El formato de fecha y hora está especificado en la configuración de su computadora y puede ser diferente de este ejemplo.

AAAA: Cuenta.

CCCCC: Código de alarma.

Descripción de código de alarma: tal como se introduce en ST para el código de alarma correspondiente.

#### Códigos.

Los 10 códigos más recibidos en las últimas 24 horas.

#### VELOCIDAD DE ACTUALIZACIÓN.

SECURITHOR Carga la información cada 30 segundos. La página Web se actualizará automáticamente con la frecuencia seleccionada (30, 45 o 60 segundos). Para forzar la actualización utilice el botón actualizar/cargar de su explorador Web. Si la conexión FTP se rompe, la información de STM no será actualizada y el programa desplegará la última actualización recibida.

Seleccione la frecuencia de actualización en STnet>Mobile estado.

Es recomendable salir de la aplicación o presionar el botón de apagado de su dispositivo ya que STM continuará recargando y esto podría inducir grandes cargas en el ancho de banda de mantenerlo encendido.

#### DISPOSITIVOS DE DESTINO.

Los scripts para STM fueron desarrollados para iPhone 3Gs y 4G y los iPad de primera generación. Fueron probados con Nokia 9000 y con simuladores de Blackberry. Ningún tipo de garantía es ofrecida para su uso con dispositivos Blackberry o aquellos basados en la tecnología Android. Se requiere compatibilidad con CSS3 y HTML 5.

Ha sido probado en exploradores Web tales como Safari 4.3, Firefox 3.6 e IE 9. Algunos elementos gráficos no se ven en el explorador de Windows ya que no cumple con los estándares W3C.

#### CONFIGURACIÓN.

Toda la configuración disponible para STM desde la aplicación STnet está ubicada en el directorio MCDI>SECURITHOR.

Abra STnet>Herramientas>Estadísticas Mobile. Seleccione Estadísticas Mobile para tener acceso a los parámetros de Estadísticas Mobile. Los siguientes parámetros están disponibles:

- Ubicación FTP / Dirección IP.
- Iniciar sesión / Nombre de usuario.
- Contraseña.
- Frecuencia de actualización de la página.
- Número de eventos mostrados en la página de últimos eventos.

### SUBIENDO INFORMACIÓN VÍA FTP.

Se requiere tener una conexión a Internet todo el tiempo para subir datos a STM. Para subir datos a través de su propio FTP a STM se requiere subir scripts y páginas Web vía FTP. Esta carpeta FTP puede ser albergada en un sitio Web de su elección o por MCDI.

Por omisión, STM no crea un directorio en su FTP. Por favor créelo o seleccione una carpeta donde SECURITHOR pueda copiar los archivos necesarios. Ejemplos: FTP://securithor.com/stm todos los archivos serán transferidos al directorio 'stm' en securithor.com.

FTP IP: introduzca la dirección FTP o dirección y ruta IP.

Inicio de sesión: introduzca el nombre de usuario provisto por el administrador de su sistema.

Contraseña: introduzca la contraseña provista por el administrador de su sistema.

Utilizando una partición FTP provista por MCDI.

MCDI provee espacio libre en securithor.com para descargar y ver su STM. Contacte a MCDI para arreglar su hospedaje gratuito. MCDI no brinda garantía de fiabilidad de este servicio dado que es gratis. De cualquier forma nuestro servicio es fiable y su sitio estará en funcionamiento 99% del tiempo al año. El acceso a su STM requerirá introducir una dirección URL tal como:

<http://securithor.com/nombre de su central> o  
<http://nombre de su central.securithor.com>.

Esto necesita arreglarse previamente con el soporte de MCDI.

Instalación inicial en FTP.

Las páginas Web y los scripts se encuentran en el directorio SECURITHOR>stm4. SECURITHOR subirá los archivos necesarios automáticamente cuando defina usted la ubicación de su servidor FTP y se conecte. Desde la primera conexión, SECURITHOR subirá los archivos que se encuentran en el directorio de SECURITHOR. A partir de entonces SECURITHOR solo subirá archivos HTML a menos de que cambie la ubicación del servidor FTP.

### PERSONALIZANDO STM.

MCDI no provee servicio de personalización para STM. De cualquier manera usted mismo puede modificar los archivos CSS hasta cierto punto. Por favor nótese que MCDI no hace cambios en las cuentas al momento de realizar actualizaciones.

Usted puede modificar los siguientes archivos CSS ubicados en el directorio de SECURITHOR:

- round.css.
- SpryTabbedPanels.css.

Se sugiere no modificar las funciones del panel principal ni los tabuladores que se encuentran escritos en archivos java script.

Round.css contiene información sobre el formato de fuentes, tamaño, y colores de fondo del contenedor principal del dispositivo.

SpryTabbedPanels.css contiene información sobre la fuente, tamaño de fuente, tamaño del contenedor, color de fondo, estado de los botones y formato de tabuladores de la ventana principal. Es recomendable que esta modificación sea realizada por personal con experiencia en edición de HTML.

Favicon.gif contiene un logo de SECURITHOR. Puede reemplazarlo con el logo de su CMS. Asegúrese de que su logotipo ocupe menos de 2KB y 16 pixeles x 16 pixeles.

Puede deshacer todos los cambios y volver a los valores por omisión de MCDI cargando los archivos originales de nuevo.

SECURITHOR subirá todos estos archivos al momento de cambiar la ubicación del servidor FTP. Asegúrese de mantener una copia de respaldo. Al actualizar, SECURITHOR borrará archivos y los reemplazará con otros más actualizados por MCDI. Puede reemplazarlos con los suyos propios antes de conectarse al servidor FTP o antes de cambiarlos manualmente.

Ver en HTML .

STM requiere un explorador Web compatible con CSS3, Web 5 y que soporte javascript.

MCDI no hace cambios de cuentas al momento de realizar las actualizaciones.

### **DESBLOQUEO.**

Desbloqueo de STM al utilizar la Edición de red.

STM está desbloqueado permanentemente en la Edición de red.

Desbloqueo de STM al utilizar ST1.

Al adquirir la opción de STM para ST1, su número de serie contendrá códigos relevantes para STM. Si adquiere STM después de su compra inicial y de la instalación de ST1, necesitará otro código de MCDI.

### **CONDICIONES DE OPERACIÓN.**

STM requiere una conexión a Internet estable y continua para proveer un servicio sin interrupciones. Se requiere de Internet o de una conexión de datos de Internet vía GSM para ver los datos de STM a través de dispositivos de mano.

Hasta 5 dispositivos pueden ver datos STM simultáneamente.

Se sugiere restringir el acceso al directorio de STM en su sitio Web usando contraseñas seguras.

## 8. Enviando correos electrónicos y SMS.

### 8.1 Introducción.

#### 8.1.1 Descripción .

#### 8.1.2 Módems compatibles con GSM.

#### 8.1.3 Garantía.

### 8.2 Conectando modems SMS a STRceiver (entrantes o salientes).

### 8.3 Recibiendo correos electrónicos SMS.

### 8.4 Enviando y recibiendo eventos SMS.

### 8.5 Recibiendo correos electrónicos SMS.

### 8.6 Encabezado y asunto del evento.

### 8.7 Enviando correos electrónicos.

#### 8.7.1 Configuración del servidor de correo electrónico.

#### 8.7.2 Agregar/Eliminar direcciones de correo electrónico.

## Introducción.

### Descripción.

Cada cuenta y código de alarma permiten que los correos electrónicos o SMS notifiquen a un suscriptor al momento de recibir una alarma. Para enviar un correo electrónico o SMS, se requiere de la preconfiguración de la cuenta. Las acciones de Correo/SMS tienen que estar predefinidas para cada código de alarma deseado y la configuración del módem de Internet o GSM debidamente completada.

El mismo evento de alarma puede ser enviado a varias direcciones de correo electrónico así como a varios números de teléfono SMS.

El envío y recepción de SMS (sin puerta de salida de correo) sólo está disponible en versiones >1.1.0.7.

Está disponible para todas las configuraciones de SECURITHOR.

El envío de correos electrónicos está disponible en todas las versiones y configuraciones de SECURITHOR hasta la 1.0. La siguiente descripción aplica a versiones >1.1.0.7.

### Módems GSM compatibles.

A partir de octubre del 2010.

Probados:

Sony Ericsson GM28, GM29, GT47, GT48.

Todas las unidades que utilizan un comunicador Telit 864 GSM.

Siemens TC35i;

Navigard 2058.

Todos los demás módems relacionados con comandos SMS AT (versiones de Sony Ericsson y Siemens) deberían ser compatibles pero aún no han sido probadas.

### Garantía.

MCDI no ofrece garantía de que las funciones o señales SMS llegarán al usuario. Esta ausencia de garantía tiene relación con el uso de equipo o proveedores ajenos a MCDI, que no reconozcan toda esa gama de servicios.

MCDI no probará ninguna solución de alto tráfico que utilice la función de módem SMS. Debido a la naturaleza del sistema GSM y la interconexión con varios dispositivos, MCDI recomienda no utilizar el envío de SMS para propósitos críticos.

