Manual de Usuario

ZKBioSecurity

Versión: 2.1

Fecha: Julio 2017

Versión de Software : ZKBioSecurity 3.0.5.0_R o Superior.

Información importante

Primeramente, le damos las gracias por haber adquirido este producto. Antes de usarlo, lea este manual cuidadosamente. Le recordamos que el uso adecuado mejorará la experiencia de usuario y el efecto de uso.

Sin el previo consentimiento de nuestra empresa, ningún individuo tiene permitido extraer o copiar el contenido de este manual de manera parcial o total y distribuir el contenido en cualquier formato.

El producto descrito en el manual tal vez incluye software cuyos derechos de autor son compartidos por los licenciantes incluyendo nuestra empresa. Con excepción de la autorización del titular correspondiente, ningún individuo puede copiar, distribuir, revisar, modificar, extraer, descompilar, desensamblar, descifrar, invertir la ingeniería, arrendar, transferir o sub licenciar el software ni realizar otros actos de violación de los derechos de autor, pero se excluye las limitaciones aplicadas a la ley.

Debido a la constante renovación de los productos, la empresa no puede garantizar la consistencia del producto con la información en este documento o cualquier disputa causada por la diferencia entre los parámetros técnicos actuales y la información contenida en este documento. Por favor, disculpe cualquier cambio sin previo aviso.

Contenido

Información importante i

1 Introducción del Sistema 1

1.1 Breve Introducción de Módulo de Personal 1
1.2 Breve Introducción de Módulo de Control de Acceso 1
1.3 Breve Introducción de Módulo de Elevador 2
1.4 Breve Introducción de Módulo de Hotel 2
1.5 Breve Introducción de Módulo de Visitantes 2
1.6 Breve Introducción de Módulo de Rondas 2
1.7 Breve Introducción de Módulo de Video 2
1.8 Breve Introducción de Módulo de Gestión de Sistema 2

2 Operaciones del Sistema 3

2.1 Inicio de Sesión 3
2.2 Gestión de Visitas 4
2.3 Panel del Sistema 4
2.4 Activar el Sistema 5
2.5 Modificar Contraseña 5
2.6 Soporte Técnico 6
2.7 Salir del Sistema 6

3 Usuarios del Sistema 6

3.1 Personal 7
3.1.1 Gestión de Departamentos 7
3.1.2 Personal 8
3.1.3 Atributos Personalizables 19
3.1.4 Parámetros 20
3.2 Gestión de Tarjetas 21
3.2.1 Tarjetas 21
3.2.2 Formato Wiegand 22
3.2.3 Bitácora de Tarjetas 24
3.3 Gestión de Directorio Activo 25

4 Acceso 26

4.1 Dispositivos 26
4.1.1 Dispositivos 26
4.1.2 Operaciones del Dispositivo 30
4.1.3 Puertas 37
4.1.4 Lectores 40
4.1.5 Entradas Auxiliares 41
4.1.6 Salidas Auxiliares 42
4.1.7 Tipo de Evento 43
4.1.8 Horario de Verano 44
4.1.9 Monitoreo de Dispositivos 46

4.1.10 Monitoreo en Tiempo Real 46
4.1.11 Monitoreo de Alarmas 50
4.1.12 Mapa Virtual 50
4.2 Gestión de Control de Acceso 51
4.2.1 Horarios 51
4.2.2 Días Festivos 53
4.2.3 Niveles de Acceso 54
4.2.4 Esclusamiento 55
4.2.5 Vínculos 56
4.2.6 Anti-Passback 60
4.2.7 Primera Apertura Normalmente Abierto 61
4.2.8 Grupos Multi-Usuario 61
4.2.9 Verificación Multi-Usuario 62
4.2.10 Modo de Verificación 63
4.2.11 Parámetros 63
4.3 Funciones Avanzadas de Control de Acceso 64
4.3.1 Zona 64
4.3.2 Definir Lectores 65
4.3.3 Quién Está Dentro 67
4.3.4 Anti-Passback Global 67
4.3.5 Vínculos Globales 69
4.3.6 Grupo Esclusamiento Global 70
4.3.7 Esclusamiento Global 70
4.3.8 Datos LED 71
4.4 Reportes de Acceso 72
4.4.1 Todos los Eventos 72
4.4.2 Eventos de Hoy 72
4.4.3 Última Posición Registrada 73
4.4.4 Eventos de Excepción 73
4.4.5 Privilegios de Acceso 73
4.5 Integración VMS 75
5 Elevador 76
5.1 Dispositivo de Elevador 76
5.1.1 Agregar un Dispositivo de Elevador 76
5.1.2 Lectores 78
5.1.3 Pisos 79
5.1.4 Entradas Auxiliares 80
5.1.5 Tipo de Evento 81
5.1.6 Monitoreo de Dispositivos 82
5.1.7 Monitoreo en Tiempo Real 83
5.2 Reglas de Elevador 87
5.2.1 Horarios de Elevador 87
5.2.2 Días Festivos de Elevador 89
5.2.3 Niveles de Acceso de Elevador 90

5.2.4 Vínculos Globales 92
5.2.5 Parámetros 93
5.3 Reportes de Elevador 93
5.3.1 Todos los Eventos 94
5.3.2 Eventos de Excepción 94
5.3.3 Privilegios de Acceso 94
6 Módulo de Hotel 96
6.1 Información de Hotel 96
6.2 Habitaciones 97
6.2.1 Tipos de Habitación 97
6.2.2 Edificios 98
6.2.3 Pisos 98
6.2.4 Habitaciones 98
6.2.5 Áreas 100
6.2.6 Métodos de Reserva 101
6.2.7 Control de Acceso/Elevador 101
6.3 Gestión de Tarjetas 104
6.3.1 Gestión de Tarjetas 104
6.3.2 Tarjetas para Empleados 108
6.3.3 Tarjetas de Mantenimiento 111
6.4 Gestión de Hotel 113
6.4.1 Recepción 113
6.2.4 Reservas 127
6.4.3 Gestión de Reservas 129
6.5 Reportes 131
6.5.1 Reporte de Check In de Huésped 131
6.5.2 Reporte de Check In de Habitación 131
6.5.3 Reporte de Pagos 132
6.5.4 Reporte de Emisión de Tarjetas 132
6.5.5 Reporte de Eventos de Cerradura 133
7 Módulo de Visitantes 133
7.1 Registro de Visitas 134
7.1.1 Registro de Entrada 134
7.1.2 Información de Visitantes 138
7.2 Reservación 138
7.3 Gestión Básica 139
7.3.1 Parámetros 139
7.3.2 Depuración de Equipo 141
7.3.3 Ajustes de Impresión 142
7.3.4 Niveles de Acceso de Visitantes 143
7.3.5 Lugar de Entrada 144
7.3.6 Razón de Visita 144
7.4 Reportes de Visitantes 145

7.4.1 Último Acceso Registrado 145
7.4.2 Historial de Visitas 145
7.4.3 Gráficas 145

8 Sistema de Rondas 146

8.1 Asistente de Configuración 146
8.2 Monitoreo de Rondas 146
8.3 Gestión Básica 147
8.3.1 Dispositivos 147
8.3.2 Puntos de Ronda 148
8.3.3 Parámetros 149
8.4 Gestión de Rondas 149
8.4.1 Plan 149
8.4.2 Grupos de Ronda 150
8.4.3 Rutas 151
8.5 Reportes 153
8.5.1 Todos los Eventos 153
8.5.2 Eventos de Rondas de Hoy 153
8.5.3 Estadísticas de Rutas 153
8.5.4 Estadísticas del Personal 153

9 Video 154

9.1 Dispositivo de Video 154
9.2 Canales de Video 155
9.3 Video en Tiempo Real 156
9.4 Eventos de Video 157
9.5 Parámetros 158
9.6 Solución de Excepciones 158

10 Gestión de Sistema 160

10.1 Gestión Básica 160
10.1.1 Bitácora de Eventos 160
10.1.2 Base de Datos 160
10.1.3 Áreas 162
10.1.4 Parámetros del Sistema 163
10.1.5 Correo Electrónico 163
10.1.6 Eliminar Eventos 164
10.1.7 Archivos de Audio 165
10.1.8 Tipos de Documento 165
10.1.9 Parámetros 166
10.2 Privilegios 166
10.2.1 Usuarios 166
10.2.2 Privilegios 168
10.2.3 Grupo de Privilegios 168
10.3 Comunicación 169
10.4 Gestión Extendida 170

10.4.1 Dispositivos LED 170

11 Anexos 173

11.1 Operaciones Comunes 173
11.2 Tipo de Evento de Acceso 177
11.3 Tipos de Eventos de Elevador 181
11.4 Preguntas y Respuestas 183
11.5 Acuerdo de Licencia de Software para Usuario Final 184

1 Introducción del Sistema

La gestión de seguridad se ha vuelto cada vez más importante para empresas y corporativos. El manejo y dominio de éste sistema ayuda a los usuarios a integrar las operaciones, procedimientos y elementos de seguridad en una sola plataforma. Actualmente el sistema está dividido en ocho módulos: Personal, Acceso, Elevador, Hotel, Visitantes, Rondas, Video y Sistema.

- Características del Sistema
  - Procesamiento de gran capacidad de datos, permitiendo la gestión de hasta 30,000 usuarios.
  - Gestión de privilegios multi-nivel asegura la confidencialidad de los datos.
  - Sistema de obtención de datos en tiempo real que asegura la pronta retroalimentación del administrador.
- Requerimientos de PC
  - CPU: 2 o más núcleos con velocidad de 2.4Ghz o superior.
  - Memoria: 4G o superior.
  - Hardware: Espacio disponible de 30G o superior. Es recomendado usar un disco NTFS en la partición del disco donde se instalará el software.
  - Resolución del monitor: 1024 x 768 pixeles o superior.
- Sistema Operativo
  - Sistemas operativos soportados: Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows Server 2008 (32/64).
  - Base de datos soportadas: PostgreSQL (por defecto), SQL Server y Oracle (Opcionales).
  - Navegadores recomendados: IE 11+ / Firefox 27+ / Chrome 33+.

✍Nota: Para el registro y autenticación de huella digital debe usar IE 8.0 o superior.

1.1 Breve Introducción de Módulo de Personal

Está dividido principalmente en dos partes: primero, la configuración de departamentos, en el cual se define el organigrama de la compañía. Segundo, la gestión de personal, en el cual se ingresa la información de los usuarios, se asigna los departamentos y se administra el personal.

1.2 Breve Introducción de Módulo de Control de Acceso

Es un sistema de gestión basado en web que permite configurar las funciones de control de acceso, administrar

paneles de control de acceso vía red y gestionar personal en un ambiente unificado. El sistema de control de acceso establece niveles y el horario de apertura de puerta para los usuarios registrados.

1.3 Breve Introducción de Módulo de Elevador

El módulo de control de elevador es usado para configurar los parámetros de los dispositivos y establecer privilegios de acceso al elevador y los pisos, además de supervisar los eventos de elevador. Es posible asignar privilegios de acceso a pisos específicos a los usuarios. Solo los usuarios autorizados pueden acceder a los pisos especificados en el periodo de tiempo válido después de haber sido autentificados.

