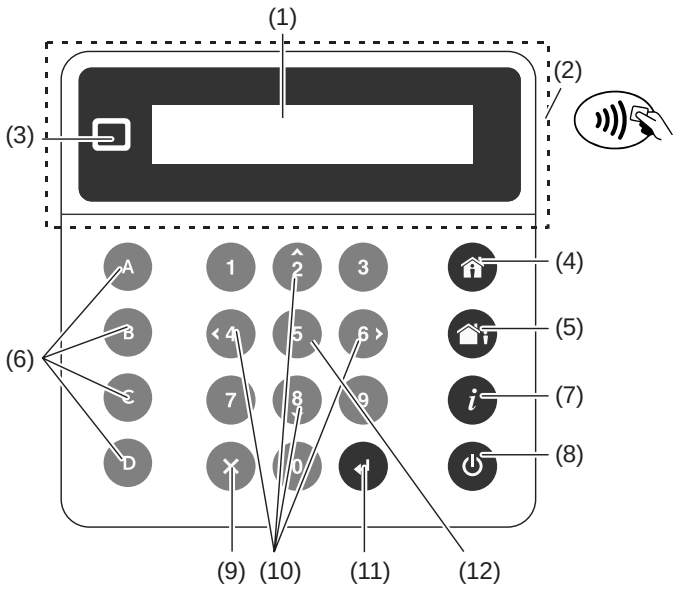
Manual del usuario del teclado de la serie NXG-183x-EUR

1



Descripción

NXG-183x-EUR es una interfaz para usuarios de la familia de sistemas de seguridad xGenConnect.

Figura 1: Diseño del teclado NXG-183x

(1) Pantalla gráfica
(2) Área activa del lector de tarjetas
(3) LED de estado
(4) Botón Armado perimetral
(5) Botón Armado total
(6) Botones de función A, B, C, D
(7) Botón de información del sistema (*i*)
(8) Botón de desarmado
(9) Botón cancelar
(10) Botones de navegación: Arriba (2), Abajo (8), Izquierda (4), Derecha (6)
(11) Botón Entrar (↵)
(12) Botón de selección (5)

Introducción del código PIN

Deberá introducir un código PIN válido para acceder a diversas funciones y a la información del sistema.

Tras un periodo de inactividad, aparecerá un protector de pantalla y el teclado entrará en el modo de ahorro de energía. Pulse cualquier botón para activarlo. Aparecerá una pantalla que le solicitará el código PIN. Se necesita un código PIN válido para desbloquear la pantalla y acceder al sistema.

```
Entre código, entonces ↵
****
```

Introduzca un código de usuario válido y pulse Entrar. Los PIN de usuario pueden contener entre 4 y 8 dígitos. El PIN de usuario maestro predeterminado es 1234.

Si el PIN no es válido para la función a la que intenta acceder, aparecerá el mensaje de advertencia Acceso denegado.

Se asignan los permisos a los usuarios y los teclados para determinar a qué funciones puede acceder un usuario y en qué momentos puede hacerlo. Si no puede acceder a una función, póngase en contacto con la empresa instaladora o el administrador del edificio.

Uso de tarjetas

Los teclados NXG-1832-EUR y NXG-1833-EUR están equipados con un lector de tarjetas Mifare que permite usar tarjetas para iniciar sesión en el sistema y realizar operaciones específicas (serie de tarjetas NXG-180x-5).

Las tarjetas/mandos deben presentarse cerca de la pantalla del teclado, preferiblemente en mitad del área de la pantalla (elemento 1 de la Figura 1).

- Una vez reconocida la tarjeta, el lector genera un único pitido.
- Si se sostiene la tarjeta frente al lector durante un segundo, este generará un doble pitido.
- Si se sostiene la tarjeta frente al lector durante otro segundo, este generará un triple pitido.

Al quitar la tarjeta después de un pitido simple/doble/triple, el usuario puede seleccionar las funciones que se activarán.

Cada nivel de pitido se puede configurar de forma independiente para cualquier combinación de las siguientes acciones:

- Iniciar sesión en el sistema.
- Armado/desarmado.
- Activar escenas o acciones del sistema.
- Desbloquear la puerta.

Consulte la *Guía de instalación y programación de xGenConnect* para obtener más información.

Nota: las funciones de la tarjeta se activan solo si el teclado muestra el protector de pantalla o la pantalla principal.

Las tarjetas están inactivas si el usuario ya ha accedido a los menús del teclado o está en proceso de armado/desarmado. El menú Tarjetas de usuario es una excepción. Consulte “Programación de tarjetas” en la página 7 para obtener información.

P/N 466-5559-ES • REV E • ISS 02MAY22

Estado del sistema

El sistema de seguridad xGenConnect muestra los mensajes de estado del sistema en la pantalla (Figura 1, elemento 1). Por ejemplo, la pantalla principal a continuación muestra la categoría de estado del sistema de Fallo.

```
        Fallo
   Pulse 𝒊 para info
```

Para obtener más detalles sobre el fallo del sistema, pulse el botón Información del sistema (***i***).

Otras categorías de estado del sistema son Alarma, Anulado, No listo, Listo, Armado, etc.

Tenga en cuenta que puede aparecer más de una categoría de estado del sistema a la vez. La pantalla se desplazará por cada categoría automáticamente. También puede desplazarse de forma manual pulsando los botones Arriba (2) o Abajo (8).

Nota: En la condición de alarma, solo se muestran la categoría de estado de la alarma y los mensajes hasta que se confirma la alarma pulsando el botón Desarmar (Elemento 8) y se introduce un PIN válido. No se mostrarán otras categorías de estado en esta condición.

Si se le solicita, pulse el botón Información del sistema (***i***) (Figura 1, elemento 7) para mostrar la lista de mensajes en la categoría de estado actual.

```
Zona en tamper
2-Ent almacén principa_𝒊
```

Para desplazarse por varias alarmas de la categoría, pulse los botones Arriba (2) o Abajo (8).