SECURITHOR puede poner las señales SMS en una cola de espera en caso de no haber canales disponibles. Esto puede resultar en un retraso en el envío y recepción de señales SMS.

La transmisión entre un operador GSM a otro puede producir retardos a veces medidos en horas.

A pesar de que SECURITHOR puede ser configurado para enviar correos electrónicos o SMS de forma automática, la función SMS no está diseñada para

trabajar de manera completamente desatendida. Los mecanismos de programación para reiniciar o reconectar esta función a equipos o proveedores terciarios no son garantizados por MCDI.

### **CONECTANDO MODEMS SMS A STReceiver (entrantes y salientes)**

Los módems emisores y receptores deben conectarse a STReceiver (> 1.1.0.5) Ubique STReceiver en la carpeta MCDI>STReceiver. Ábralo si aún no está siendo ejecutado con su SECURITHOR. Típicamente se muestra un icono de STReceiver en su escritorio durante la primera instalación de SECURITHOR.

Los módems SMS se conectan por medio del puerto en serie o USB. Ambos tipos aparecerán en la columna izquierda de STReceiver Ej. un puerto COM será mostrado.

Si STReceiver no logra inicializar al módem SMS el mensaje de 'error al abrir puerto' será desplegado en la parte derecha de la ventana de tráfico.

Haga clic en puerto COM en la ventana de STReceiver. Una ventana emergente desplegara los parámetros. Seleccione SMS desde la lista tipo de receptor. Haga clic en abrir si no necesita cambiar los parámetros. Generalmente no necesita cambiar absolutamente nada.

Una vez inicializado, el número de puerto COM será desplegado en la ventana de tráfico. Las señales SMS recibidas serán también mostradas.

En la lista de puertos COM de la izquierda, verá el nombre SMS seguido de un número telefónico.

### **RECIBIENDO SEÑALES DE ALARMA MEDIANTE SMS.**

El receptor de alarmas SMS acepta mensajes que contienen dos formatos: ID de contacto y 4x2. El mensaje puede contener varios eventos de alarma así como una combinación de los diferentes formatos. Cada evento de alarma tiene que estar separado por un espacio (ASCII 32), un carácter de línea (ASCII 10) o retorno de carro (ASCII 13).

Ejemplo:

AAAATZ AAAATTTTPPZZZ AAAA18TTTTTPPZZZC del mensaje SMS:  
455401 0000140100001 222218145101002E.

A – Cuenta.

T - Tipo de alarma.

Z - Zona usuario.

P – Partición.

C - Suma de verificación.

Alarma transmitida a SECURITHOR usando ejemplos de mensajes SMS previos, Receptor(1) y Línea(1):

Fecha y hora 11 4554 01 { teléfono }.

Fecha y hora 11 0000 E401 00 001 { teléfono }.

Fecha y hora 11 2222 E451 01 002 { teléfono } .

Módems SMS entrantes y salientes, utilice el mismo proceso de conexión para STReceiver. Un módem puede ser compartido como entrante o saliente a pesar de que sólo un canal puede ser utilizado en un momento dado.

Las señales entrantes son tratadas en orden FIFO (primero en entrar primero en salir). La cola de salida es virtualmente ilimitada ya que cada elemento es grabado en la base de datos antes de ser enviado. ADVERTENCIA: Si se rompe la conexión con el módem, grandes cantidades de señales pueden potencialmente ser puestas en la cola por SECURITHOR.

### **ENVIANDO SMS.**

Los SMS pueden enviarse de distintas formas:

- Usando un formato de correo electrónico a SMS (Los proveedores GSM deben permitir correos a SMS). Refiérase a la sección de envío de correos electrónicos.

- Usando una puerta de salida que provea envíos de correo a SMS. Refiérase a la sección de envío de correos electrónicos.
- Usando un módem SMS.

### **Enviando SMS vía puerta de salida de correo electrónico (Operadores GSM o puertas de salida de correo a SMS).**

Los SMS vía puerta de salida de correo electrónico son enviados por SECURITHOR como correos y convertidos a SMS mediante la puerta de salida. Siga las instrucciones de su operador GSM para formatear las direcciones de correo electrónico o siga las instrucciones de su proveedor de puerta de salida de correo a SMS.

Refiérase a la sección ENVÍO DE CORREOS para ver acciones de correo específicas.

### **ENVIANDO SMS USANDO UNO O MÁS MÓDEMS.**

Es posible utilizar el mismo módem SMS para enviar y recibir. Típicamente los módems permiten sólo una acción en un momento dado.

SECURITHOR puede usar varios módems SMS ya sea para enviar o recibir permitiendo de esta manera que hayan más canales disponibles.

SECURITHOR no pone límites de SMS enviados por cada señal de alarma. El límite es por lo general el número de canales salientes disponibles que estén conectados a su componente STReceiver en SECURITHOR. Pueden enviarse correos electrónicos y SMS al mismo tiempo. Es posible distribuir módems SMS a lo largo de una red utilizando varios STReceiver. Vea instalación y configuración de STReceiver para aprender a conectar varios STReceiver a SECURITHOR.

Vaya a Cuentas>Administración de códigos de alarma >SMS

Descripción SMS:

Nombre: usado para identificar un número de teléfono específico Ej. 'MCDI HQ'

Remitente SMS (Cualquiera): el primer módem disponible que enviará SMS (round robin).

Remitente SMS (ninguno): no se envían SMS para esta cuenta.

Remitente SMS (primario): identifica al primer módem para salida (por medio de alias).

Remitente SMS (secundario): identifica al módem secundario para salida (por medio de alias).

Nota: el seleccionar siempre 'cualquiera' podría permitir mayor disponibilidad. Seleccionar 'específico' permite adaptar un módem SMS que utilice una tarjeta SIM de cierto proveedor a un proveedor GSM reduciendo a veces el costo de transmisión.

Número telefónico: este es el número al que está enviando SMS. Hay una entrada definida por cada cuenta y todas las particiones utilizarán este número.

### **Encabezado, asunto y pie de página de eventos.**

Puede escribir un asunto, encabezado o pie de página de un mensaje para identificar su CMS o felicitar sus suscriptores. Los pies de página y encabezados son comunes en los correos/SMS enviados. Vaya a Configuraciones>Configuraciones de Internet > Configuración de notificación de eventos para cambiar el asunto, el encabezado y el pie de página de un evento,. Estos cambios serán aplicados a todos los correos electrónicos y SMS enviados. Puede introducir más de 20000 caracteres en el asunto, encabezado o pie de página. De cualquier manera si utiliza SMS, tenga en mente las restricciones de su longitud.

### **Limitaciones del número de caracteres de un SMS.**

La mayoría de los proveedores limitaran este número a 140 y a veces a 155. ADVERTENCIA: enviar caracteres doble byte (no latinos) reducirá la cantidad permitida a 77.

**ENVIANDO CORREOS ELECTRÓNICOS.**

**ADVERTENCIA:** Enviar correos electrónicos requiere conexión a Internet. Debe tener instalado un Firewall. Su proveedor de Internet deberá estar al tanto de una posible alta demanda de tráfico de correo.

Cómo configurar:

Vaya a Cuentas>Administración de códigos de alarma >Códigos de alarma  
Seleccione la fila de códigos de alarma. Agregue las direcciones de correo que le gustaría contactar al recibir este código de alarma y selecciónelo.

Por favor note que todas las direcciones de correo para esta cuenta serán desplegadas en la lista pero únicamente los elementos seleccionados de la columna evento serán atribuidos a este código de alarma.

Cada vez que se recibe un código de alarma seleccionado y definido en SECURITHOR, un correo electrónico será enviado a la dirección seleccionada con un asunto, encabezado y pie de página generales.

Vea la sección encabezado asunto y pie de página de eventos para más información acerca de estos temas.

Tenga cuidado si la cuenta, partición o código de alarma están deshabilitados ya que no será enviado ningún correo electrónico o SMS.

**CONFIGURACIÓN DEL SERVIDOR DE CORREO ELECTRÓNICO.**

Cómo configurar:

Vaya a Configuración> Configuración de Internet.

Seleccione 'Habilitar correo electrónico' para usar esta función.

Llene el cuadro servidor SMTP y los cuadros de puertos SMTP con los datos proporcionados por el administrador de su sistema. Si su servidor SMTP requiere autenticación, introduzca la clave y contraseña del servidor SMTP tal como le indique el administrador de su sistema.

SECURITHOR únicamente soporta autenticación de usuario / contraseña. SSL no es soportado.

Verifique si el software antivirus permite que su puerto dirija el tráfico al servidor de correo electrónico saliente.

Verifique con el administrador de su sistema / proveedor de Internet que puede dirigir grandes cantidades de correos electrónicos. Esto podría requerir ancho de banda de carga así como una provisión especial en el servidor de correo.

**AGREGAR/ELIMINAR DIRECCIONES DE CORREO ELECTRÓNICO.**

Cómo configurar:

Vaya a Cuentas>Administración de códigos de alarma >Lista de Correos / SMS para eventos entrantes >Correos de partición.