1.4 Breve Introducción de Módulo de Hotel

El módulo de hotel brinda funciones para configuración de cerraduras y gestión de huéspedes como check in, check out, extensión de estadía, tarifas, entre otras.

1.5 Breve Introducción de Módulo de Visitantes

El módulo de visitantes es un sistema de gestión basado en web que implementa el registro de entrada, registro de salida, captura de imágenes, brinda estadísticas de la cantidad de visitantes y permite gestionar las reservaciones, así como compartir información entre los sitios de registro. Está integrado con el sistema de control de acceso y sistema de control de elevador, generalmente utilizado en mostradores o porterías para la recepción y administración de visitantes.

1.6 Breve Introducción de Módulo de Rondas

El módulo permite usar los dispositivos de control de acceso como puntos de rondas de vigilancia para ayudar a corporativos a supervisar y gestionar de manera efectiva al personal de vigilancia, planes y rutas. Además, es posible realizar análisis y estadísticas periódicas basados en los resultados y rutas de vigilancia.

1.7 Breve Introducción de Módulo de Video

El sistema brinda la función de vínculo de video, así como la gestión de los dispositivos, visualización de video en tiempo real, consulta de videos y pop-up de video cuando ocurre el vínculo.

1.8 Breve Introducción de Módulo de Gestión de Sistema

Utilizado principalmente para asignar usuarios del sistema y configurar las funciones de los módulos correspondientes tales como la gestión de base de datos para generar y restaurar respaldos, establecer los parámetros del sistema y administrar registros de operación del sistema.

2 Operaciones del Sistema

2.1 Inicio de Sesión

Después de instalar el software, puede dar doble clic en el ícono de ZKBioSecurity para acceder al sistema o puede abrir uno de los navegadores recomendados e introducir la dirección IP y el puerto en la barra de dirección http://127.0.0.1:8088 (por defecto).

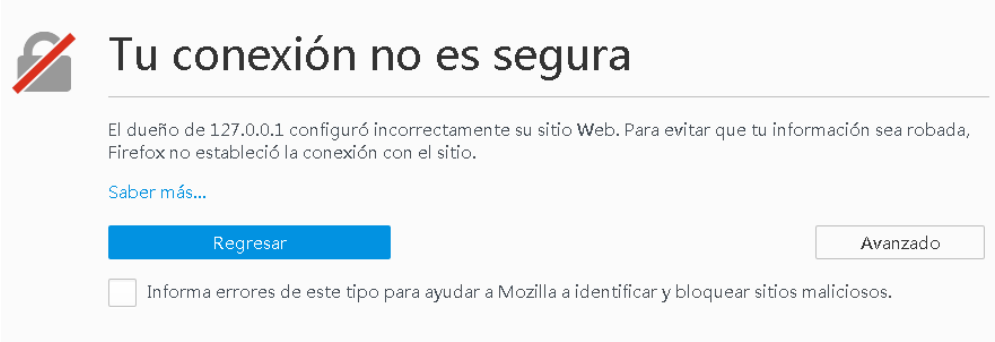
Si accede como PC cliente, introduzca la dirección IP y el puerto del servidor en la barra de dirección.

Introduzca el usuario y la contraseña y de clic en [Login], o de clic en [Huella Digital] y pulse la huella de administrador para acceder al sistema.

.✍Nota:

1. El usuario administrador por defecto es [admin] y la contraseña es [admin]. Después de acceder al sistema por primera vez, cambie la contraseña en [Información Personal].

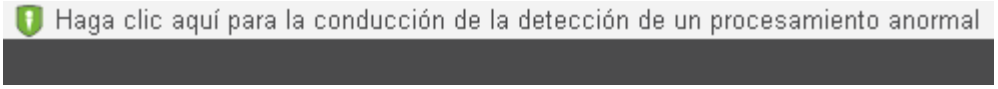
2. Si selecciona el puerto HTTPS durante la instalación del software, introduzca la dirección IP del servidor y el puerto (por ejemplo: https://127.0.0.1:8448) en la barra de dirección y presione Enter. La siguiente página puede ser mostrada:



Aquí, será necesario agregar una excepción de sitio después de que se muestra el mensaje después de presionar el

botón de Avanzado. Esta operación puede variar en los diferentes navegadores.

3. Si usted selecciona el puerto HTTPS durante la instalación del software puede mostrarse el siguiente mensaje en la página de inicio de sesión:



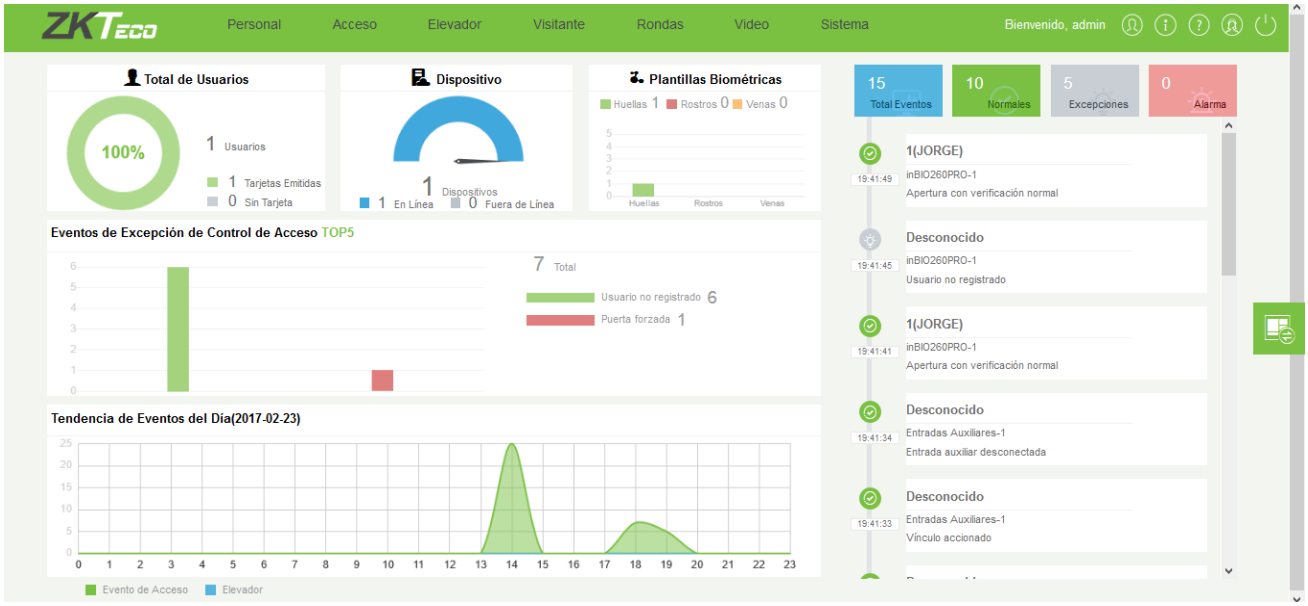
De clic en Conectar. En la página que se muestra, descargue ISSOnline.exe y los certificados correspondientes antes de usar funciones tales como huella digital y dispositivos externos.

2.2 Gestión de Visitas

De clic en [Gestión de Visitas], el personal puede generar reservaciones de visitante por sí mismos. El personal debe estar registrado en el sistema. El usuario y contraseña es el ID de usuario y la contraseña de reservación registrada en el sistema. La contraseña por defecto es 123456. Para más información sobre la gestión de visitas y reservaciones de visitantes consulte Reservación.

2.3 Panel del Sistema

Al iniciar sesión, se muestra la interfaz principal a continuación. Puede dar clic en en la esquina superior izquierda de la interfaz para regresar a la interfaz principal en cualquier momento.



Este panel le permite ver las estadísticas de cada módulo y monitorear los eventos del sistema en tiempo real. De clic en el botón en el lado derecho para cambiar a la interfaz de accesos directos.

Cada módulo contiene una lista de funciones las cuales puede acceder rápidamente dando clic.

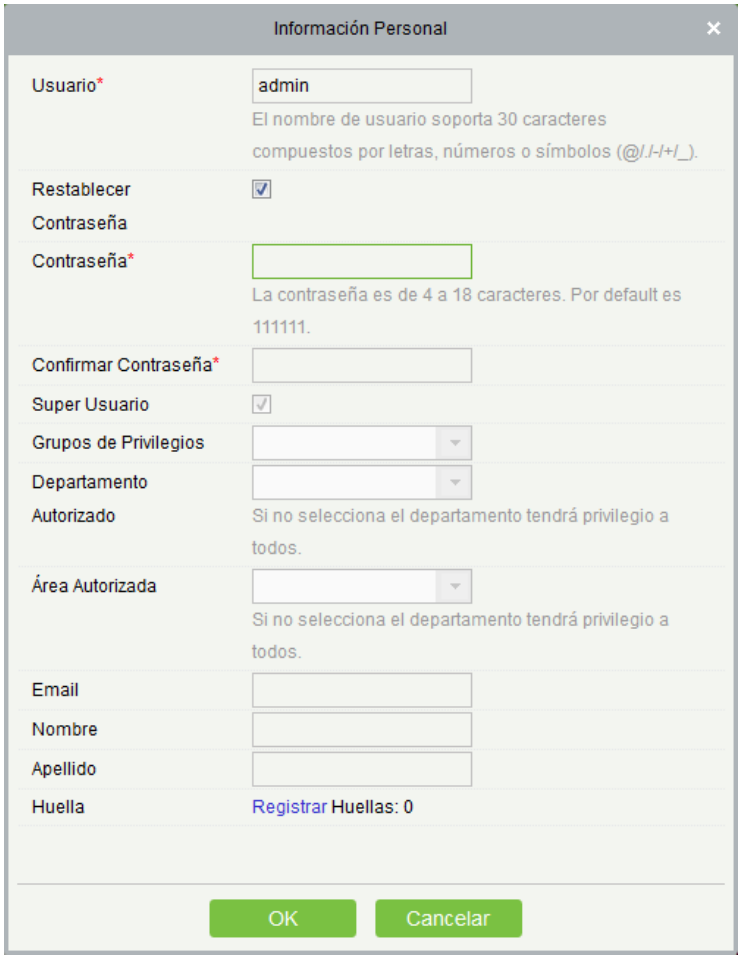
De clic en el la esquina superior derecha de cada módulo para modificar la lista de funciones.

2.4 Activar el Sistema

Consulte el documento de licencia correspondiente.

2.5 Modificar Contraseña

Puede modificar la contraseña de inicio de sesión en [Información Personal] :



Marque la casilla [Restablecer Contraseña] para modificar la contraseña.

Nota: El súper usuario y el usuario nuevo creado por el súper usuario tienen la contraseña 111111 por defecto. El nombre de usuario es sensible a mayúsculas y minúsculas.

2.6 Soporte Técnico

De clic en el botón de [Soporte Técnico] ubicado en la esquina superior derecha de la interfaz para obtener ayuda.

2.7 Salir del Sistema

De clic [Cerrar Sesión] ubicado en la esquina superior derecha de la interfaz para salir del sistema.