Puede que los nombres de las particiones o de las zonas no quepan en la pantalla. En este caso, desplácese hacia la izquierda o hacia la derecha con el botón Información del sistema (***i***).

Consulte también “Mensajes de estado del sistema” en la página 8.

LED de estado

El LED de estado (Figura 1, elemento 3) puede mostrar uno de los siguientes estados del sistema (comenzando desde la prioridad más alta):

- Rojo intermitente: Alarma.
- Azul: Fallo, Modo programación on, Sistema no listo, Sistema listo para forzar el armado.
- Amarillo: Anulado, Armado en modo Perimetral.
- Verde: Listo para armado.
- Rojo: Armado en modo Total.

Nota: El LED de estado estará apagado cuando el protector de pantalla esté activo y el sistema esté armado.

Armar el sistema en el modo Total

Introduzca un código válido para desbloquear la pantalla. pulse el botón Armado total (Figura 1, elemento 5) para armar su sistema en modo Total.

Introduzca su PIN y pulse Entrar.

Nota: En caso de que la función de Armado rápido esté habilitada, no se necesitará un PIN para armar el sistema.

Se oirá un sonido (pitidos) que anuncian el retardo de salida. El teclado, que se usa para armar el sistema, mostrará el tiempo (en segundos) que queda para salir de las instalaciones. Salga de las instalaciones durante este tiempo.

Si su sistema tiene habilitado el control de varias particiones y el usuario tiene activada la opción Mostrar lista de particiones, se mostrará la pantalla de selección de Partición. Consulte “Control de varias particiones” en la página 3.

Armar el sistema en el modo Perimetral

Introduzca un código válido para desbloquear la pantalla. Pulse el botón Armado perimetral (Figura 1, elemento 4) para armar el sistema en modo Perimetral.

```
Sel. modo arm y pulse ↵
>Perimetral<
```

Con los botones Arriba (2) y Abajo (8), seleccione uno de los siguientes modos de Armado perimetral:

- Perimetral
- Perimetral instantáneo
- Perimetral instantáneo nocturno

A continuación, pulse Entrar, introduzca el PIN y vuelva a pulsar Entrar.

Nota: En caso de que la función de Armado rápido esté habilitada, no se necesitará un PIN para armar el sistema en el modo Perimetral.

Si su sistema tiene habilitado el control de varias particiones y el usuario tiene activada la opción Mostrar lista de particiones, se mostrará la pantalla de selección de Partición. Consulte “Control de varias particiones” en la página 3.

Modo perimetral

Las zonas de entrada/salida estarán activas y las zonas con la opción de modo Perimetral o modo Nocturno se anularán. La entrada a través de una zona con la opción de entrada/salida iniciará el temporizador de entrada de partición.

El Modo Perimetral le permitirá moverse por el interior de su domicilio o del edificio de oficinas sin que el sistema active la alarma, mientras las puertas y ventanas permanecen activas. La persona que entre en la partición protegida deberá que desarmar el sistema en el tiempo de entrada.

Modo perimetral instantáneo

Las zonas de entrada/salida estarán activas con el periodo de retardo de entrada eliminado y se anularán las zonas con la opción de modo Perimetral o modo Nocturno. La entrada a través de una zona con la opción de entrada/salida activará una alarma instantánea.

El Modo Perimetral instantáneo proporciona un nivel mayor de seguridad y requiere que se desarme el sistema (desde el interior o de forma remota) antes de entrar en la partición protegida. Si se intenta entrar en la partición, se activará una alarma instantánea sin retardo de entrada.

Modo perimetral instantáneo nocturno

Las zonas de entrada/salida estarán activas con el periodo de retardo de entrada eliminado, se anularán las zonas con la opción de modo Perimetral y las zonas con la opción de modo Nocturno estarán activas. La entrada a través de una zona con la opción de entrada/salida activará una alarma instantánea.

Al igual que el Modo Perimetral instantáneo, el Modo Nocturno requiere que se desarme el sistema (desde el interior o de forma remota) antes de entrar en la partición protegida. Al cambiar al modo Nocturno, las zonas en modo Perimetral permanecen anuladas (por ejemplo, el dormitorio) mientras las zonas de modo Nocturno se activan (por ejemplo, el vestíbulo). El Modo Nocturno es un tercer modo de armado que proporciona mayor seguridad y que normalmente se utiliza cuando se permanece en la planta superior y no se espera que haya nadie en la planta inferior.

Control de varias particiones

Si su sistema tiene habilitado el control de varias particiones y el usuario tiene activada la opción Mostrar lista de particiones, se mostrará la pantalla de selección de Partición, por ejemplo:

La línea superior contiene la lista de particiones disponibles que se pueden seleccionar.

La línea inferior representa el estado de partición. Para obtener más información, consulte “Estatus de partición” más adelante.

Para controlar un sistema xGen, utilice el cursor a fin de seleccionar particiones o anular su selección.

Para seleccionar una partición, use los botones de navegación Derecha (6) e Izquierda (4) para mover el cursor. Seleccione o anule la selección de una partición con el botón Selección (5). Los números de partición seleccionados están invertidos. Pulse Enter para confirmar la selección.

La pantalla puede mostrar hasta 8 particiones. Si hay más de 8 particiones, utilice los botones de navegación Abajo (8) y Arriba (2) para ver las 8 particiones siguientes o anteriores.

Para controlar un sistema xGenConnect, utilice los botones numéricos del 1 al 8 a fin de seleccionar las particiones del 1 al 8 o anular su selección.

Para seleccionar una partición, pulse el número de partición. Los números de partición seleccionados están invertidos. Pulse Enter para confirmar la selección.

Pulse 0 para seleccionar todas las particiones disponibles o anular su selección.