Nombre : descripción de cuenta de correo.

Evento: Habilitar o deshabilitar el envío a esta dirección.

Dirección de correo electrónico: introduzca el correo.

Las direcciones de correo electrónico pueden agregarse o eliminarse en esta sección.

No hay límites en el número de correos electrónicos o destinos que puede introducir.

## SECCIÓN MISCELÁNEA.

Contenido del directorio de SECURITHOR.

Esto debería de ser documentado.

Requerimientos mínimos de hardware para SECURITHOR ST1 – estación sencilla.

### REQUERIMIENTOS.

#### **Para ST1 Estación Sencilla.**

Requerimientos mínimos para Windows XP (preferido):

Windows XP service pack 2.

Procesador 1.8 Ghz en adelante (Core dúo recomendado).

Compatible con la mayoría de los procesadores Core dúo y de 64 bits.

512MB de memoria (1Gb en adelante).

Procesador grafico con 64Mb de memoria (128 Mb en adelante).

200MB de espacio libre en disco duro para la instalación inicial.

Espacio libre en disco duro de acuerdo con el tráfico.

Dispositivo de archivado: unidad removible para respaldos

Capacidad de salida de audio.

Capacidad de acceso a Internet.

Cuenta de administrador para la instalación inicial.

#### **Requerimientos minimos para Windows VISTA o 7**

Requerimientos propios de Windows VISTA o 7 compatible con la mayoría de los procesadores Core dúo y de 64 bits.

#### **SECURITHOR STnet EDICIÓN DE RED.**

Nota: Los siguientes son requerimientos mínimos. Operaciones específicas o de alto tráfico probablemente requerirán mayores recursos. Discuta estos últimos con MCDI a la hora de hacer la planificación de su red.

#### **SERVIDOR PARA STnet.**

Windows XP SP3, VISTA (con actualización de plataforma), Windows 7.

CMS con mayor trafico deberá considerar:

Windows server 2003 SP2, Windows server 2008 R2, Windows SBS 2008.

Motor de SQL: PostgreSQL (provisto con STnet). No requiere o permite otro motor SQL.

La base de datos con PostgreSQL puede instalarse en un servidor de forma separada.

Los receptores pueden distribuirse en red o conectarse a una PC/servidor dedicado.

Mínimo (<5000 cuentas, 1-4 estaciones).

>2 Ghz Pentium 4.

>1 Gb de memoria.

Ethernet a 100Mb.

Tarjeta de video con 64 Mb si se usa un despliegue.

Disco duro con espacio suficiente (instalación inicial de 750Mb).

Dispositivo de almacenamiento removible o independiente para respaldos.

Un ruteador/switch ethernet fiable.

Recomendado (mínimo para >5000 cuentas o 4 estaciones+).

2 Ghz Procesador Core dúo o superior.

4 Gb de memoria en adelante .

Ethernet a 100/1000.

Tarjeta de video con 64 Mb si se usa con despliegue.

Disco duro con capacidad suficiente (instalación inicial 750 Mb). SSD de alta velocidad de lecto-escritura preferiblemente.

Dispositivo de almacenamiento removible o independiente para respaldos.

Un ruteador/switch ethernet fiable.

Para las estaciones conectadas al servidor los requerimientos son iguales a los de ST1.

#### **SOPORTE A IDIOMAS.**

La versión Beta actual incluye Danés, Inglés, Francés, Griego, Italiano, Español, Portugués y Ruso. Pueden agregarse más idiomas si se proporciona la traducción de forma gratuita. Contacte al grupo de soporte de MCDI para añadir otro idioma.

Algunos OEM (fabricantes de equipo original) o versiones específicas tienen restricciones de idioma.

Pueden agregarse otros idiomas con la previa traducción del archivo maestro de SECURITHOR y un acuerdo comercial con MCDI SP Inc.

SECURITHOR usa un motor de bases de datos llamado PostgreSQL. Para mayor información sobre PostgreSQL, visite [postgresql.org](http://postgresql.org) o Wikipedia. SECURITHOR utiliza la versión 8.3.

Hasta el momento SECURITHOR no está diseñado para administrar las tablas de SQL mediante usuarios. MCDI está trabajando en un componente especial para la versión 2.0.

En la versión de estación sencilla de SECURITHOR, la tabla de SQL es local. Para la versión de red, esta tabla SQL será ubicada en un servidor conectado sobre IP.

Ningún otro motor SQL será permitido o utilizado.

Preguntas, actualizaciones y capacitación están disponibles en SECURITHOR.COM. También hay otros recursos disponibles en MCDI.COM.

Inglés y francés.

Ventas e información general [securithor@mcdi.com](mailto:securithor@mcdi.com)  
Soporte [support@mcdi.com](mailto:support@mcdi.com).

Español.

Ventas e información general [ventas@mcdi.com](mailto:ventas@mcdi.com)  
Soporte [soporte@mcdi.com](mailto:soporte@mcdi.com).

## **PostgreSQL.**

## **Recursos WEB .**

## Opciones de soporte.

Los contratos de soporte están disponibles mas allá del límite de garantía de un año en incrementos de 3, 6 y 12 meses. El soporte esta disponible durante las horas de oficina de MCDI. Un contrato de soporte de 24 horas también está disponible después del límite de garantía original de un año. Este contrato de soporte las 24 horas no esta ofrecido por MCDI Security Products Inc. sino directamente por MCDI Sudamérica.

La recuperación y migración de datos se hacen solamente mediante un contrato de soporte de un año.

Debido a la complejidad de la base de datos SAMM / WinSAMM y de las formas que tienen las estaciones centrales para introducir y utilizar los datos, MCDI ofrece herramientas generales para la migración de SAMM o WinSAMM a SECURITHOR en un mejor esfuerzo sin ningún tipo de garantía. La migración de datos de SAMM o WinSAMM a SECURITHOR no está soportada aunque MCDI continúe recibiendo reportes de errores y a futuro juzgará si se requiere una corrección a las herramientas de migración.

Contacte al equipo de soporte de MCDI para discutir la mejor opción de soporte para su estación central en [support@mcdi.com](mailto:support@mcdi.com) o llame al +514-481-1067

## Garantía limitada de productos de software.

El software de aplicación de SECURITHOR está bajo garantía limitada de un año comenzando con la fecha de compra. Las actualizaciones pagadas de SECURITHOR están cubiertas por garantías limitadas de 3 meses partiendo de la fecha de compra.

Durante este periodo, el soporte técnico está libre de cargo durante horario normal de trabajo. El soporte técnico es una ayuda en la instalación inicial del software de MCDI Security Products Inc. para asegurarse de que las funciones básicas trabajen. La capacitación no está incluida y el soporte técnico deberá hacerse en un acuerdo separado. Los problemas de compatibilidad o funcionamiento de la computadora no relacionados directamente a SECURITHOR no están cubiertos. Los conflictos de operación con software o equipo de terceros están excluidos de la garantía de software de MCDI Security Products Inc.

Después del periodo original de garantía limitada, tenemos disponibles contratos de soporte a software de distinta duración. Los contratos de soporte anuales incluyen actualizaciones a las últimas versiones.

Esta garantía solo es valida en forma de contrato entre el comprador original y MCDI Security Products Inc. MCDI Security Products Inc. no otorga ninguna otra garantía ya sea oral o escrita, expresa o implícita. MCDI Products Inc. Tampoco asume ni autoriza a ninguna otra persona a actuar a su nombre para modificar o cambiar esta garantía, ni a asumir ninguna otra garantía o responsabilidad con respecto a este producto.

MCDI Security Products Inc. no se hace responsable de los daños resultantes de forma directa o indirecta, pérdidas de ganancias anticipadas en tiempo o cualquier otra pérdida en la que incurra el comprador o usuario en relación con la compra, instalación, operación o fallo de este producto. Por favor refiérase a la licencia incluida con SECURITHOR, WinSAMM y el instalador de SAMM. También puede pedir una copia por via electrónica a MCDI Security Products Inc. de acuerdo con su licencia de software en [securithor@mcdi.com](mailto:securithor@mcdi.com).

## Productos de Hardware.

Las versiones OEM, de prueba y los demos no están cubiertas por la presente garantía excepto cuando se especifique.

Las herramientas de conversión de datos de SAMM o WinSAMM a SECURITHOR no están cubiertas por ninguna garantía y son provistas tal cual. MCDI dará soporte haciendo su mejor esfuerzo pero no ofrece garantía a las herramientas de conversión de datos.

El material electrónico fabricado por MCDI está bajo garantía limitada de tres años partiendo de la fecha de compra a menos de que se especifique lo contrario. Todo el equipo fabricado conforme a RoHS tiene garantía de 2 años a partir de la fecha de compra. Durante estos periodos, los productos electrónicos deberán estar libres de defectos en materiales y mano de obra bajo uso normal. En cumplimiento a cualquier violación a esta garantía, MCDI Security Products Inc. deberá, a su criterio, reparar o reemplazar el equipo defectuoso una vez que sea regresado a nuestra compañía o centro de servicio con el porte pagado.