3 Usuarios del Sistema

Antes de usar las otras funciones, configure los usuarios del sistema: Personal y Gestión de Tarjetas.

3.1 Personal

El módulo de personal incluye los sub módulos: Usuarios, Departamentos, Atributos Personalizables y Parámetros.

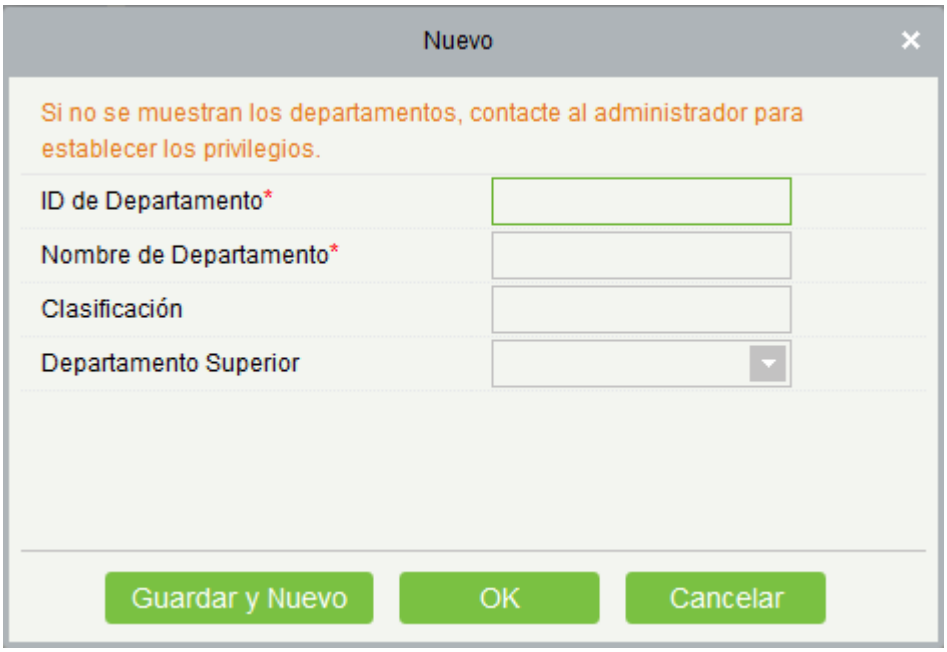
3.1.1 Gestión de Departamentos

Antes de gestionar el personal es necesario establecer el organigrama de departamentos de la compañía. El sistema cuenta con un departamento raíz llamado [Nombre de Departamento] con el número de ID [1]. Este departamento puede ser modificado, pero no puede ser eliminado.

Las funciones principales incluyen Agregar, Editar y Borrar Departamento.

- Agregar un Departamento

- 1. De clic en [Personal] > [Departamentos] > [Nuevo]:



Descripción de los campos:

ID de Departamento.: Se pueden introducir letras y números. No se puede repetir y no debe exceder 30 caracteres.

Nombre de Departamento: Cualquier caracter. Máximo 100 caracteres.

Clasificación: Solo soporta números y el rango válido es de 1 a 999999999. Mientras menor sea el número de un departamento en la clasificación de un mismo nivel, mayor jerarquía tendrá. Si no se ingresa ningún valor será asignado de acuerdo al orden en que se agregue.

Departamento Superior: Seleccione un departamento superior de la lista desplegable. El departamento superior es un parámetro importante para determinar el organigrama de la compañía. En la parte izquierda de la interfaz se mostrará el organigrama de la compañía en forma de diagrama de árbol.

2. Después de editar, de clic en [OK] para agregar, de clic en [Cancelar] para cancelar o de clic en [Guardar y Nuevo] para guardar los cambios y agregar uno nuevo.

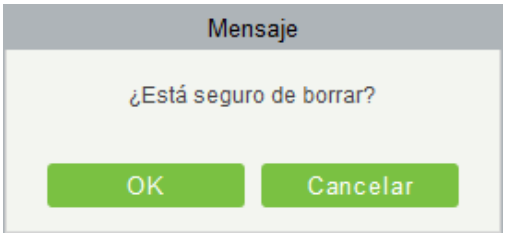
Para agregar un departamento, también puede usar la herramienta [Importar] para importar la información de departamentos de un documento o un software de terceros a este sistema. Para más detalles consulte el anexo Operaciones Comunes.

- Editar un Departamento

De clic en [Personal] > [Personal] > [Departamentos] > [Editar].

- Borrar un Departamento

De clic en [Personal] > [Personal] > [Departamentos] > [Borrar]:



2. De clic en [OK] para borrar.

✍ **Nota:** Si el departamento contiene sub-departamentos o personal, no podrá ser borrado.

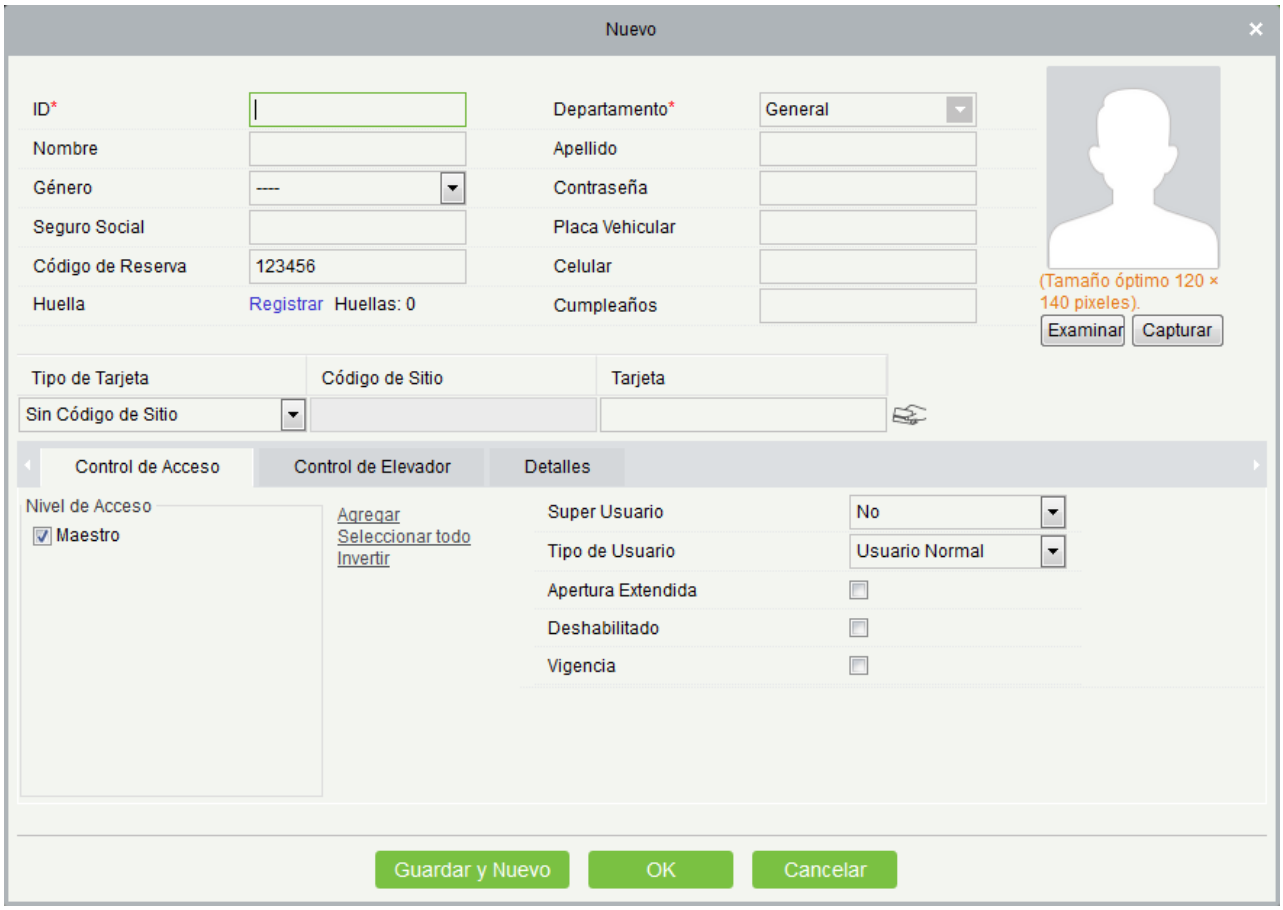
3.1.2 Personal

Al usar éste módulo de gestión, el usuario debe registrar personal en el Sistema o importar la información de personal de un documento o software de terceros a este sistema. Para más detalles, consulte Operaciones Comunes.

Las funciones principales de gestión de personal incluyen Agregar, Editar, Borrar y Ajustar Departamento.

- Agregar Personal

1. De clic en [Personal] > [Personal] > [Usuarios] > [Nuevo]:



Descripción de los campos a continuación:

ID de Usuario.: Debe ser único y de máximo 9 caracteres de longitud. El rango válido es de 1 a 79999999 y puede ser configurado según sea necesario. El ID de Usuario por defecto solo incluye números, pero también pudiera incluir letras.

✍Notas:

(1) Cuando introduzca el ID de Usuario confirme que el dispositivo soporta la longitud máxima de números y la inclusión de letras en el ID.

(2) Cuando modifique la longitud máxima o la inclusión de letras de en el ID de Usuario, ingrese a Personal > Parámetros para configurar.

Departamento: Seleccione en el menú desplegable y de clic en [OK]. Si no ha agregado departamentos anteriormente sólo podrá seleccionar el departamento predeterminado [General].

Nombre/Apellido: La longitud máxima es de 50 caracteres para cada campo.

Contraseña: Establece la contraseña del personal. Sólo admite 6 dígitos. Si la contraseña excede la longitud especificada, el sistema truncará automáticamente. No puede ser igual a otras o la contraseña de coacción.

Cédula/Seguro Social: Establece el número de cédula o seguro social con longitud máxima de 20.

Placa/Celular: La longitud máxima es de 20.

Número de Tarjeta: La longitud máxima es de 10, y no pueda ser duplicada.

Fecha de Empleo: Introduzca la fecha en que el empleado fue contratado.

Código de Reservación: La longitud máxima es de 6. La contraseña por defecto es 123456.

Foto Personal: Puede usar la vista previa, soportando formatos de imagen comunes tales como jpg, jpeg, bmp, png, gif etc. La resolución óptima es de 120×140 pixeles.

- Examinar: De clic en [Examinar] para seleccionar una imagen local para subir.
- Capturar: Puede capturar una foto si existe una cámara conectada a la PC.