Estatus de partición

Los siguientes estados de partición pueden aparecer en pantalla:

✓: la partición está lista para el armado.

✓ (parpadeo): la partición está lista para forzar el armado.

–: la partición no está lista para el armado (por ejemplo, una zona está activa o hay un fallo).

: la partición está armada en el modo Total.

: la partición está armada en el modo Perimetral.

(parpadeo): la partición está armada en el modo Perimetral instantáneo.

: la partición está armada en el modo Perimetral instantáneo nocturno.

Nota: el número de partición de la línea superior parpadea si se ha producido una alarma u otro evento audible en la partición correspondiente.

Eventos del sistema que impiden el armado

Los siguientes eventos del sistema pueden impedirle armar el sistema de seguridad. En función del grado de seguridad, o bien usted o la compañía que llevó a cabo su instalación deberán confirmar estos eventos o fallos antes de poder armar el sistema. Consulte el siguiente capítulo o póngase en contacto con su compañía de instalación para obtener ayuda al respecto.

- Fallos de supervisión del sensor inalámbrico
- Sensor inalámbrico con batería baja
- Tamper
- Problema
- Fallo de Ethernet o wifi
- Interferencias inalámbricas
- Fallo de sobrecorriente
- Fallo de red de CA
- Fallo de batería de respaldo
- Fallo de expansor

Error de salida / Fallo al cerrar

Si durante el retardo de salida se dispara una zona instantánea, las particiones afectadas no se armarán y las sirenas emitirán una advertencia. Se registrarán un Error de salida y un Fallo al cerrar en el historial de eventos de xGen.

Compruebe que la zona sea segura e intente armar de nuevo las particiones.

Desarmar particiones

Introduzca un código válido para desbloquear la pantalla.

Normalmente oirá un sonido (un tono continuo) para anunciar el retardo de entrada.

Pulse el botón Desarmar (Figura 1, elemento 7) seguido de un código PIN válido para desarmar su sistema.

Si su sistema tiene habilitado el control de varias particiones y el usuario tiene activada la opción Mostrar lista de particiones, se mostrará la pantalla de selección de Partición. Consulte “Control de varias particiones” más atrás.

Habrá que introducir un código válido para determinar qué permisos se tienen. Esto incluye las particiones a las que puede acceder el usuario y las horas o los días que puede hacerlo.

Desarmar después de una alarma

Cuando se produzca una condición de alarma, la pantalla podría emitir un pitido constante.

Introduzca un código válido para desbloquear la pantalla.

Para obtener más detalles, pulse Información del sistema (Figura 1, elemento 6). Aparecerá la partición y la zona en la que se ha producido la alarma.

Pulse Desarmar para confirmar la condición de alarma y desarmar las particiones.

Nota: de forma predeterminada, solo las particiones en alarma están desarmadas. Para desarmar las particiones restantes, vuelva a realizar la secuencia de desarmado. Si el sistema se ha configurado para mostrar primero la lista de particiones, seleccione las particiones para desarmarlas manualmente. Consulte “Control de varias particiones” en la página 3 para obtener información.

Bloqueo al tercer intento de introducción del PIN no válido

Si se introduce un código PIN incorrecto tres veces, el teclado ignorará todos los intentos de inicio de sesión durante 90 segundos. Se tendrán en cuenta los intentos de introducir un código desde el teclado, aplicación o página web. Deberá esperar 90 segundos antes de poder volver a intentar introducir el código PIN. De esta manera, se evitan intentos de adivinar los códigos PIN por la fuerza.

Bloqueo al décimo intento de presentación de tarjeta no válido

Si se presenta una tarjeta incorrecta al lector 10 veces (por ejemplo, si presenta un formato incorrecto, no está protegida, no se ha asignado a ningún usuario o está desactivada), el teclado omite los demás pases de tarjeta durante los siguientes 90 segundos. Debe esperar este tiempo antes de intentarlo de nuevo con las tarjetas correctas.

Botones de función

Hay cuatro botones de función, de la A a la D (consulte la Figura 1, elemento 5).

Cada botón se puede asignar a una de las siguientes funciones programables:

- Conmutación de chivato rápido (asignada al botón C de manera predeterminada).
- Anulación rápida (asignada al botón B de manera predeterminada).
- Activar escena.
- Restablecimiento de detector de humo

Pulsar brevemente el botón iniciará la función.

Si se ha programado, mantener pulsado el botón durante 2 segundos generará una de las siguientes alarmas de emergencia:

- A: Alarma de incendio
- B: Alarma médica
- C: Alarma de pánico

Alarmas de emergencia

Las alarmas de pánico, médicas y de incendio deben estar habilitadas en las opciones de partición.

Mantenga pulsado el botón de función correspondiente durante 2 segundos para activar la alarma de emergencia.

Conmutación de chivato rápido

El botón activa o desactiva el chivato del teclado.

```
Chivato rápido ON
```

Una zona con chivato activado hará que el teclado emita un sonido de timbre cuando se active el sensor. El botón C está habilitado de manera predeterminada como Chivato rápido.

Anulación rápida

Si la partición no se puede armar porque una zona no está lista, pulse Información del sistema (***i***) para mostrar las zonas que no están listas.

```
Zona no lista
12-Ventana delantera
```

Desplácese por la lista de zonas y pulse el botón Anulación rápida (por defecto, el botón B) en cada zona que aparezca que deba quedar anulada. Pulse Anulación rápida de nuevo para anular la zona mostrada.

Pulse Cancelar para salir.

Edición de texto

Al editar texto o introducir un código PIN, estarán disponibles los siguientes botones:

- Botones de función:

  - A: modo cursor. Pulse A y, a continuación, Izquierda o Derecha para mover el cursor. Pulse A nuevamente para regresar al modo de escritura de caracteres.
  - B: retroceso.
  - D: borrar.