Esta garantía aplica a defectos en partes y mano de obra y no a daños por causas fuera del control de MCDI Security Products Inc., tales como daños en el manejo o envío, descargas, voltaje excesivo, golpes, humedad o daños por abuso, alteración o aplicaciones no previstas o impropias del equipo.

Esta garantía sólo es válida en forma de contrato entre el comprador original y MCDI Security Products Inc. MCDI Security Products Inc. no otorga ninguna otra garantía ya sea oral o escrita, expresa o implícita. MCDI Security Products Inc. Tampoco asume ni autoriza a ninguna otra persona a actuar a su nombre para modificar o cambiar esta garantía, ni a asumir ninguna otra garantía o responsabilidad con respecto a este producto.

MCDI Security Products Inc. no se hace responsable de los daños resultantes de forma directa o indirecta, pérdidas de ganancias anticipadas en tiempo o cualquier otra pérdida en la que incurra el comprador o usuario en relación con la compra, instalación, operación o fallo de este producto.

**Advertencia:** Todo equipo o producto de software usado para monitoreo, vigilancia o cualquier otro propósito de seguridad deberá ser probado completamente con cierta frecuencia. A pesar de las constantes pruebas realizadas es posible que en algunos casos el desempeño de nuestros productos no sea óptimo.

**Extensión de garantía para hardware:** Es posible adquirir una extensión de garantía para algunos productos de MCDI Security Products Inc. al momento de la compra del equipo. La extensión de garantía que se otorga actualmente (a partir de noviembre del 2010) cubre 4 modelos: Exprecium 2 ( \$250.00 dólares americanos al año), Exprecium 3: (\$275.00 dólares americanos al año) Decrypta 3 (\$325.00 dólares americanos al año) Decrypta 5/6 (contacte a MCDI). Para la protección contra alto voltaje agregue \$175.00 dólares americanos al año si se trata de un receptor de 2 líneas (la extensión debe hacerse dentro de la garantía original), y agregue \$525.00 dólares americanos al año para los receptores de 6 líneas. Reemplazo avanzado: \$100.00 dólares de cuota fija al usuario final + costo de envío (requiere depósito mediante tarjeta de crédito o valor de reemplazo).

Términos de la extensión de garantía:

- La extensión de garantía es válida para el propietario original solamente.
- El cliente deberá obtener el número de retorno de mercancía (RMA) o beneficiarse del servicio de garantía.
- La extensión de garantía deberá adquirirse con la compra original.
- Los daños cosméticos y a las cajas no están cubiertos.
- La protección contra alto voltaje no esta cubierta a menos que se especifique.
- Los cables y accesorios no están cubiertos.
- El equipo deberá reenviarse con porte pagado a MCDI Montreal.
- El equipo será reemplazado por otro nuevo o reacondicionado a criterio de MCDI.
- El equipo será reemplazado por otro de nueva generación si el original ya no está disponible.
- El costo de envío no está incluido.
- Las estimaciones de reparación se efectúan en dos días hábiles.
- Las ofertas están sujetas a cambio sin previo aviso.

## Actualizando desde SAMM

Es posible migrar algunos datos de SAMM a SECURITHOR. Esta migración requiere la compra de una licencia de SECURITHOR. Algunos precios especiales están disponibles para los usuarios de SAMM SSUU que deseen migrar a SECURITHOR ST1.

La migración de datos es posible desde la versión de SAMM 8.1 en adelante. Esta migración se hace convirtiendo primeramente los datos de SAMM a WinSAMM WSUU 1.2.17a (provisto por MCDI en el paquete de migración de SECURITHOR).

Primero ejecute WinSAMM\_installer.exe. Esto realizará un respaldo de los datos de SAMM al directorio de SAMM en su PC.

Seleccione la opción actualizar en SAMM. El instalador hará la conversión de la base de datos al formato de WinSAMM. Deberá verificar la integridad de los datos una vez que la conversión haya finalizado y antes de continuar, seleccionando cuentas, códigos de alarmas y programación.

Una vez que se encuentre satisfecho con la transferencia de datos de SAMM a WinSAMM, inicie la herramienta de importación provista por MCDI. La herramienta de importación debe estar ubicada en el mismo directorio de SECURITHOR y debería correr en una base de datos nueva. La herramienta de importación no debe de ser usada en SECURITHOR con entradas previas. Algunos datos no son transferidos a SECURITHOR tales como los eventos. Contacte a MCDI para aplicaciones específicas.

Sería adecuado ensayar en repetidas ocasiones la conversión de datos para verificar su integridad y repetir este proceso cuando esté listo para migrarlos. Los datos introducidos en SAMM al momento de hacer la migración a SECURITHOR no serán transferidos a WinSAMM o SECURITHOR.

Debido al gran número de bases de datos, las versiones y la manera en que las estaciones centrales introducen y utilizan los datos, MCDI no garantiza la eficiencia de las herramientas de migración. Están diseñadas de manera óptima. No se brinda soporte a la migración de datos a pesar de que se reciban reportes de error, se decidirá si son necesarias ciertas correcciones en futuras versiones.

MCDI proveerá números serie para sus viejas versiones de SAMM después de 3 meses de la fecha de compra o actualización de la licencia de SECURITHOR. Si decidió adquirir una nueva licencia de SECURITHOR, MCDI proveerá números de serie a ambas aplicaciones.

### **Actualización desde WinSAMM (próximamente).**

Es posible migrar algunos datos desde WinSAMM a SECURITHOR. Esta migración requiere de una licencia de SECURITHOR. Algunos descuentos especiales están disponibles a usuarios de WinSAMM WSUU1 que quieran migrar a SECURITHOR ST1.

La migración de datos es posible desde WinSAMM 1.2.17a. con la compra de su licencia de SECURITHOR, una herramienta de migración hará la conversión de los datos de WinSAMM al formato de SECURITHOR automáticamente. Contacte al equipo de soporte de MCDI para recibir notas de las aplicaciones y las últimas herramientas de conversión.

Este proceso es transparente para el usuario. Deberá verificar rigurosamente los datos convertidos antes de utilizar a SECURITHOR para propósitos de monitoreo.

La herramienta de importación debe estar ubicada en el mismo directorio que SECURITHOR y deberá ser ejecutada en una base de datos nueva. La herramienta de importación no puede ser utilizada en SECURITHOR con entradas previas. Algunos datos como los eventos no son transferidos a SECURITHOR. Contacte a MCDI para aplicaciones específicas.

Sería adecuado ensayar en repetidas ocasiones la conversión de datos para verificar su integridad y repetir este proceso cuando esté listo para migrarlos. Los datos introducidos en WinSAMM al momento de hacer la migración a SECURITHOR no serán transferidos a WinSAMM o SECURITHOR.

Debido al gran número de bases de datos, las versiones y la manera en que las estaciones centrales introducen y utilizan los datos, MCDI no garantiza la eficiencia de las herramientas de migración. Están diseñadas de manera óptima. No se brinda

soporte a la migración de datos a pesar de que se reciban reportes de error, se decidirá si son necesarias ciertas correcciones en futuras versiones. Algunos campos de datos son diferentes en WinSAMM y SECURITHOR, algunos muy notorios como Nombre que ahora se ha dividido en Nombre y Apellido en SECURITHOR.

MCDI proveerá números serie para sus viejas versiones de WinSAMM después de 3 meses de la fecha de compra o actualización de la licencia de SECURITHOR. Si decidió adquirir una nueva licencia de SECURITHOR, MCDI proveerá números de serie a ambas aplicaciones.

Una vez satisfecho con el resultado de la transferencia de datos, debería hacer una transferencia de datos final y comenzar a utilizar SECURITHOR de inmediato ya que los datos introducidos en WinSAMM al momento de realizar la migración a SECURITHOR no serán transferidos a este último. Nótese también que **LOS DATOS INTRODUCIDOS A SECURITHOR NO PUEDEN SER TRANSFERIDOS DE VUELTA A WINSAMM.**