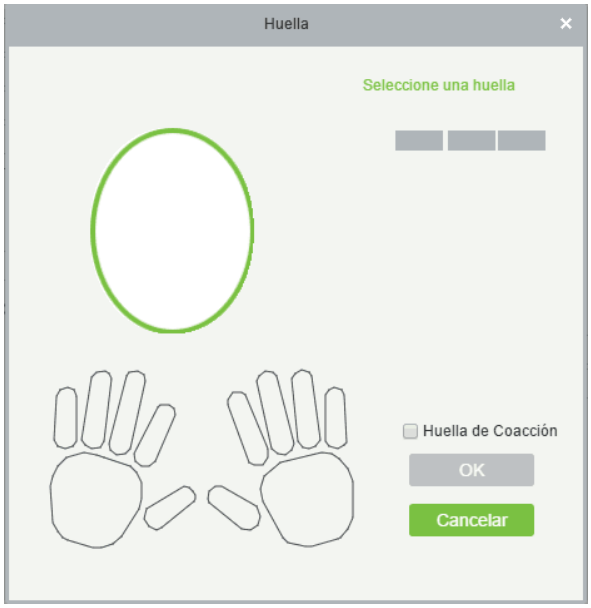
Registro de Huellas/Venas: Registre la huella o vena de acceso o huella de coacción del personal. Al registrar la huella de coacción y verificarla se envía una señal de alarma al Sistema.

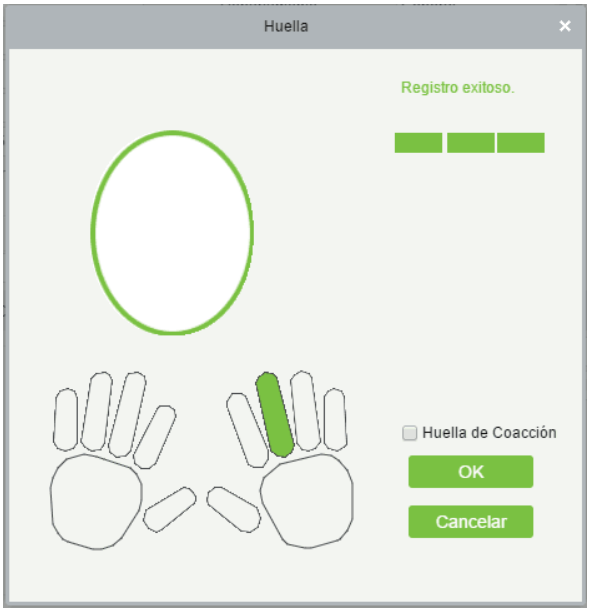
Como registrar las huellas digitales:

1) De clic en [Registrar].

2) Seleccione una huella y pulse la huella en el lector USB tres veces. Si el registro fue exitoso se mostrará el mensaje "Registro exitoso".

3) De clic en [OK] para finalizar el registro.





De clic en una huella registrada para borrarla. Si requiere registrar una huella de coacción, de clic en la casilla de huella de coacción antes de seleccionar la huella y registre normalmente.

✍Notas:

- Si se duplican las huellas se mostrará el mensaje "Huella duplicada".
- Si el driver del lector USB no está instalado, de clic en "Descargar Driver" y el Sistema le pedirá descargar e instalar el driver.
- Después de instalar el driver, si la huella de registrar está en gris (deshabilitada) en IE, pero está habilitada en otros navegadores (Firefox, Chrome, etc.) es necesario cambiar la configuración de IE como se describe a continuación:

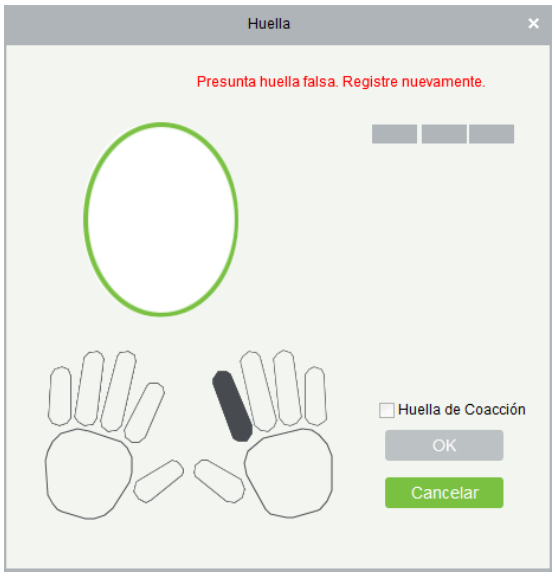
  1) En IE de clic en [Herramientas] → [Opciones de Internet] → [Seguridad] → [Sitios Seguros] y agregar http://localhost a la lista de sitios seguros y después reiniciar IE.

2) En IE de clic en [Herramientas] → [Opciones de Internet] →[Avanzado] →[Reset] para abrir una ventana de dialogo para restablecer los ajustes de IE, de clic en [Reset] para confirmar; después reinicie IE. Este paso es solo necesario si el paso 1 no fue exitoso.

3) Si los ajustes anteriores no funcionan, ejecute las siguientes operaciones (tome IE11 como ejemplo): de clic en [Herramientas] → [Opciones de Internet] →[Avanzado] →[Seguridad], habilite la opción de [Permitir el software ejecutar aún si la firma…], y remueva la casilla entes [Revisar revocación de certificado del servidor] y luego reinicie IE.

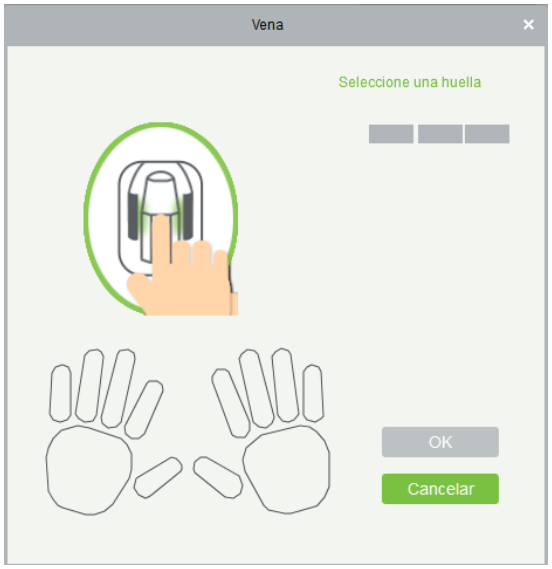
4) Si el navegador es anterior a IE8, la interfaz de registro de huellas será diferente:

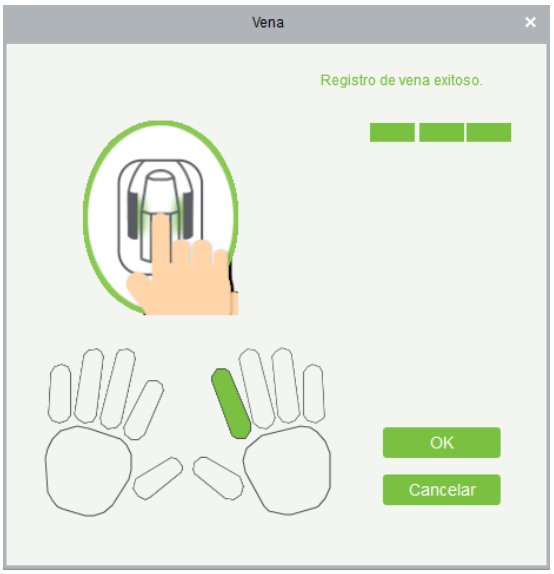
(5) El sistema soporta el lector SLK20R con la función de detección de huella digital falsa.



El proceso de registro de venas dactilares se realiza de la siguiente manera:

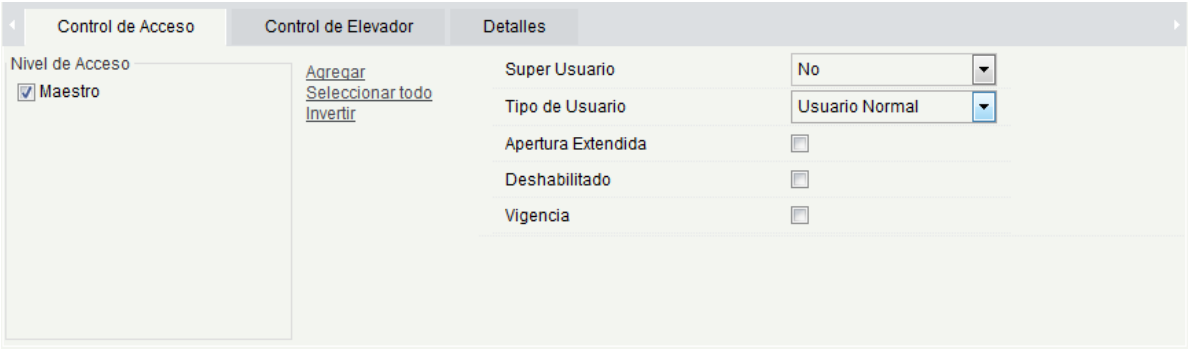
1) Clic en [Registrar]. Se muestra la página de registro.
2) Seleccione un dedo y presione la vena dactilar en el dispositivo 3 veces consecutivas. El sistema mostrará el mensaje "Registro de vena exitoso".
3) Clic en [OK] para guardar y cerrar la ventana de registro de vena dactilar.





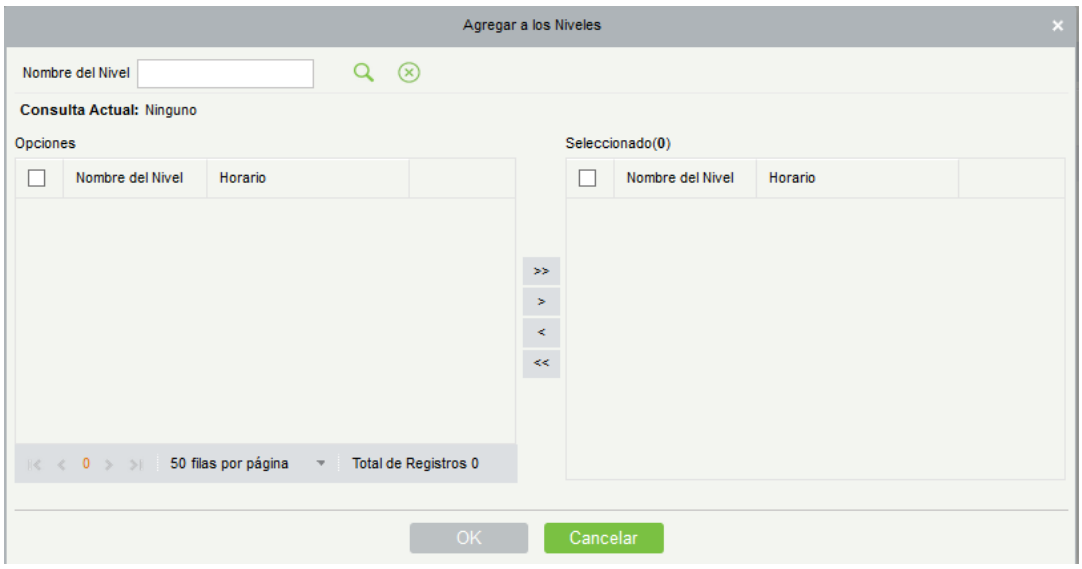
Para borrar una vena dactilar registrada, de clic en la vena dactilar y luego clic en [OK].

2. Configure los parámetros de control de acceso del personal. De clic en [Control de Acceso]:



Descripción de los campos:

Nivel de Acceso**:** De clic en [Agregar], establezca las reglas de acceso y horarios.