- Botones numéricos: los botones del 1 al 9 tienen caracteres alfabéticos. Para escribir una letra, pulse la tecla el número de veces necesarias hasta llegar a la posición de la letra. Además de las letras mayúsculas y minúsculas, estarán disponibles valores numéricos y espacios.
- Entrar: confirmar cambios.
- Cancelar: desechar cambios y salir.

Nota: utilice los botones numéricos 1 y 2 y el botón funcional C para insertar caracteres especiales. Pulse varias veces para seleccionar un carácter especial y añadirlo al texto.

Navegación por el menú principal

Para entrar al usuario o al menú de programación, según los privilegios del usuario, pulse Entrar, introduzca su PIN y, a continuación, vuelva a pulsar Entrar.

La línea superior de la pantalla LCD mostrará el menú actual.

La línea inferior le permitirá seleccionar un submenú o cambiar el valor de la opción, por ejemplo:

```
Seguridad
Zonas
```

```
Zonas
Entrada principal
```

Use los botones Arriba (2) y Abajo (8) para navegar por el menú y cambiar los valores de las opciones. Use Entrar para confirmar y Cancelar para salir. Consulte también “Edición de texto” más atrás.

Los siguientes menús de usuarios y operaciones estarán disponibles.

Seguridad

Existen los siguientes menús:

- Particiones: este menú le permite ver y controlar cada partición del sistema de seguridad y activar/desactivar el modo Chivato en una partición.
- Zonas: este menú permite ver los estados de las zonas, anular las zonas y activar/desactivar el Chivato de las zonas.
- Puertas: si el panel admite la función de acceso a puertas, estará disponible el menú Puertas. Este permite ver el estado de las puertas, además de controlarlas (desbloquear, desactivar, etc.).
- Restablecer el detector de humo: Esta función restaura los detectores de humo conectados al sistema de seguridad xGen. Es preciso realizar una restauración después de cada alarma de incendio o fallo.

Al visualizar las particiones, las zonas y las puertas, utilice los botones Arriba (2) y Abajo (8) para seleccionar la zona o la partición específica. Use los botones Izquierda (4) y Derecha (6) para aplicar uno de los siguientes filtros de estado:

- Todo
- Off normal
- No listo
- Anulado
- Chivato habilitado
- Armado total
- Armado parcial
- En alarma
- En tamper
- En problema

Controles

Acción: consulte y active las acciones.

Histórico

Este menú da acceso al registro de eventos de xGen. El registro de eventos mostrará primero el evento más reciente.

La categoría de registro se puede seleccionar al acceder al menú.

Use los botones Arriba (2) y Abajo (8) para que aparezcan en la lista eventos más antiguos. Use el botón Derecha (4) para ver más detalles sobre el evento seleccionado.

Usuarios

Existen los siguientes menús:

- Añadir/Modificar: Añadir o modificar un usuario existente.

  Se pueden modificar los siguientes detalles de usuario:

  - Nombre, apellidos
  - PIN
  - Tipo de usuario (estándar / coacción / solo armar / personalizado / master)
  - Idioma
  - Mostrar lista de particiones (activar / desactivar)
  - Grupo de particiones
  - Grupo de puertas
  - Invalidar tipo de partición (activar / desactivar)
  - Perfiles 1 a 4 (0: deshabilitado / 1: todas las particiones / 2: partición N, etc.)
  - Horarios 1 a 4 (0: deshabilitado / 1: horario N, etc.)
  - Fecha de inicio, fecha de finalización: el tiempo de usuario activo.

  Nota: los grupos de particiones y puertas solo están disponibles si la versión del panel admite las funciones de acceso a puertas.
- Ver: consultar los detalles de un usuario existente.
- Borrar: eliminar un usuario del sistema.
- Copiar: copiar los usuarios existentes a otros nuevos.

  Establezca los siguientes parámetros: copiar desde el número de usuario, copiar al número de usuario, total de usuarios para copiar.
- Buscar por PIN: introduzca un PIN para buscar al usuario. Si se encuentra el PIN, pasará al menú Añadir/Modificar del usuario.

Nota: Solo el usuario maestro tiene acceso a las opciones enumeradas anteriormente. Los usuarios estándar solo pueden cambiar su propio PIN y el idioma.

Prueba

Están disponibles las siguientes pruebas:

- Sirena
- Batería
- Comunicador
- Test de paseo de zona
- Prueba automática

Hora

Asegúrese de que el sistema tenga acceso a Internet para la actualización automática de la hora y la fecha o configure el reloj manualmente desde un teclado.

Existen los siguientes menús:

- Fecha y hora: establezca la fecha y la hora.
- Festivo: ver y programar los festivos.

Configuración

Existen los siguientes menús:

- Teclado: ajuste la siguiente configuración del teclado:

  - Pantalla: contraste, brillo, brillo inactivo, color.
  - Retroiluminación de las teclas: brillo, brillo inactivo, color.
  - Sonido: tono, volumen de pulsación de teclas, volumen de alarma, volumen de entrada y salida.
  - Temporizador de inactividad
  - Formato 24 h (Sí / No)
  - Mostrar logotipo (Sí / No)
  - Mostrar reloj (Sí / No)
- Etiquetas: consulte y edite los nombres de particiones, zonas y salidas.
- Elaboración de informes: consulte y edite las direcciones de correo electrónico para la elaboración de informes.
- Estado: consulte la conexión y el estado del dispositivo.

  - Estado de conexión: Estado de LAN, Ruta IP, Estado móvil, Estado UltraSync, UltraSyncPath, Servicio móvil, Intensidad de la señal de la comunicación móvil, ID de operador, Tecnología de radio, SIM activa, Estado de wifi, SSID de wifi, ID único de dispositivo (UID).

  - Detalles del panel

Realización de funciones adicionales

Anular y cancelar la anulación de las zonas

El menú de zona anulada permite anular (aislar) las zonas seleccionadas en el sistema de seguridad. Una zona anulada no puede activar una alarma, ya que se ha desactivado temporalmente en el sistema.