**Addendum.**

**Capturas de pantalla.**

**Interfaz de uso general.**

**Interfaz de usuario con ventanas fijas.**

**Interfaz de usuario con ventanas flotantes.**

**Ventana de manejo de cuentas.**

**Ventana de ciudades.**

**Ventana de procesamiento de alarmas.**

**Ventana de tráfico de alarmas.**

**Ventana de seguimiento.**

**Ventana de eventos pendientes.**

**Notas de operador.**

**Administración de operadores.**

**Configuración.**

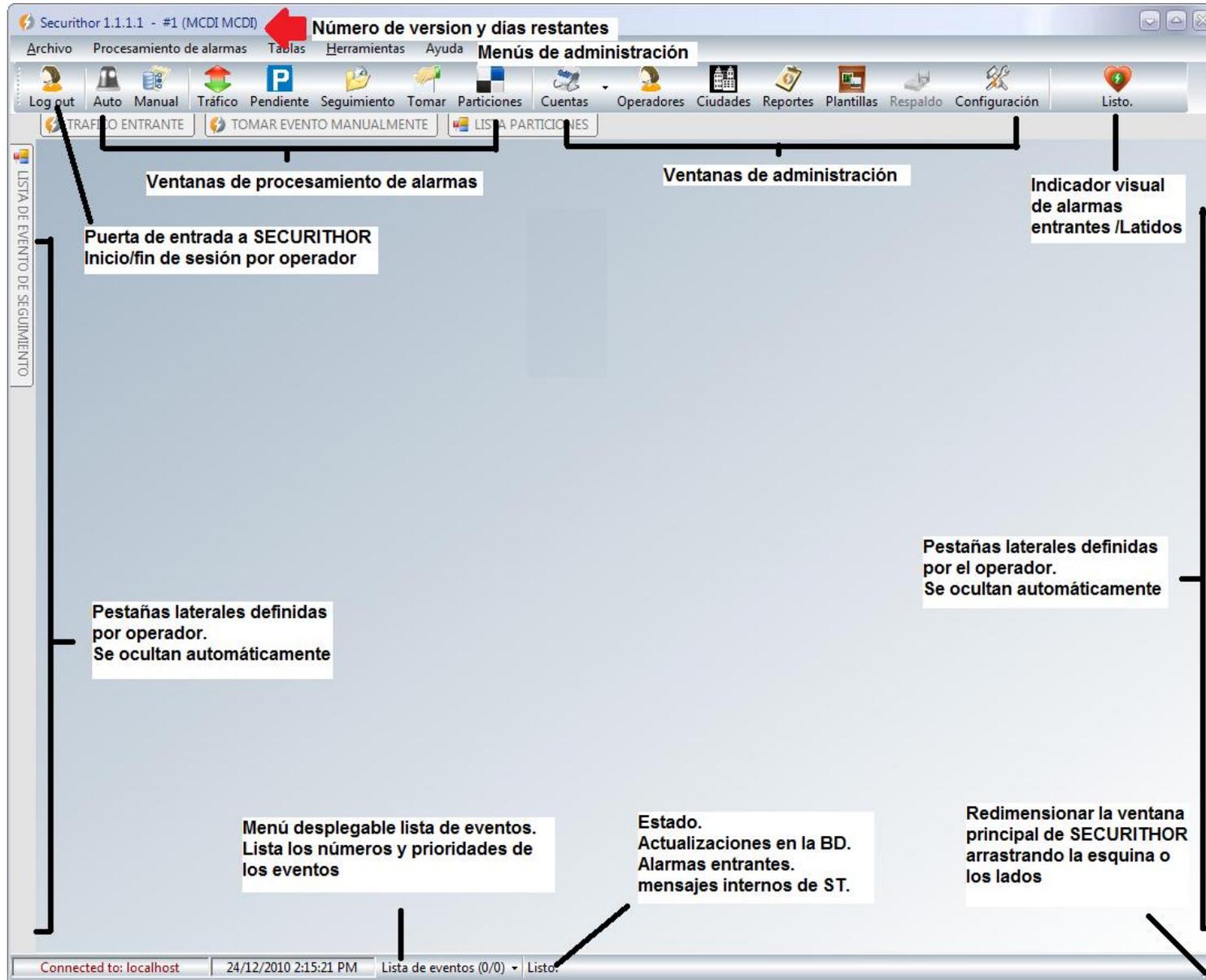