Superusuario: Un superusuario no está restringido por las normativas de horarios, anti-passback y en esclusamiento tiene muy alta prioridad de apertura de puerta.

Tipo de Usuario: Seleccione administrador o usuario normal según sea el caso.

Apertura Extendida: Extiende el tiempo normal de apertura de puerta para personas con capacidades diferentes o especiales.

Deshabilitado: Deshabilita temporalmente el nivel de acceso del usuario.

Vigencia: Establece la validez temporal de un nivel de acceso. Las puertas se pueden configurar para ser abiertas durante un periodo de tiempo específico. Si no se configura, el tiempo de validez es permanente.

✍Nota: El ID de un usuario, se encuentre activo o no, debe ser único. Al verificar, el sistema buscará el ID automáticamente en la librería de salida.

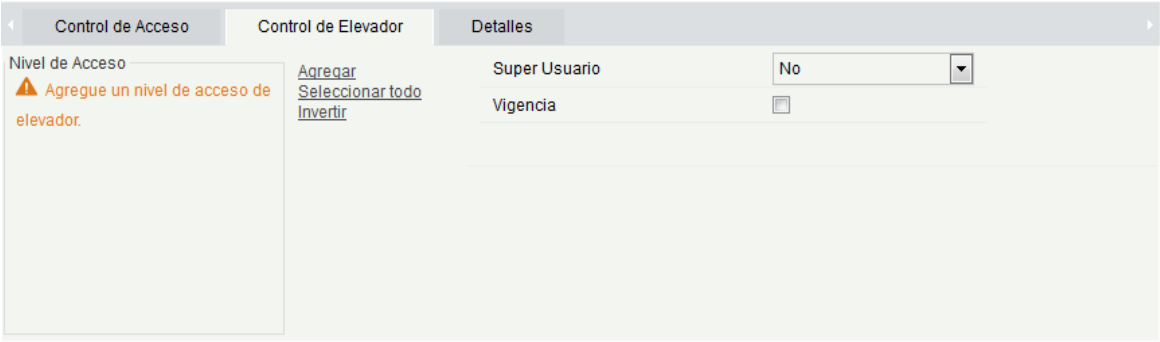
La lista de información de personal, por defecto, se muestra como una tabla. Si selecciona pantalla gráfica se mostrarán fotos y números. Coloque el cursor en una foto y se mostrará la información sobre el personal.

✍Notas:

(1) No todos los dispositivos soportan la función "Deshabilitado". Cuando un usuario agregue un dispositivo, el sistema notificará al usuario si el dispositivo actual soporta esta función. Si el usuario requiere usar esta función, actualice el dispositivo que no soporta esta función.

(2) No todos los dispositivos soportan la función de "Vigencia" de establecer la hora, fecha, minuto y segundo. Algunos dispositivos solo permiten a los usuarios establecer el año, mes y día de la vigencia. Cuando un usuario agregue un dispositivo, el sistema notificará al usuario si el dispositivo actual soporta esta función. Si el usuario requiere usar esta función, actualice el dispositivo que no soporta esta función.

3. Configure los parámetros de control de elevador del personal. De clic en [Elevador]:



Descripción de los campos a continuación:

Superusuario: Un superusuario no está restringido por las normativas de horarios, anti-passback y en esclusamiento tiene muy alta prioridad de control elevador.

Vigencia**:** Establece la validez temporal de un nivel de acceso de elevador. Los botones de los pisos se pueden configurar para estar habilitados durante un periodo de tiempo específico. Si no se configura, el tiempo de validez es permanente.

✍Nota: Los niveles de elevador deben configurarse previamente.

4. De clic en [Detalles] para introducir información adicional del personal y activar el envío de notificaciones por eventos relacionados con el usuario.

Descripción de los campos a continuación:

Email: Introduzca el correo electrónico del personal. La longitud máxima es de 30 caracteres. Los caracteres "-", "_" y "." son soportados.

Notificación de Correo: Después de marcar esta opción, el sistema enviará correos a esta persona cada vez que realice un evento de acceso o elevador. Si no se ha configurado el servidor de correo, emergerá la ventana de configuración de correo. Consulte Correo Electrónico para más información.

5. Después de completar la información, de clic en [OK] para guardar y salir. El personal se mostrará en la lista de usuarios.

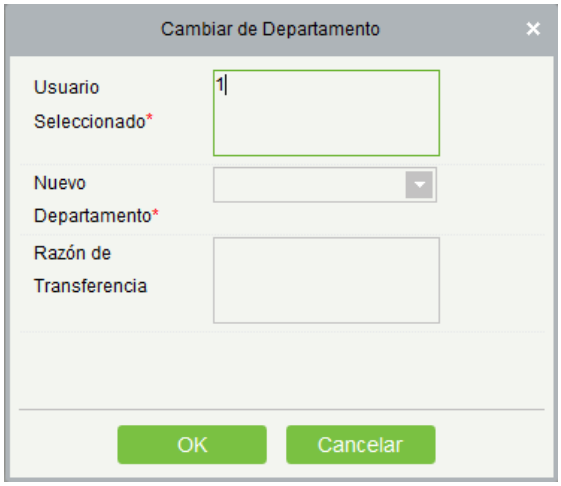
- Borrar Personal

De clic en [Personal] > [Usuarios], seleccione un usuario, de clic en [Borrar] y luego en [OK] para borrar.

✍Nota: Al borrar un usuario toda la información de esa persona será eliminada.

- Cambiar de Departamento

1) De clic en [Personal] > [Usuarios], seleccione un usuario y de clic en [Cambiar Departamento]:

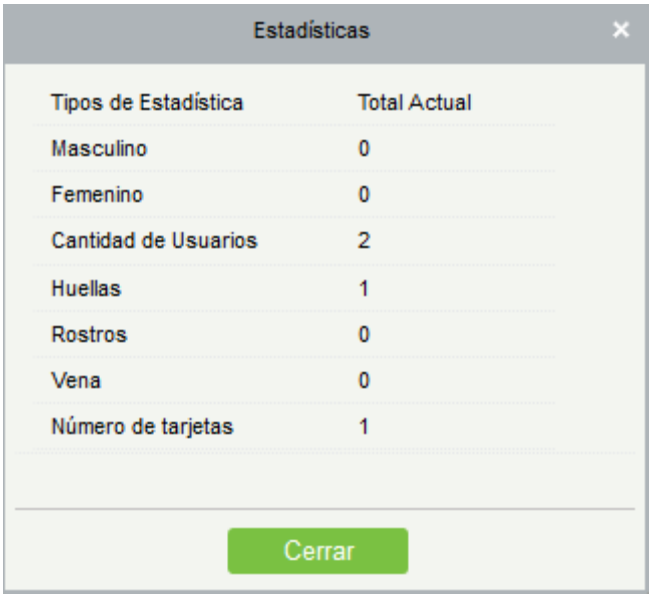


2) Seleccione el "Nuevo Departamento".

3) De clic en "OK" para guardar y salir.

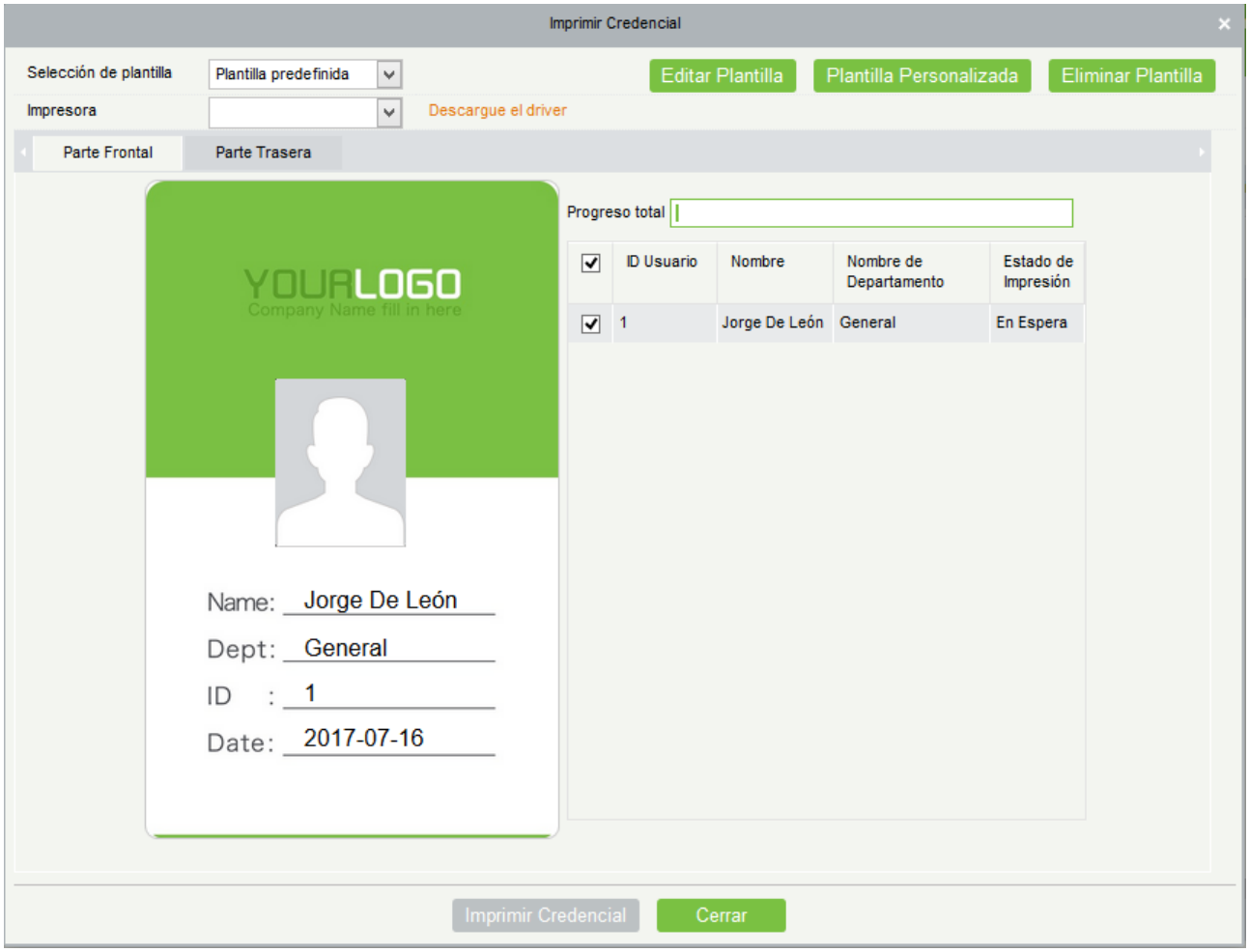
- Estadísticas

De clic en [Personal] > [Usuario] > [Estadísticas]. Vea el número de usuarios, huellas digitales, rostros, venas dactilares, tarjetas, género y otros datos.