Esta opción suele utilizarse para anular zonas que desee añadir de forma temporal al modo Perimetral. Aunque aún se ofrece protección en las zonas restantes, la anulación de zonas reduce el nivel de seguridad. Todas las zonas anuladas se restablecerán y se desanularán cuando el sistema se desarme la próxima vez. Este debe desarmarse (desactivarse) antes de poder anular zonas. Después de anular las zonas seleccionadas, el sistema de seguridad debe armarse (activarse) en el modo Total o Perimetral para proteger las zonas restantes.

1. Introduzca un PIN válido para desbloquear el protector de pantalla.
2. Pulse Entrar.
3. Vaya a Seguridad > Zonas.
4. Seleccione la zona que desee anular. Use los botones Izquierda (4) y Derecha (6) para aplicar un filtro, si fuera necesario. Para obtener más información, consulte “Seguridad” en la página 5.
5. Pulse Entrar para ver la lista de casillas de verificación de conmutación disponibles. La primera es Anular.

   Pulse Entrar de nuevo para activar y desactivar el modo de anulación.
6. Pulse Cancelar para salir del menú.

De manera alternativa, puede usar la función Anulación rápida. Para obtener más información, consulte “Anulación rápida” en la página 4.

Configurar el modo Chivato

Puede configurar el teclado para que suene un timbre cuando las áreas seleccionadas se disparen o activen; esto se denomina chivato.

El modo Chivato se puede activar o desactivar para cada partición y no activa alarmas. En este caso solo se utiliza como alerta de bajo nivel, como el timbre de entrada del cliente.

Nota: La función Chivato en una zona requiere que tanto la zona como su partición tengan habilitado el chivato.

Puede habilitar o deshabilitar fácilmente el chivato a nivel de partición con la función Chivato rápido. Para obtener más información, consulte “Conmutación de chivato rápido” en la página 4.

1. Introduzca un PIN válido para desbloquear el protector de pantalla.
2. Pulse Entrar.
3. Vaya a Particiones o Zonas.
4. Seleccione la partición que desea añadir al modo chivato.
5. Pulse Seleccionar (5).
6. Pulse Cancelar para salir del menú.

Programar PIN de usuario

Cada usuario tiene un código PIN único que le permite acceder a varias funciones del sistema. Solo los usuarios con un nivel de autoridad maestro podrán añadir, modificar y eliminar usuarios.

1. Introduzca un código PIN válido para desbloquear el protector de pantalla.
2. Pulse Entrar.
3. Vaya a Usuarios.
4. Seleccione la función que desee realizar:

   - Añadir/modificar: añadir o editar un PIN y los permisos de usuarios.
   - Ver: consultar los detalles y el PIN de un usuario existente.
   - Borrar: borrar un usuario.
   - Estado: consultar el estado de un usuario existente.
   - Copiar: duplicar usuarios existentes.
5. Seleccione el usuario.
6. Siga las instrucciones que aparecen en la pantalla.

Cambio de la fecha y la hora, y de las fechas de festivos

1. Introduzca un PIN válido para desbloquear el protector de pantalla.
2. Pulse Entrar.
3. Seleccione la función que desee realizar:

   - Fecha y hora: cambiar la hora actual.

   - Festivo: cambiar las fechas de los cuatro (4) grupos de festivos.
4. Siga las instrucciones que aparecen en la pantalla.

Lectura del registro de eventos

El sistema conserva un registro de los eventos que se han producido. Se puede acceder al registro de eventos a través del teclado.

1. Introduzca un código PIN válido para desbloquear el protector de pantalla.
2. Pulse Entrar.
3. Vaya a Historial.
4. Seleccione la categoría de registro que desee visualizar. En función de la versión del panel, pueden estar disponibles las siguientes categorías:

   - Principal: todos los eventos, excepto los eventos relacionados con las tarjetas y las puertas que se produzcan frecuentemente.

   - Alarma: eventos relacionados con la intrusión y las alarmas, según la norma EN 50131.

   - Vídeo: eventos relacionados con la cámara.

   - Acceso: eventos relacionados con las tarjetas y las puertas. Disponible solo si el panel admite funciones de acceso a puertas.

Use los botones Arriba (2) y Abajo (8) para que aparezcan en la lista los eventos. Use el botón Derecha (4) para ver más detalles sobre el evento seleccionado. Consulte también “Histórico” en la página 5.

Funciones de prueba

Realizar periódicamente pruebas en el sistema de seguridad es fundamental para garantizar un correcto funcionamiento y el envío de los mensajes de alarma en caso de una detección de alarma.

1. Introduzca un PIN válido para desbloquear el protector de pantalla.
2. Pulse Entrar.
3. Vaya a Probando.
4. Seleccione el componente de seguridad que desee probar:

   - Sirena: probar las funciones de sirena. Las sirenas interiores y exteriores se activarán durante el tiempo configurado. Pulse Cancelar para cancelar la prueba de sirena.

   - Batería: probar la batería por si puede proporcionar alimentación auxiliar. La duración de la prueba es automática. Puede tardar unos minutos en mostrar el resultado.

   - Prueba de comunicador: probar si el sistema es capaz de enviar mensajes de alarma. El resultado aparecerá en unos pocos segundos.

   - Prueba de andado de zona: verificar que todos los sensores son capaces de enviar señales de alarma al sistema. Debe especificar el rango de zonas (como zona inicial y final) para realizar la prueba. El procedimiento de prueba muestra la lista de zonas que se están probando. La activación de zonas concretas las elimina de la lista hasta que la lista esté vacía, lo que significa que se ha pasado la prueba. La prueba fallará si todavía hay zonas sin probar después del tiempo configurado en el panel.

   - Prueba automática: probar la pantalla del teclado, los indicadores, la retroiluminación de las teclas y el dispositivo sonoro.
5. Siga las instrucciones que aparecen en pantalla para realizar la prueba.