**Configuración de alarma.**

**Configuración de Internet.**

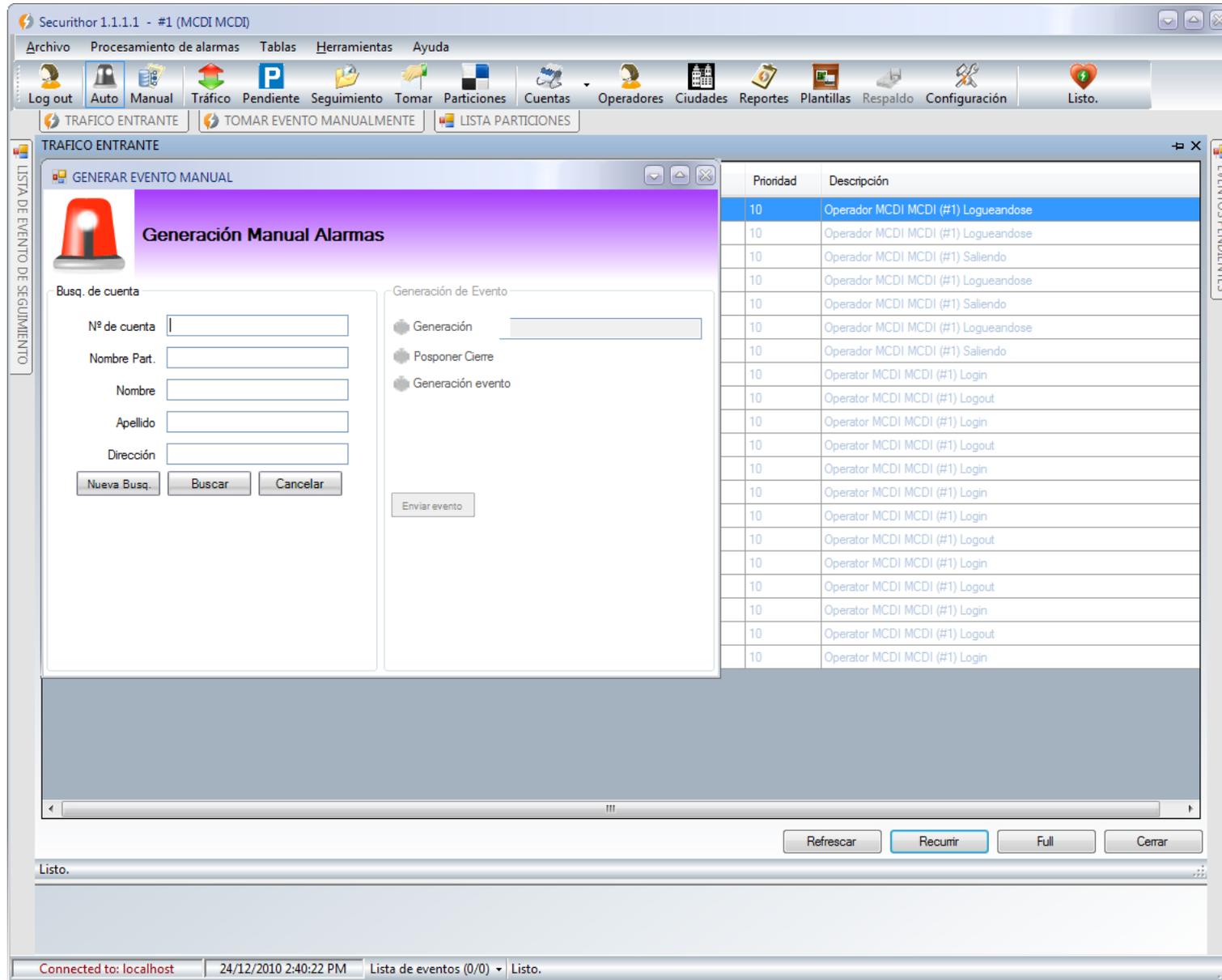
**Configuración de escritorio.**

**Selección de carátulas y muestras.**

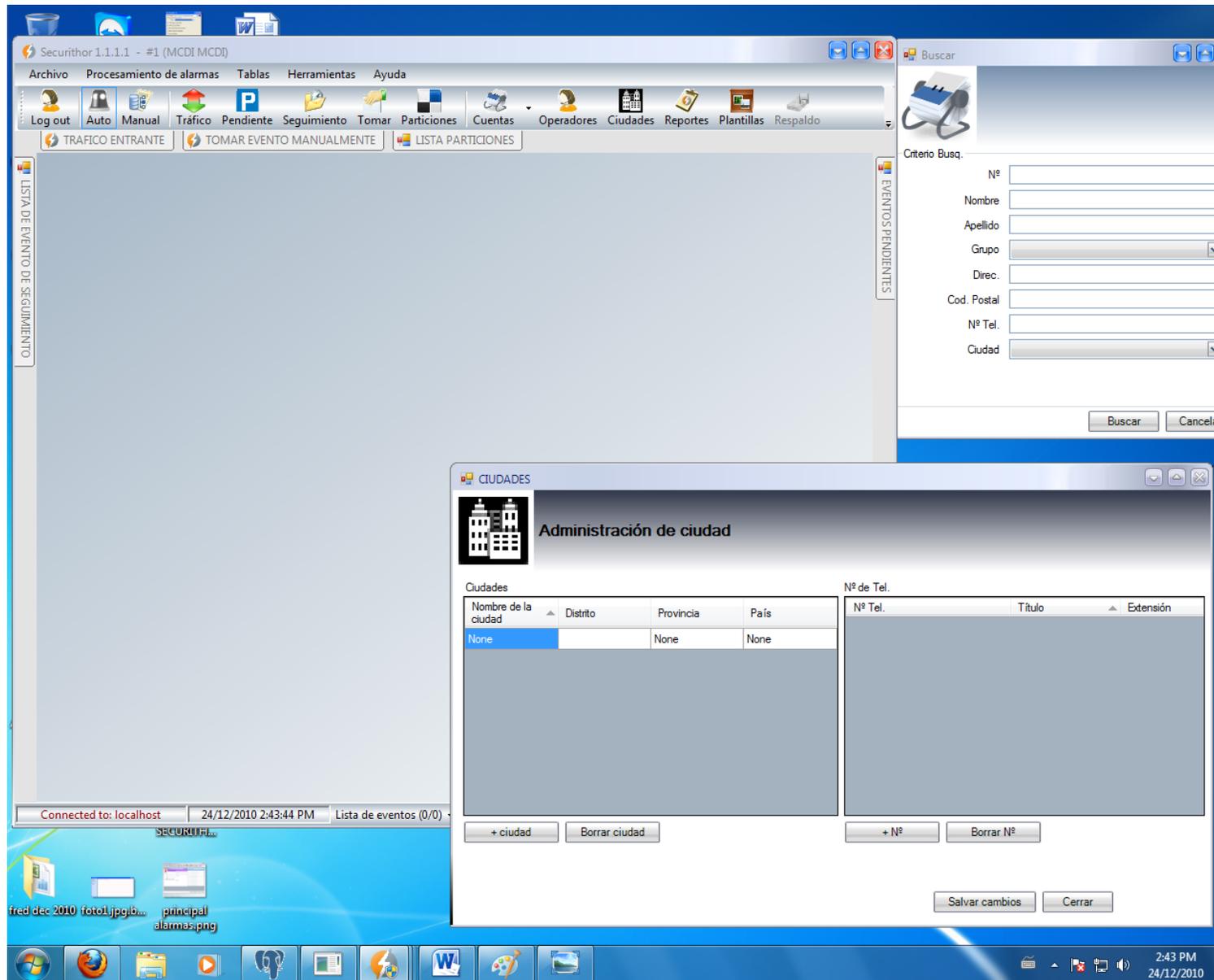
**Ventana principal de SECURITHOR.**



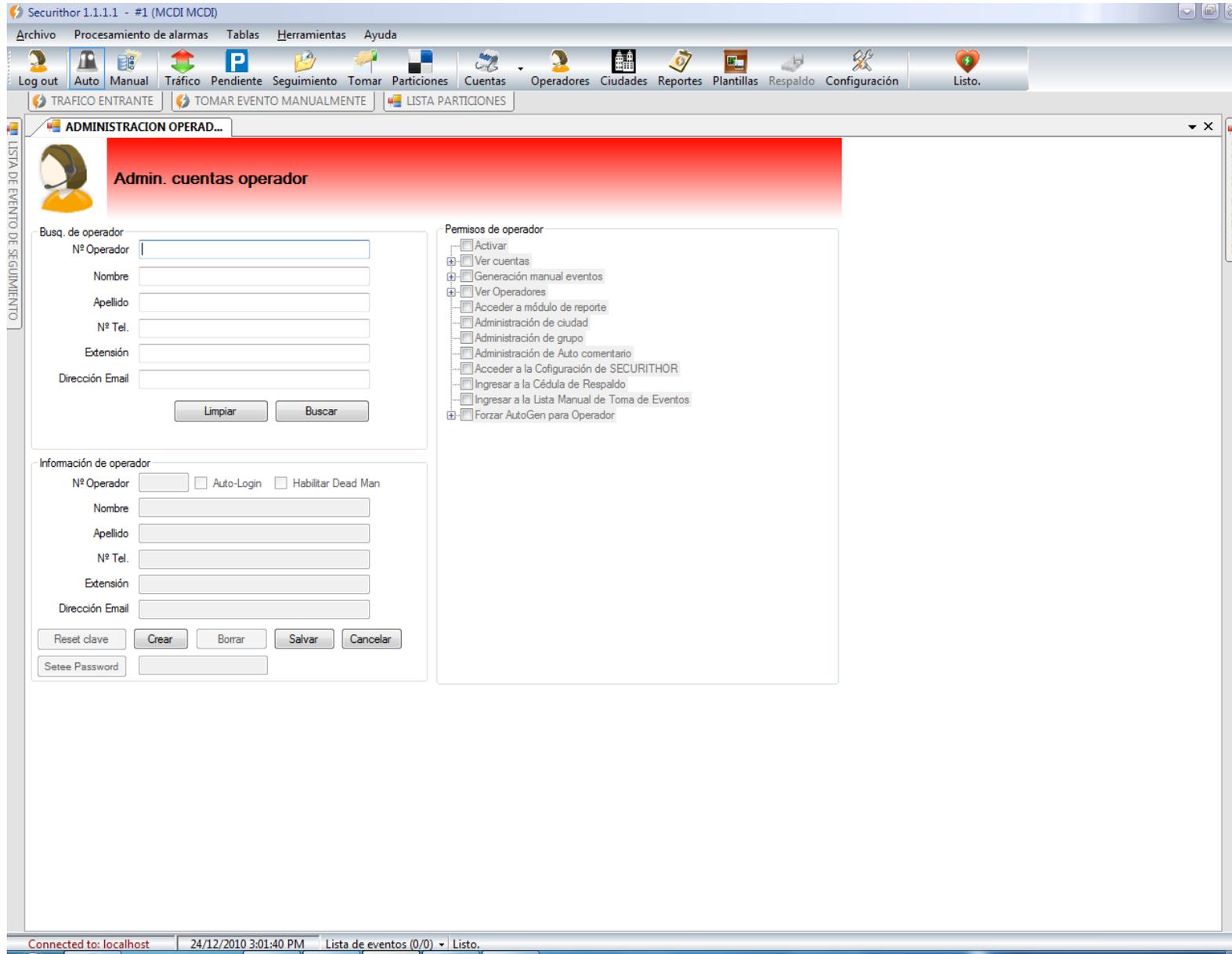
**Interfaz de usuario con ventanas fijas (igual que la anterior mostrando esta vez un formulario).**



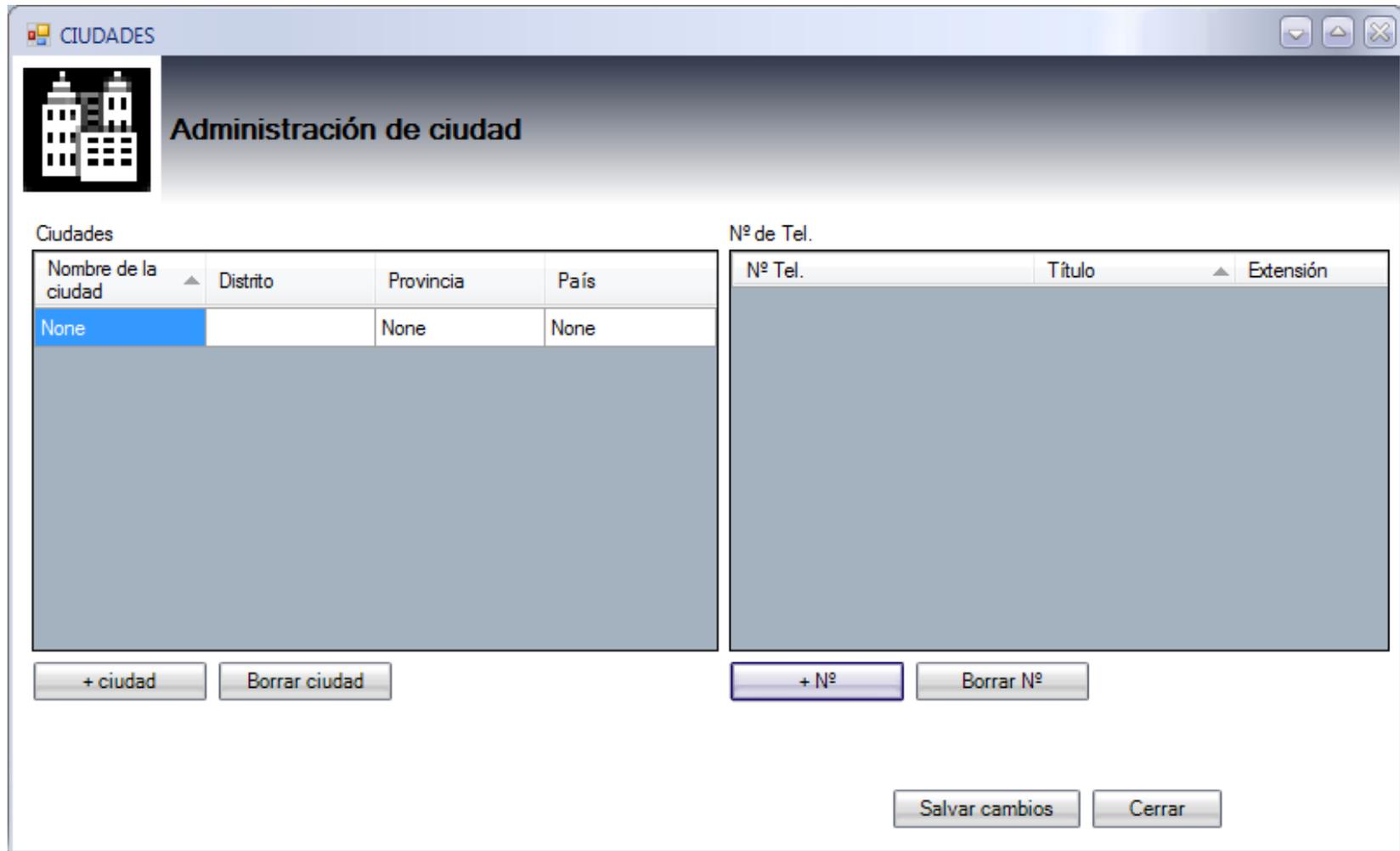
**Interfaz de usuario con ventanas fijas (igual que la anterior mostrando esta vez ventanas flotantes).**