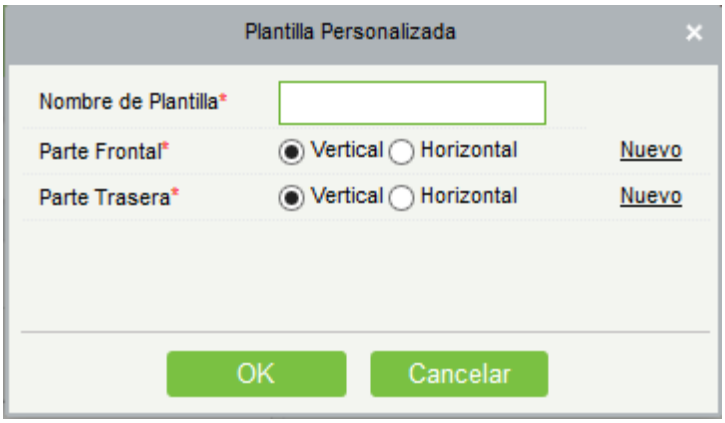
- Credencialización (Imprimir Credencial)

De clic en [Personal] seleccione un usuario y de clic en [Imprimir Credencial].

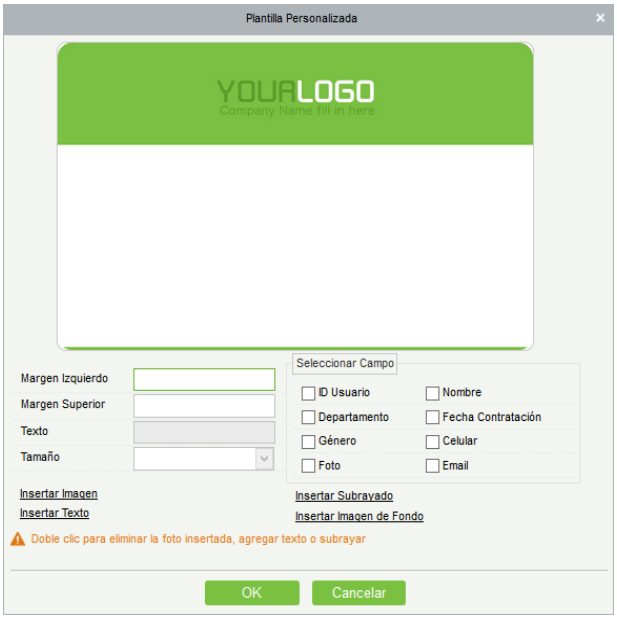


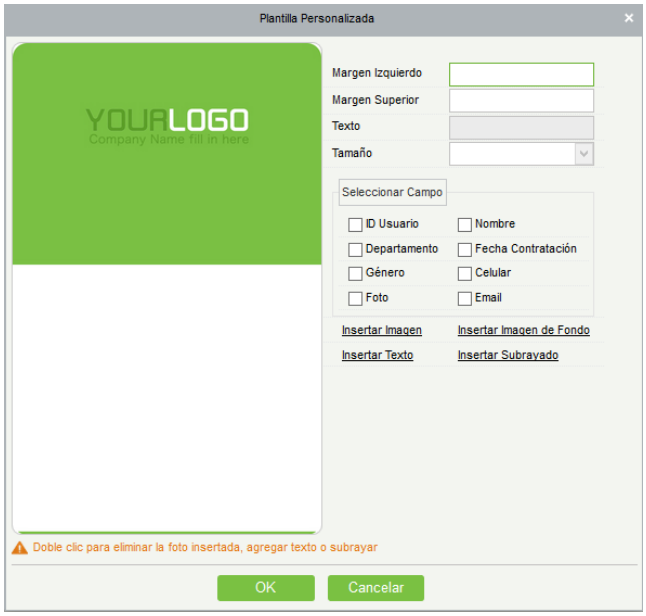
Seleccione una plantilla de credencial y una impresora y de clic en [Imprimir Credencial].

1. Para agregar una plantilla, de clic en [Plantilla Personalizada].

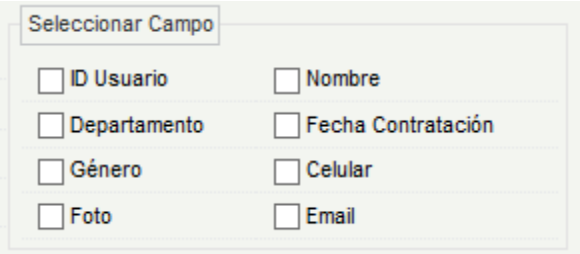


Introduzca el [Nombre de Plantilla], seleccione la dirección de la plantilla y de clic en [OK]. La figura de la izquierda es una plantilla vertical y la de la derecha es una plantilla horizontal.

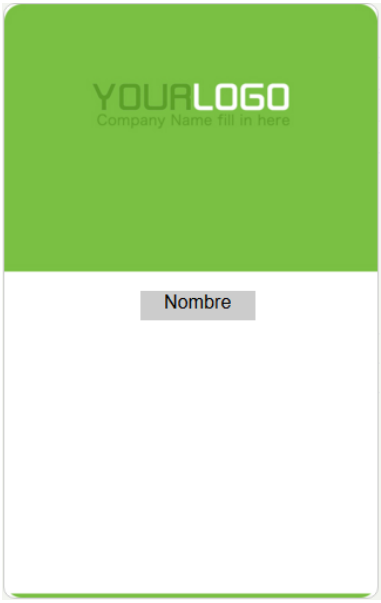




(1) Seleccione los campos.



Seleccione los campos correspondientes. Los campos se mostrarán en la plantilla. Puede arrastrar los campos para cambiar el diseño de la credencial.



(2) Es posible insertar fotografías, imágenes de fondo, textos y subrayados en la plantilla.

Introduzca el texto que será insertado en [Texto] para insertarlo en la plantilla.

Margen Izquierdo	78
Margen Superior	174
Texto	ZKTeco
Tamaño	18px

Notas:

1) De clic en para eliminar los campos insertados.

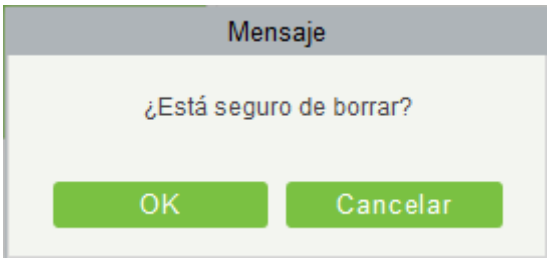
2) De doble clic en las imágenes insertadas, texto o subrayado para eliminar.

3) Cargue una imagen de fondo de 635 x 1010 pixeles para la plantilla vertical o una imagen de 1010 x 635 pixeles para la plantilla horizontal.

2. Para editar una plantilla, de clic en [Editar Plantilla]. El procedimiento para editar una plantilla es el mismo que para agregar una plantilla por lo que no será descrito.

Nota: La plantilla vertical y horizontal por defecto no puede ser editada. Solo las plantillas personalizadas pueden ser editadas.

3. Para borrar una plantilla de clic en [Eliminar Plantilla].



De clic [OK] para borrar la plantilla.

Nota:

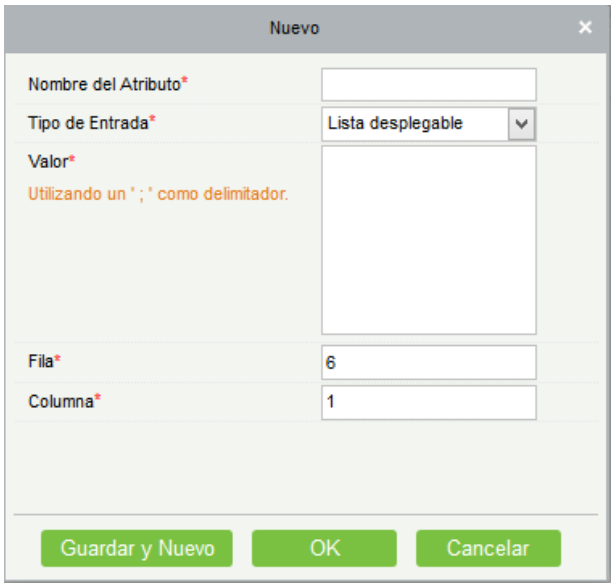
La plantilla vertical y horizontal por defecto no puede ser eliminada. Solo las plantillas personalizadas pueden ser eliminadas.

3.1.3 Atributos Personalizables

Algunos atributos personales pueden ser personalizados o eliminados para cubrir requisitos especiales de algunos clientes. Cuando el sistema es usado por primera vez, algunos atributos serán establecidos por defecto. Puede ajustar estos atributos para cumplir los requerimientos del proyecto.

- Nuevo Atributo

1) De clic en [Personal] > [Personal] > [Atributos Personalizables] > [Nuevo], edite los parámetros y de clic en [OK] para guardar y salir.



Descripción de los campos a continuación:

Nombre del Atributo: Debe introducir un nombre único de máximo 30 caracteres.

Tipo de Entrada: Seleccione el tipo de entrada la cual incluye "Lista desplegable", "Opción Múltiple", "Opción Única" y "Texto".

Valor: Adecuado para entrada de lista desplegable, opción múltiple y opción única. Uso de "1" para distinguir los valores múltiples. Si la entrada de datos es texto el campo de valor no es adecuado.

Fila/Columna: La fila y columna de un campo se utilizan juntos para controlar la posición de visualización de un campo. Es posible introducir números y el número de columna no puede exceder de 99 y el número de fila solo puede ser 1 ó 2. La combinación de fila y columna debe ser única. Ejemplo: en la siguiente figura, el campo de tipo de empleado se encuentra en la columna 1, fila 1 y el campo de tipo de contratación está en columna 1, fila 2.

- Editar un Atributo Personalizable.

De clic en [Editar] debajo de Operaciones para modificar el atributo correspondiente.

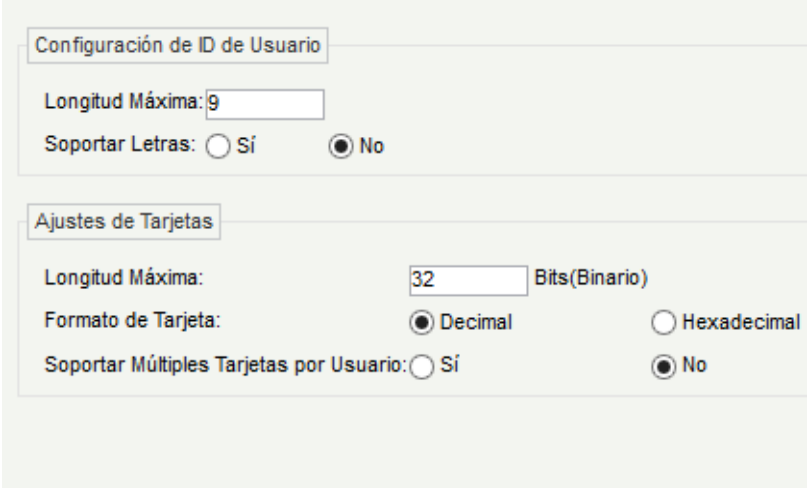
- Borrar un Atributo Personalizable.

De clic en [Borrar] debajo de Operaciones para borrar el atributo correspondiente. Si el atributo se encuentra en uso, el Sistema mostrará una advertencia para confirmar la operación.