Configuración de las opciones del teclado

Los teclados se pueden personalizar en función de los requisitos del sitio configurando el volumen, el brillo y el tiempo que tarda en aparecer el protector de pantalla.

1. Introduzca un PIN válido para desbloquear el protector de pantalla.
2. Pulse Entrar.
3. Vaya a Configuración > Teclado.
4. Seleccione el parámetro que desee personalizar:

   - Pantalla: contraste, brillo, brillo inactivo, color.
   - Retroiluminación de las teclas: brillo, brillo inactivo, color.
   - Sonido: tono, volumen de pulsación de teclas, volumen de alarma, volumen de entrada y salida.
   - Temporizador de inactividad
   - Formato 24 h (Sí / No)
   - Mostrar logotipo (Sí / No)
   - Mostrar reloj (Sí / No)

Programación de tarjetas

Si el teclado está equipado con un lector de tarjetas Mifare (NXG-1832-EUR y NXG-1833-EUR) y el sistema admite funciones de acceso a puertas, el usuario maestro puede configurar las tarjetas de usuario en el menú "Tarjetas de usuario".

Nota: el menú permite añadir o modificar tarjetas de los usuarios existentes.

Para modificar una tarjeta de usuario:

1. Introduzca un código PIN válido para desbloquear el protector de pantalla.
2. Pulse Entrar.
3. Vaya a Tarjetas de usuario.
4. Seleccione la función que desee realizar.

Añadir/modificar tarjeta

Añada o edite la tarjeta para el usuario.

Seleccione primero un usuario. Para ello, introduzca el ID de usuario y confírmelo pulsando la tecla ENTER.

En la pantalla, se muestra "Pase tarjeta o escriba ID".

Puede cambiar o introducir el número de tarjeta en el teclado o pasar la tarjeta (este es el método recomendado).

Si se pasa la tarjeta, se protegerá automáticamente si es necesario; la clave de seguridad se aplicará a la tarjeta.

Nota: presente la tarjeta en el lector y sosténgala hasta que el teclado emita un pitido. Si se requiere la operación de protección, la aplicación de la clave de seguridad en la tarjeta puede tardar de 1 a 2 segundos en completarse.

Si protege la tarjeta correctamente, se genera un sonido especial de dos tonos.

Si se introduce el número de tarjeta en el teclado, la tarjeta debe protegerse manualmente (por ejemplo, mediante la opción de protección de tarjetas).

Hab./Deshabilitar tarjeta

Permite activar o desactivar la tarjeta, que ya se ha asignado al usuario.

Seleccione primero el usuario. Para ello, introduzca el ID de usuario y confírmelo pulsando la tecla ENTER.

También puede pasar una tarjeta de usuario para seleccionar su usuario.

A continuación, cambie el parámetro Habilitar como desee.

Borrar tarjeta

Seleccione primero el usuario. Para ello, introduzca el ID de usuario.

También puede pasar una tarjeta de usuario para seleccionar su usuario.

Una vez que se haya seleccionado el usuario, se eliminará la tarjeta asignada al usuario.

Añadir múltiples tarjetas

Esta opción permite asignar tarjetas a varios usuarios existentes.

Nota: este es el método recomendado y más fácil para añadir tarjetas a los usuarios en la configuración inicial del sistema.

Se deben crear primero todas las cuentas de usuario mediante el método correspondiente (DLX900 / página web / menús de usuarios).

Acceda a la opción Añadir múltiples tarjetas en un teclado NXG-1832 / NXG-1833 como usuario maestro.

En el teclado, se muestra la lista de usuarios sin una tarjeta asignada. Si ya se han asignado tarjetas a todos los usuarios, se muestra el mensaje correspondiente.

Solo se muestra un usuario cada vez, empezando por el ID de usuario más bajo. Se pueden seleccionar usuarios mediante los botones Arriba y Abajo.

Una vez que se muestre el número de usuario en la pantalla, presente la tarjeta en el lector. Esto ejecuta las siguientes operaciones: asignar la tarjeta al usuario y activar y proteger la tarjeta.

Nota: presente la tarjeta en el lector y sosténgala hasta que el teclado emita un pitido. Si se requiere la operación de protección, la aplicación de la clave de seguridad en la tarjeta puede tardar de 1 a 2 segundos en completarse.

Si protege la tarjeta correctamente, se genera un sonido especial de dos tonos.

Tras la asignación correcta, el usuario se elimina de la lista de usuarios y el teclado cambia automáticamente al siguiente usuario sin tarjeta asignada o muestra el mensaje "TodosUsuar.ConTarjeta".

Tarjetas seguras (información de la tarjeta)

Esta opción permite proteger varias tarjetas. Además, se puede utilizar como opción de "Información de la tarjeta".

Es recomendable (aunque no obligatorio) realizar la operación de protección en todas las tarjetas de repuesto que no se utilicen en la configuración inicial de tarjetas. Esto permitirá asignar estas tarjetas a nuevos usuarios en el futuro mediante la introducción del ID de tarjeta sin necesidad de pasar la tarjeta en el lector.

Una vez introducido, el menú muestra el mensaje "Pasar tarjeta". Cualquier tarjeta que se pase cuando la función esté activa quedará protegida y se mostrará el mensaje pertinente durante unos segundos.

Nota: el menú Tarjetas seguras también se puede utilizar para obtener información sobre las tarjetas. Puede presentar tarjetas ya protegidas o asignadas a usuarios. En la pantalla del teclado, se mostrará el mensaje de que la tarjeta ya está protegida y aparecerá el ID de usuario y el estado de activación.

Mensajes de estado del sistema

Puede que aparezcan varios mensajes sobre el estado de la pantalla del teclado.