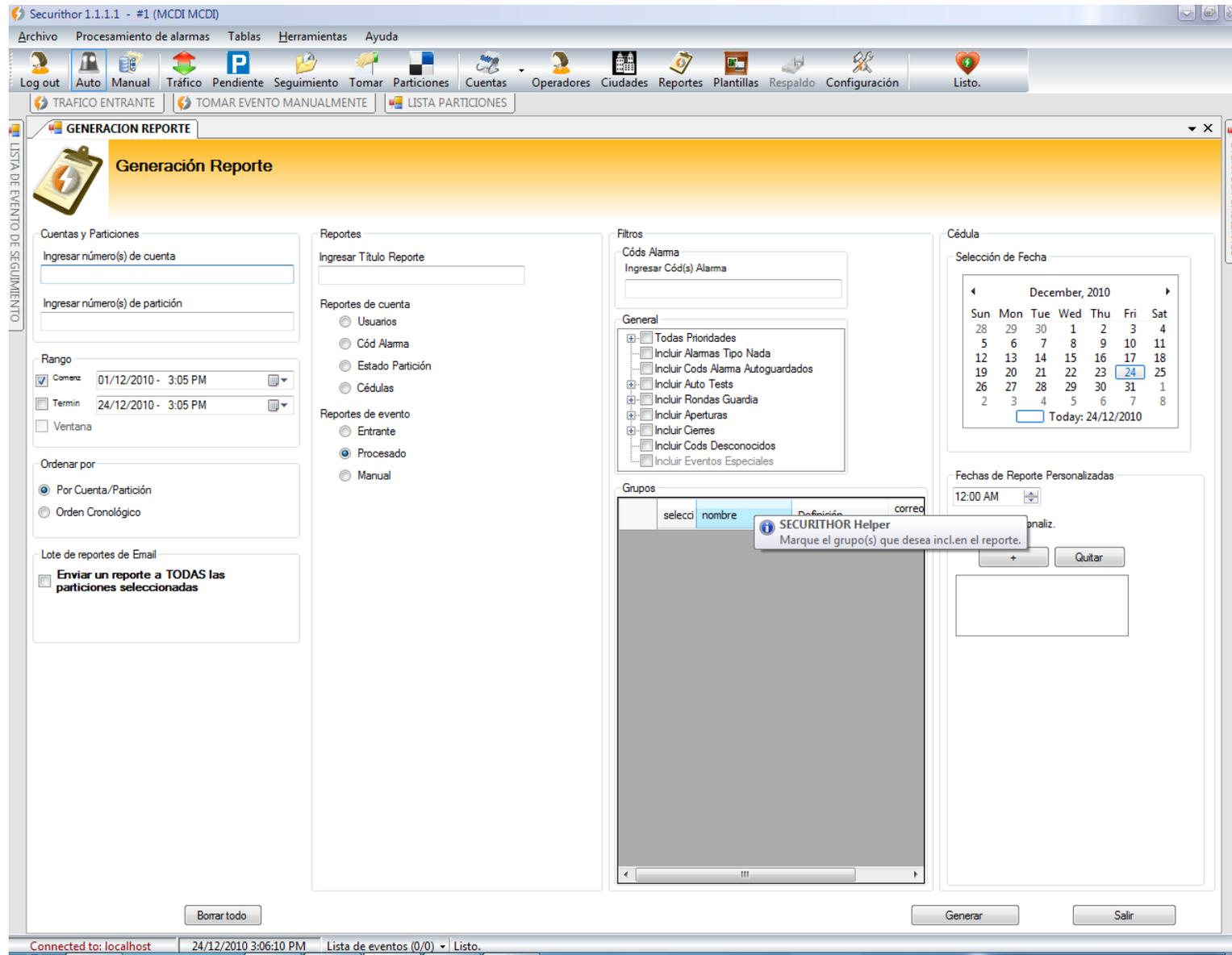
**Administración de cuentas de operadores.**



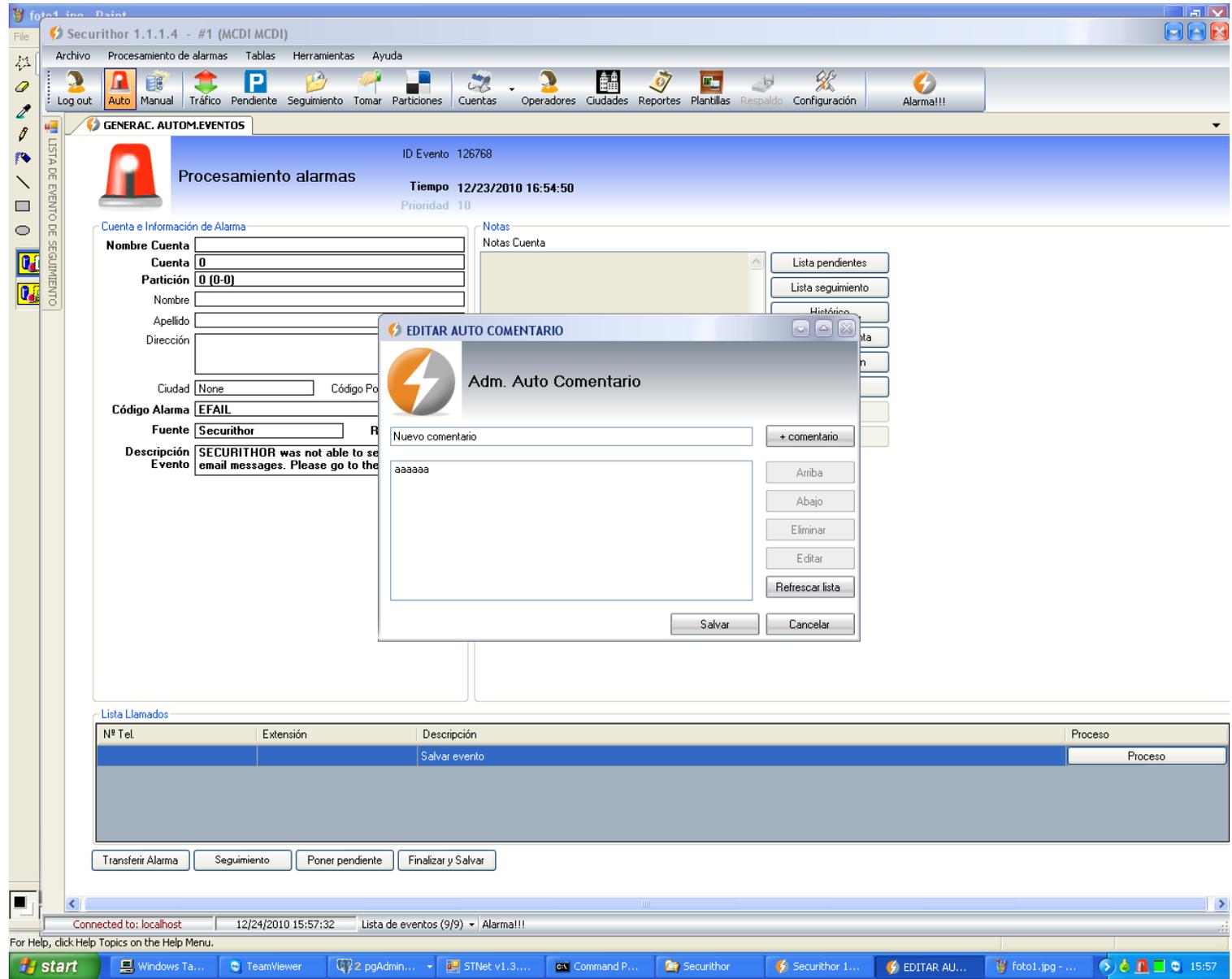
**Ventana de administración de ciudades.**