✍Nota: Una vez que se elimina el atributo no puede ser recuperado.

3.1.4 Parámetros

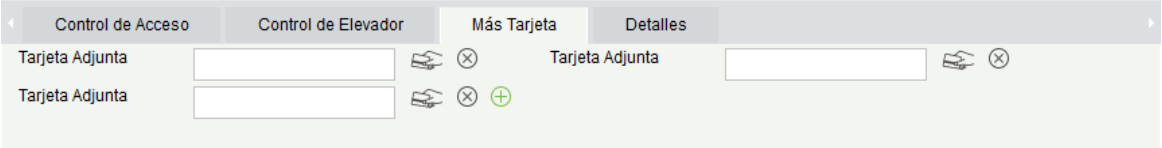
De clic en [Personal] > [Personal] > [Parámetros]:



2) Establece la longitud máxima del ID de Usuario y si soporta letras.
3) Establece la longitud máxima (bits) del número de tarjeta que el sistema soporta actualmente.
4) Establece el formato de tarjeta usado en el sistema actualmente. El formato de tarjeta no puede ser cambiado cuando el sistema tiene una tarjeta.
5) Establece si se habilita la función de Múltiples Tarjetas por Usuario en el sistema.
6) De clic en [OK] para guardar los ajustes y salir.

- Múltiples Tarjetas

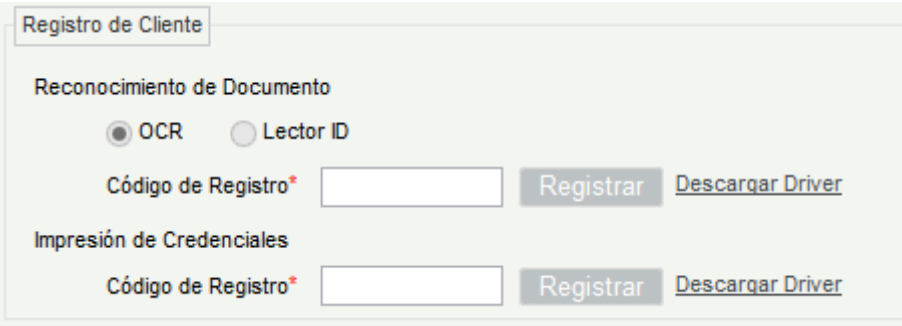
Después de habilitar la función de Múltiples Tarjetas por Usuario, es posible asignar varias tarjetas a los usuarios en el módulo de personal.



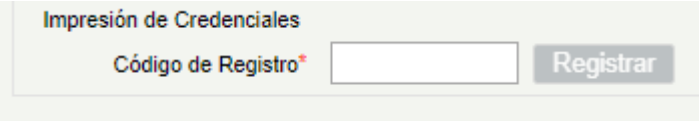
✍Nota: No todos los dispositivos soportan la función de Múltiples Tarjetas por Usuario. Para los detalles por favor consulte con el personal de soporte técnico.

- Registro de Cliente

1) Si no ha instalado el driver se mostrará el enlace [Descargar Driver]. De clic en el enlace para descargar e instalar el driver.



2) Introduzca el código de registro correspondiente y de clic en [Registrar].



✍ **Nota:** De clic en [Sistema] > [Privilegios] > [Registro de Clientes] para ver los códigos de registro.

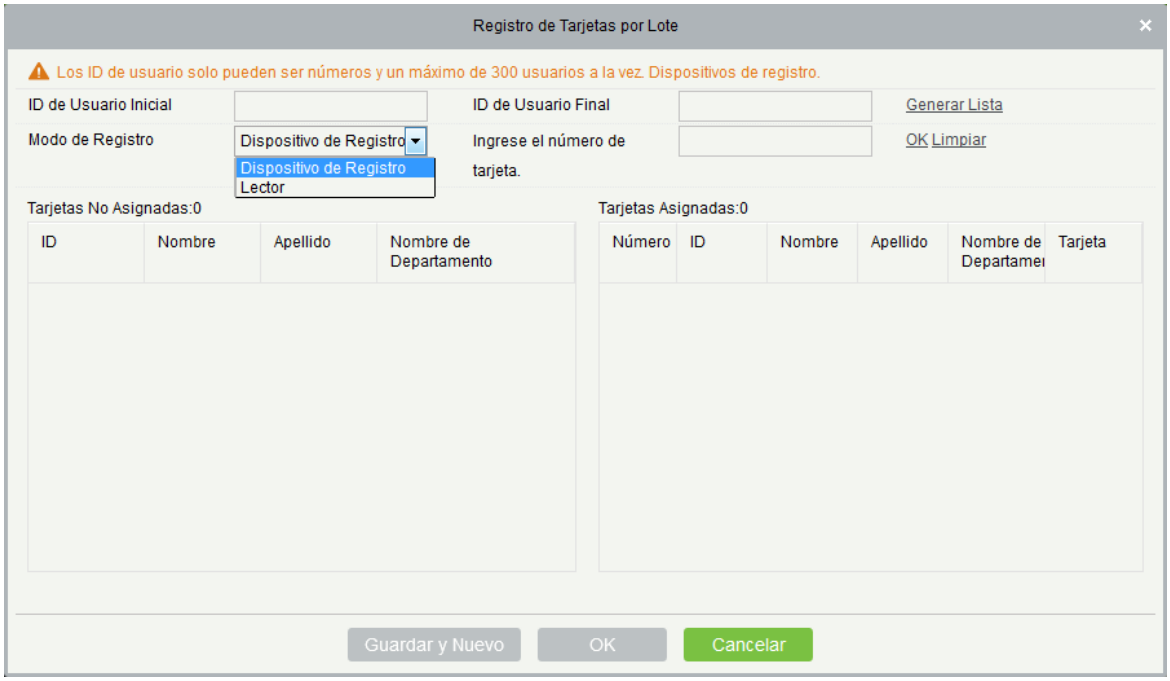
3.2 Gestión de Tarjetas

Existen tres módulos en Gestión de Tarjetas: Tarjetas, Formato Wiegand y Bitácora de Tarjetas.

3.2.1 Tarjetas

- Registro de Tarjetas por Lote

1) De clic en [Personal] > [Gestión de Tarjetas] > [Tarjetas] > [Registro de Tarjetas por Lote]:



2) Introduzca el ID de Usuario inicial y final y de clic en [Generar Lista] para generar la lista de usuarios que se asignarán las tarjetas.

✍Nota: El ID de Usuario inicial y final solo soporta números.

3) Seleccione el modo de registro de las tarjetas: Dispositivo de Registro o Lector.

Para el uso de Dispositivo de Registro deberá presentar la tarjeta directamente en el dispositivo. El sistema capturará el número de tarjeta y lo asignará al personal de la lista.

Para el uso de Lector, debe seleccionar el punto de captura y dar clic en [Iniciar la Captura], el Sistema capturará el número de tarjeta automáticamente y lo asignará al personal de la lista uno por uno. Al finalizar de capturar, de clic en [Detener la Captura].

✍Nota: Durante el registro de tarjetas por lote, el sistema verificará si la tarjeta ha sido asignada previamente. Si la tarjeta ha sido registrada previamente mostrará la advertencia.

4) De clic en [OK] para completar el registro de tarjetas y regresar.

3.2.2 Formato Wiegand

El formato Wiegand es el formato de tarjeta que puede ser identificado por los lectores Wiegand. El software incluye 9 formatos Wiegand por defecto. Es posible configurar el formato según las necesidades.

Refrescar Nuevo Borrar

Nombre	Modo	Auto	Operaciones
Formato Wiegand26	Modo Uno	Sí	Editar
Formato Wiegand26a	Modo Uno	No	Editar
Formato Wiegand34	Modo Uno	Sí	Editar
Formato Wiegand34a	Modo Uno	No	Editar
Formato Wiegand36	Modo Uno	Sí	Editar
Formato Wiegand37	Modo Uno	Sí	Editar
Formato Wiegand37a	Modo Uno	No	Editar
Formato Wiegand50	Modo Uno	Sí	Editar
Formato Wiegand66	Modo Uno	Sí	Editar

El software soporta dos modos para agregar formatos Wiegand. Si el modo 1 no cumple sus requerimientos de configuración, cambie al modo 2. Ejemplo del formato Wiegand 37:

Editar

Nombre* Formato Wiegand26

Total de Bits* 26

Auto ☑

◉ Modo Uno

Primer Bit de Paridad(p) 1

Segundo Bit de Paridad(p) 26

Comprobación de paridad impar(o)		Comprobación de paridad par (e)		CID(c)		Facility Code(f)		Código de Sitio(s)		Código de Fabricante(m)	
Bit de Inicio	Longitud Máxima	Bit de Inicio	Longitud Máxima	Bit de Inicio	Longitud Máxima	Bit de Inicio	Longitud Máxima	Bit de Inicio	Longitud Máxima	Bit de Inicio	Longitud Máxima
14	13	1	13	2	24	0	0	0	0	0	0

○ Modo Dos

Formato de Tarjeta*	pcccccccccccccccccccccccp
Formato de Paridad*	eeeeeeeeeeeeeoooooooooooooo

OK Cancelar

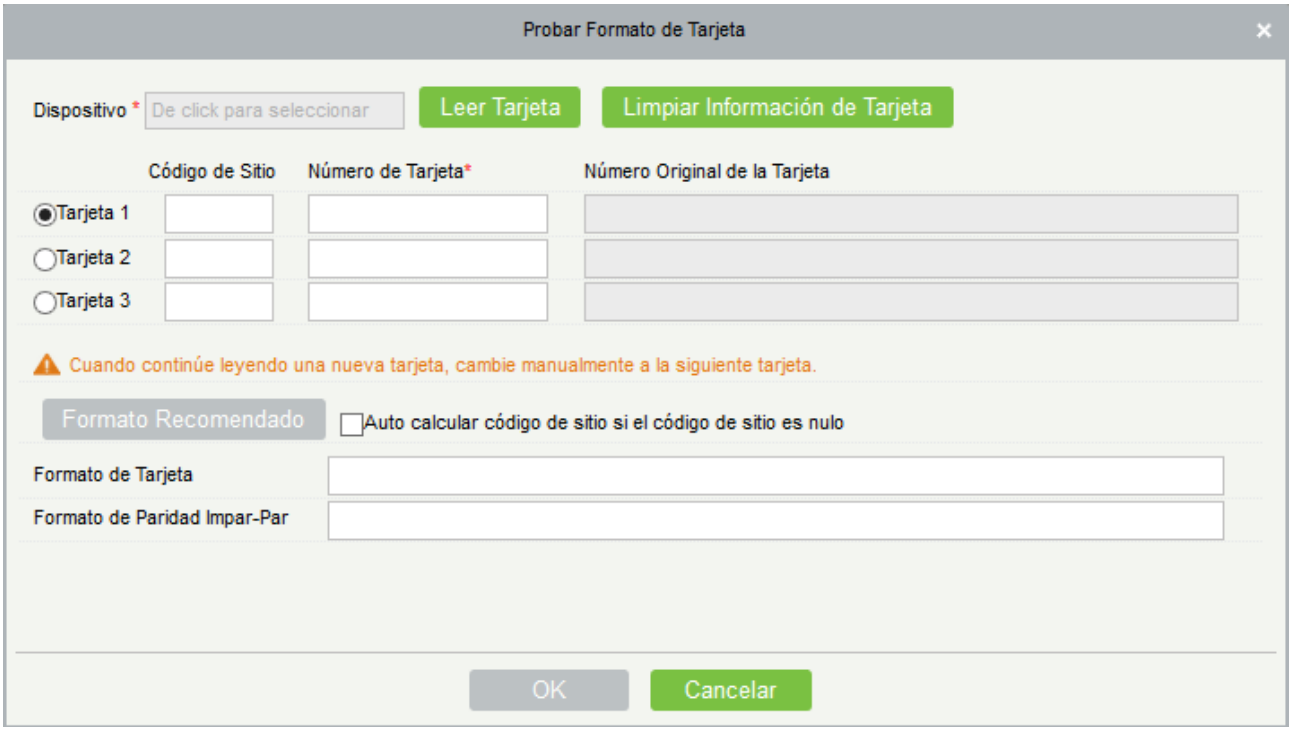
Especificación del Formato:

La letra (p) indica la posición de paridad, (s) indica el código de sitio, (c) indica el número de tarjeta, (f) indica el facility code, (m) indica el código de fabricante, (e) indica paridad par, (o) indica paridad impar, (b) indica ambas par e impar y (x) indica bits de paridad.