Alarmas

Pueden aparecer las siguientes alarmas:

- Alarma de pánico
- Alarma médica
- Alarma de robo (en este caso solo se muestra el nombre de la zona).
- Alarma de incendio

Si hay alarmas, no se mostrarán otros mensajes de estado en la pantalla de estado del sistema. Pulse el botón Información del sistema (***i***) para ver las alarmas.

- Zona en alarma, número de zona y nombre
- SOS – Alarma de incendio
- SOS – Alarma de pánico
- SOS – Alarma médica

Si se activa una alarma manual con los botones de función del teclado (A, B, C), no se mostrará información de la zona.

Las categorías distintas a las alarmas se pueden visualizar de manera alternativa.

Fallos

Pueden aparecer los siguientes fallos:

- Pérdida de hora: es necesario restablecer la fecha y la hora del sistema de seguridad. Asegúrese de que el sistema tenga acceso a Internet para la actualización automática de la hora o para configurar el reloj manualmente desde un teclado.
- Fallo alim. CA: el sistema de seguridad ha perdido la alimentación eléctrica. Compruebe si hay suministro eléctrico en el resto del edificio, restablezca el interruptor de potencia si fuera necesario y póngase en contacto con el proveedor del servicio en caso de que no se restablezca el suministro eléctrico.
- Batería baja del sistema: la batería de reserva del sistema de seguridad necesita carga. Espere 24 horas. Si no se soluciona el problema, póngase en contacto con el proveedor del servicio.
- Tamper de caja del sistema: se ha activado la entrada del tamper de la caja del sistema de seguridad. Compruebe si la tapa está bien cerrada.
- Problema de sirena del sistema: hay un problema con la sirena interna del sistema de seguridad. Póngase en contacto con el proveedor del servicio.
- Sobrecorriente del sistema: el sistema de seguridad o una fuente de alimentación inteligente consumen demasiada energía. Póngase en contacto con el proveedor del servicio.
- Fallo de línea telefónica, Fallo de línea de Ethernet en el sistema, Fallo de enlace inalámbrico: el sistema de seguridad ha detectado un problema con una línea de comunicaciones. Compruebe la conexión a Internet y póngase en contacto con el proveedor del servicio si el problema no se soluciona.
- Fallo de comunicación telefónica, Fallo de comunicación de Ethernet, Fallo de comunicación inalámbrica: el

sistema no pudo informar de un mensaje por un canal de comunicación. Póngase en contacto con el proveedor del servicio.

- Dispositivo del sistema sin conexión, Dispositivo del sistema anulado: se ha desconectado o anulado un expansor o un teclado.
- Interferencia inalámbrica del sistema: se ha detectado una interferencia de dispositivo inalámbrico. Póngase en contacto con el proveedor del servicio.
- Fallo de la fuente de alimentación del sistema: una fuente de alimentación inteligente tiene un problema de hardware. Póngase en contacto con su proveedor de servicios para obtener un repuesto.
- Zona en tamper: en esta zona se ha activado una alarma de tamper.
- Zona en problema: esta zona tiene un circuito abierto.
- Batería baja en zona: esta zona es un dispositivo inalámbrico y hay que cambiar su batería.
- Zona perdida: esta zona es un dispositivo inalámbrico que no se comunica.
- Antienmascaramiento en la zona: esta zona es un detector y se ha enmascarado.
- Zona de partición en tamper: se ha restaurado un tamper de zona en la partición.
- Zona de partición en problema: se ha restaurado un cortocircuito de zona en la partición.
- Zona de partición con batería baja: se ha restaurado una alarma de batería baja en la zona.
- Zona de partición perdida: se ha restaurado una alarma de zona perdida en la partición.

La segunda línea del mensaje de fallo contiene un número de zona y el nombre de la zona defectuosa, o el nombre de un dispositivo en el caso de que se produzcan fallos del sistema.

Fallos de puerta

Pueden aparecer los siguientes fallos de puerta en la pantalla:

- Puerta abierta (DLO): La puerta sigue abierta cuando el temporizador de desviación de la zona de la puerta ha expirado, y la puerta está configurada para informar del estado DLO.
- Advertencia de la puerta: la puerta sigue abierta durante el tiempo de advertencia de la zona de la puerta antes de que finalice el temporizador de desviación de la zona de la puerta y esta se ha configurado para informar del estado DLO.

  Ejemplo

  Si la derivación de la zona de la puerta se ha establecido en 60 segundos, la advertencia de la zona de la puerta se ha establecido en 15 segundos y la puerta se mantiene abierta:

  - El mensaje de advertencia de la puerta aparece 45 segundos después de abrir la puerta.
  - El mensaje Puerta dejada abierta aparece 60 segundos después de abrir la puerta (ya no se informa de la advertencia de la puerta).

  Nota: si la advertencia de la puerta está activa en las puertas asignadas a un determinado teclado, este genera un sonido especial (1 segundo encendido, 1 segundo apagado) para notificar al usuario que esta puerta se encuentra en estado de advertencia y que pronto activará la alarma DLO.
- Puerta forzada: la puerta se ha abierto a la fuerza (el bloqueo de la puerta sigue activado) y se ha configurado para informar de la condición de Puerta forzada.

En programación

Indica que se está programando el sistema. Pulse el botón Información del sistema (***i***) para visualizar los detalles del modo de programación:

- Modo de programación: el sistema se está programando desde otro teclado.
- Programación remota: el sistema se está programando de forma remota utilizando el software o la página web.

Zona anulada

Indica que una zona está anulada, ya sea de forma manual por un usuario o automática durante el armado perimetral. Pulse el botón Información del sistema (***i***) para mostrar más detalles:

- Zona en anulación | Número y nombre de zona
- Zona anulada automáticamente | Número y nombre de zona

Sistema no Listo

Una zona está en estado activo. Pulse el botón Información del sistema (***i***) para mostrar el número y el nombre de la zona activa.