**Ventana de generación de reportes (próximamente).**



**Ventana de procesamiento de alarmas con cuadro de comentarios, comentarios automáticos habilitados.**



**Configuración de procesamiento de alarmas.**



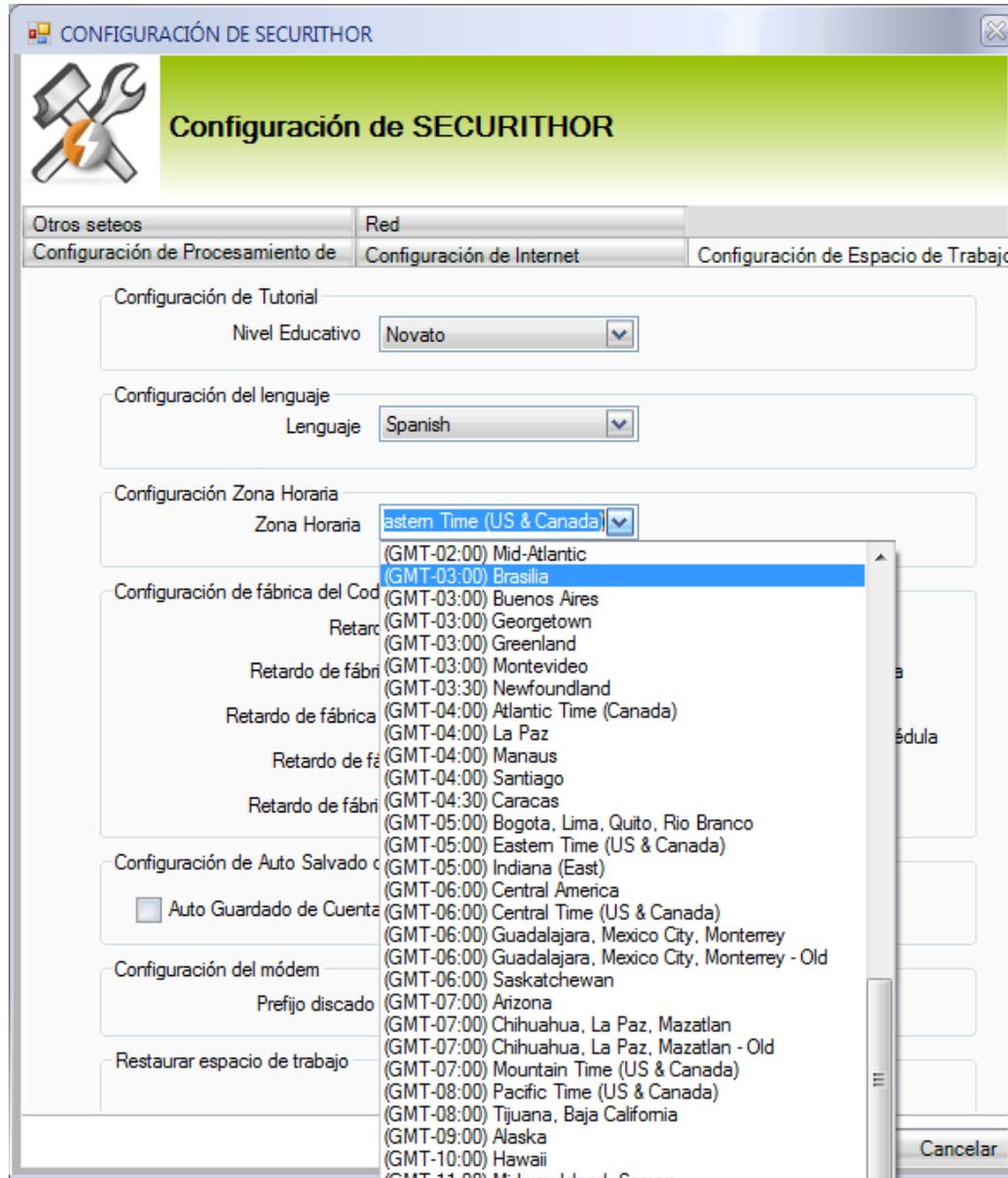
**Configuración de Internet.**

The screenshot shows a software configuration window titled 'CONFIGURACIÓN DE SECURITHOR'. The window has a green header with a wrench and screwdriver icon and the text 'Configuración de SECURITHOR'. Below the header is a tabbed interface with three tabs: 'Otros seteos', 'Red', and 'Configuración de Internet'. The 'Configuración de Internet' tab is active. The main content area contains several sections:

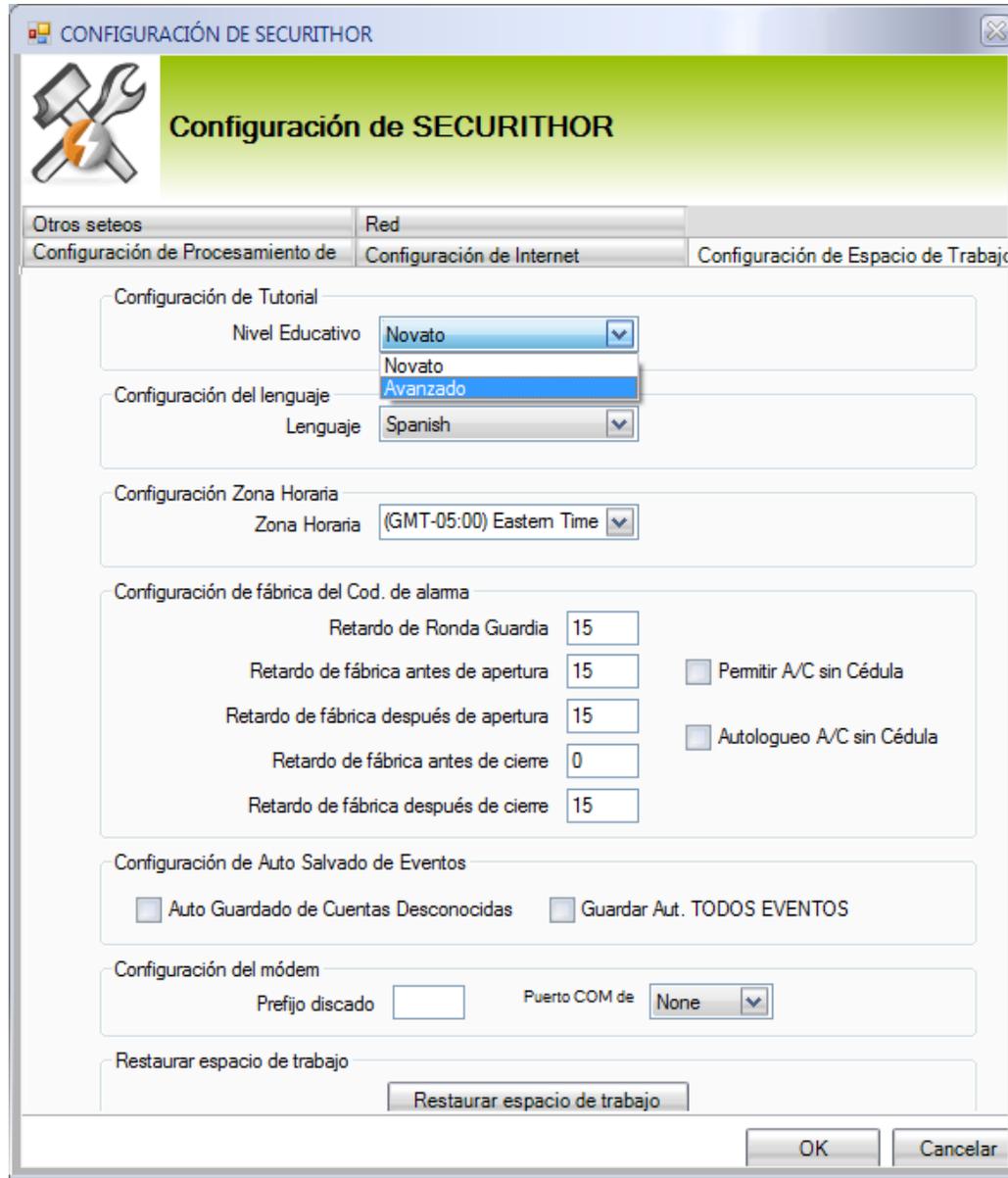
- Habilitar Email:** A checked checkbox.
- Configuración de Internet:** A section containing:
  - Servidor SMTP:** Text box with 'smtp.mcdi.com'.
  - Responder a:** Text box with 'soporte@mcdi.com'.
  - Puerto SMTP:** Text box with '25' and a 'Chequear conexión SMTP' button.
  - Este Servidor SMTP Requiere Autenticación:** A checked checkbox.
  - Usuario SMTP:** Text box with 'usuario'.
  - Clave SMTP:** Password field with masked characters.
- Config de notificación de reporte:** A section containing:
  - Asunto de reporte:** Text box with 'Reporte desde la estación central'.
  - Encabezado de:** Text box with 'Reporte mensual de mi estacion central'.
  - Pie de Página:** Text box with 'contacte al +5552 768756'.
- Configuración de la notificación de evento:** A section containing:
  - Tema de evento:** Text box with 'Notificacion de alarma'.
  - Encabezado:** Text box with 'Su panel envió el siguiente mensaje'.
  - Pie de evento:** Text box with 'Para más infomación contacte a su estación central'.

At the bottom right of the window are 'OK' and 'Cancelar' buttons.

**Configuración de escritorio (Huso horario).**



**Configuración de escritorio (Tipo de usuario).**



### Selección de carátulas.