Zonas, listas abiertas

El estado se muestra si una zona está en estado activo pero su partición está configurada para el armado forzado, por lo que se anulará automáticamente la zona activa al armarse. Pulse el botón Información del sistema (***i***) para mostrar el número y el nombre de la zona activa.

Consulte también “Zona anulada” más atrás.

Armado perimetral y armado total

Se pueden mostrar los siguientes estados armados:

- Armado perimetral, armado total: se ha armado una sola partición.
- Armado perimetral: X/Y, Armado total: X/Y: X de Y particiones están armadas.

Pulse el botón Información del sistema (***i***) para mostrar una lista de particiones con sus estados actuales. Consulte “Estatus de partición” en la página 3 para obtener información detallada sobre los estados de partición.

Sistema Listo

El sistema está listo para el armado.

Programación

Para la programación completa del sistema, consulte *Guía de instalación y programación de xGenConnect*.

Especificaciones

Compatibilidad	Serie de paneles xGenConnect
Combinaciones de código	De 10 000 a 100 000 000 (4 a 8 dígitos) No existen combinaciones de código no válidas.
Tensión	De 9 a 15 V CC (proporcionados por el panel)
Consumo de corriente (a 13,7 V CC):	
Nominal	NXG-1830-EUR, NXG-1831-EUR: 90 mA NXG-1832-EUR, NXG-1833-EUR: 130 mA
Mínimo (todas las luces apagadas)	NXG-1830-EUR, NXG-1831-EUR: 35 mA NXG-1832-EUR, NXG-1833-EUR: 40 mA
Máximo	NXG-1830-EUR, NXG-1831-EUR: 160 mA NXG-1832-EUR, NXG-1833-EUR: 200 mA
Entrada	Resistivo, Cableado compatible con entradas del panel xGenConnect
Salida	Solo NXG-1832-EUR y NXG-1833-EUR Tipo de colector abierto Pullup interno de 10 kΩ a la línea PWR principal
Carga máx. para colector abierto	100 mA
Tensión máx. conectada externamente	16 V CC
Protección contra la sobrecarga	Integrada
Lector Mifare	Solo NXG-1832-EUR y NXG-1833-EUR
Frecuencia portadora	13,560 MHz
Ancho de banda	1,696 MHz
Salida máxima de alimentación	42 dBµA/m
Tarjetas compatibles	NXG-180x-5 (compatible con Mifare DESFire EV2, EV3)
Conexiones	Bus de 4 hilos xGen
Altura de montaje	≤2 m
Dimensiones (An × Al × Pro)	133 x 130 x 25 mm
Color	NXG-1830-EUR, NXG-1832-EUR: Blanco NXG-1831-EUR, NXG-1833-EUR: Antracita
Peso	0,3 kg
Temperatura de funcionamiento	De −10 a +50°C
Humedad relativa máxima	95 % sin condensación
Partes reparables	No hay partes reparables

Información normativa

Fabricante	COLOCADO EN EL MERCADO POR: Carrier Fire & Security Americas Corporation Inc. 13995 Pasteur Blvd Palm Beach Gardens, FL 33418, EE. UU. REPRESENTANTE AUTORIZADO DE LA UE: Carrier Fire & Security B.V. Kelvinstraat 7, 6003 DH Weert, Países Bajos
Advertencias de productos y exenciones	ESTOS PRODUCTOS SE HAN DISEÑADO PARA SU VENTA E INSTALACIÓN POR PARTE DE PROFESIONALES CUALIFICADOS. CARRIER FIRE & SECURITY NO PUEDE OFRECER NINGUNA GARANTÍA DE QUE CUALQUIER PERSONA O ENTIDAD QUE COMPRE SUS PRODUCTOS, INCLUIDO CUALQUIER “DISTRIBUIDOR AUTORIZADO” O “VENDEDOR AUTORIZADO” CUENTEN CON LA FORMACIÓN O LA EXPERIENCIA ADECUADAS PARA INSTALAR CORRECTAMENTE LOS PRODUCTOS RELACIONADOS CON INCENDIOS Y SEGURIDAD. Para obtener más información sobre las exclusiones de garantía e información de seguridad de productos, consulte https://firesecurityproducts.com/policy/product-warning/ o escanee el código QR.
	CE
Certificación	EN 50131-3 Grado de seguridad 2, Clase medioambiental II. Probado y certificado por Telefication B.V.
Directivas de la Unión Europea	NXG-1830-EUR, NXG-1831-EUR: Por el presente documento, Carrier Fire & Security declara que este dispositivo cumple con los requisitos y disposiciones aplicables de las Directivas 2014/30/UE y/o 2014/35/UE. Para obtener más información, consulte www.firesecurityproducts.com/en/page/caddx
	NXG-1832-EUR, NXG-1833-EUR: Carrier Fire & Security por la presente declara que este aparato cumple los requisitos y disposiciones aplicables de todas las reglas y regulaciones, lo que incluye sin carácter limitativo la directiva 2014/53/UE. Para obtener más información, consulte www.firesecurityproducts.com/en/page/caddx
REACH	Los productos REACH pueden contener sustancias que están incluidas en la Lista de sustancias Candidatas en una concentración en peso superior al 0,1%, según la más reciente Lista de sustancias Candidatas publicada en la Web de ECHA. Puede encontrar información sobre su uso seguro en https://firesecurityproducts.com/en/content/intrusion-intro
	2012/19/UE (directiva WEEE): Los productos marcados con este símbolo no se pueden eliminar como residuos urbanos sin clasificar en la Unión Europea. Para poder reciclarlo adecuadamente, devuelva este producto a su proveedor local al adquirir un equipo nuevo equivalente o elimínelo en los puntos de recogida designados para tal efecto. Para obtener más información, consulte recyclethis.info.

Información de contacto

www.firesecurityproducts.com/en/page/caddx

P/N 466-5559-ES • REV E • ISS 02MAY22