El formato Wiegand 37: Los primeros bits de paridad (p) "eeeeeeeeeeeeeeeeee", los siguientes bits "oooooooooooooooooooo". El formato de tarjeta solo puede ser " p, x, m, f, c, s", el formato de paridad solo puede ser " x, b, o, e".

- ## Prueba de Formato de Tarjetas

Si el número impreso en la tarjeta es diferente al número mostrado después de leer la tarjeta, puede usar esta función para calibrar el formato Wiegand. La ventana se muestra a continuación:



Seleccione un dispositivo que soporte la función de prueba de formato de tarjeta e introduzca el número y código de sitio (opcional) de la tarjeta.

1)De clic en [Leer Tarjeta] y presente la tarjeta en el lector. El número de tarjeta original leído por el dispositivo será mostrado en el campo de la derecha.

2)De clic en [Recomendar Formato]. El formato Wiegand recomendado para la tarjeta se muestra debajo.

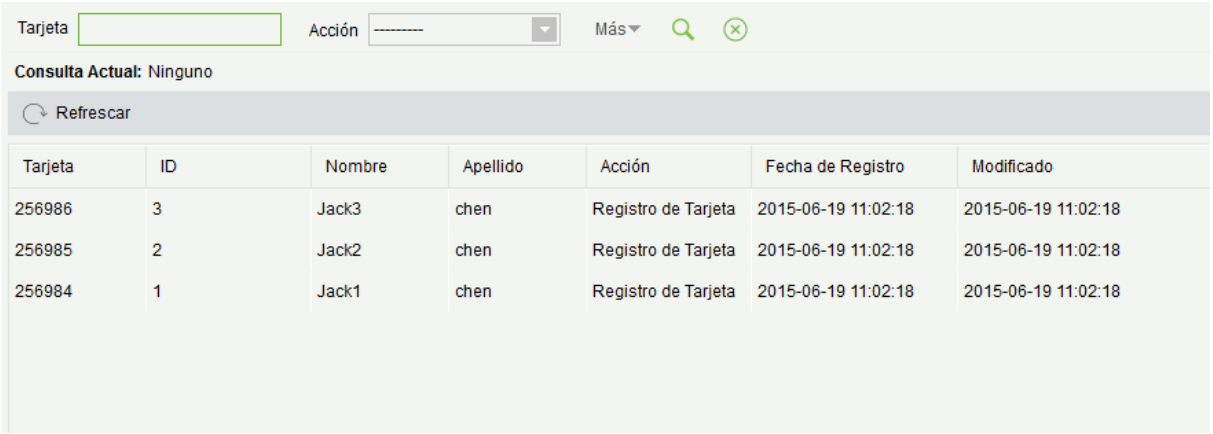
3)Si se habilita [Auto calcular código de sitio si el código de sitio es nulo], el software calculará el código de sitio basado en el formato y número de la tarjeta.

4)De clic en [OK]. La página salta a la ventana de Agregar Formato Wiegand para guardar el formato Wiegand recomendado.

✍Nota: La función de prueba de formato de tarjetas es solo soportado solamente en ciertos dispositivos.

3.2.3 Bitácora de Tarjetas

Usado para llevar el registro del ciclo de una tarjeta y mostrar las operaciones realizadas con la tarjeta.



Tarjeta	ID	Nombre	Apellido	Acción	Fecha de Registro	Modificado
256986	3	Jack3	chen	Registro de Tarjeta	2015-06-19 11:02:18	2015-06-19 11:02:18
256985	2	Jack2	chen	Registro de Tarjeta	2015-06-19 11:02:18	2015-06-19 11:02:18
256984	1	Jack1	chen	Registro de Tarjeta	2015-06-19 11:02:18	2015-06-19 11:02:18

✍Nota: Las tarjetas y los registros asignación de la tarjeta de un empleado serán borrados de manera conjunta cuando un usuario es borrado completamente.

3.3 Gestión de Directorio Activo

Para los detalles de esta función lea el respectivo manual de usuario.

4 Acceso

El sistema requiere conectar con los equipos para proveer funciones de control de acceso. Para usar éstas funciones, el usuario primero debe instalar los dispositivos y conectarlos a la red de datos y después configurar los parámetros correspondientes para la gestión de dispositivos, carga y descarga de datos de acceso, creación de reportes y lograr el control integral de la empresa.

4.1 Dispositivos

Módulo para agregar dispositivos de acceso, configurar parámetros de comunicación del sistema y dispositivos conectados. Si la comunicación con los dispositivos es exitosa, es posible ver información y detalles de los dispositivos conectados, monitorear remotamente, cargar y descargar datos y realizar diversas operaciones.

4.1.1 Dispositivos

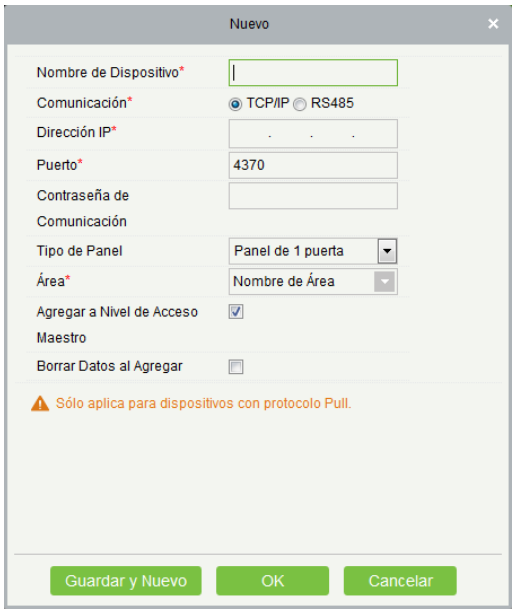
- Agregar Dispositivos

Existen tres formas de agregar dispositivos.

1. Agregar dispositivos manualmente.

(1) De clic en [Dispositivos de Acceso] > [Dispositivos] > [Nuevo] y se mostrará la siguiente interfaz:

Modo de comunicación TCP/ IP



Modo de comunicación RS485

Descripción de los campos:

Dirección IP: Introduzca la dirección IP del dispositivo.

Puerto: Puerto de comunicación del dispositivo. El valor por defecto es 4370.

Puerto Serial.: COM1 al COM254.

Dirección RS485: El ID RS485 del dispositivo. El rango es 1 a 255. En el mismo lazo de comunicación COM no se puede repetir la dirección RS485 en los dispositivos.

Baudios: Velocidad de comunicación. El defecto es 38400.

Figura de Dirección RS485: Muestra la figura del DIP Switch para ajustar la dirección RS485.

Opciones comunes:

Nombre de Dispositivo: Soporta cualquier carácter. Máx. 20.

Contraseña de Comunicación: La longitud máxima es de 6, con números o letras.

✍Notas:

1) No es necesario introducir datos en este campo si es un equipo nuevo o si recién se inicializó.

2) Al establecer la contraseña de comunicación de una terminal standalone en cero, significa que no tiene contraseña; sin embargo, para los paneles de acceso significa que la contraseña es cero.

3) Es necesario reiniciar el dispositivo después de establecer el sensor de puerta en las terminales standalone.

Tipo de Panel: Panel de 1 puerta, Panel de 2 puertas, Panel de 4 puertas o Terminal Standalone.

Zona de Tiempo: Puede establecer esta opción si el dispositivo soporta ajustar la zona de tiempo y si la zona de tiempo del dispositivo y del servidor son diferentes. Esta opción no se muestra para los dispositivos que no soportan el ajuste de zona de tiempo. Los dispositivos agregados recientemente se sincronizan con la fecha y hora del servidor por defecto.

Área: Especifica el área del dispositivo. Después de establecer las áreas es posible filtrar por área en el monitoreo en tiempo real.

Cambiar a Panel de 2 Puertas: Cuando el tipo de panel de control de acceso es de cuatro puertas es posible cambiarlo a panel de dos puertas en el sistema.

Agregar a Nivel de Acceso Maestro: Agrega el nuevo dispositivo al nivel de acceso maestro. Al agregar personal nuevo también será asignado al nivel de acceso maestro por defecto.

Borrar Datos al Agregar: Al marcar esta opción, después de agregar el dispositivo, el sistema borrará todos los datos en el dispositivo (excepto los datos de eventos). Si agrega el dispositivo sólo para demostración o pruebas no requiere marcar la opción.

(2) Después de editar de clic [OK] y el sistema tratará de conectarse con el dispositivo actual.

Si la conexión es exitosa, el sistema obtendrá los parámetros extendidos del dispositivo.

Parámetros Extendidos del Dispositivo: Estos parámetros incluyen número de serie, tipo de dispositivo, versión de firmware, cantidad de entradas y salidas auxiliares, cantidad de puertas, versión de algoritmo de huella digital, cantidad de lectores, etc.

✍Nota: Al eliminar un nuevo dispositivo, el software borrará toda información de usuarios, horarios, días festivos y configuraciones de control de acceso (incluyendo niveles de acceso, anti-passback, esclusamiento, vínculos, etc.) del dispositivo, excepto los datos de eventos (a menos que la información contenida en el dispositivo no sea útil, se

recomienda no borrar el dispositivo para evitar la pérdida de información).

Configuración de controlador de acceso:

✧ Requisitos de Comunicación TCP/ IP

Para soportar y habilitar la comunicación TCP/ IP, conecte el dispositivo directamente a la PC o a la red local, consulte la dirección IP y otros datos del dispositivo;

✧ Requisitos de Comunicación RS485

Para comunicación RS485, conecte al dispositivo a la PC mediante un convertidor e introduzca los datos al sistema como el número de puerto, ID RS485 del dispositivo, baudios, etc.

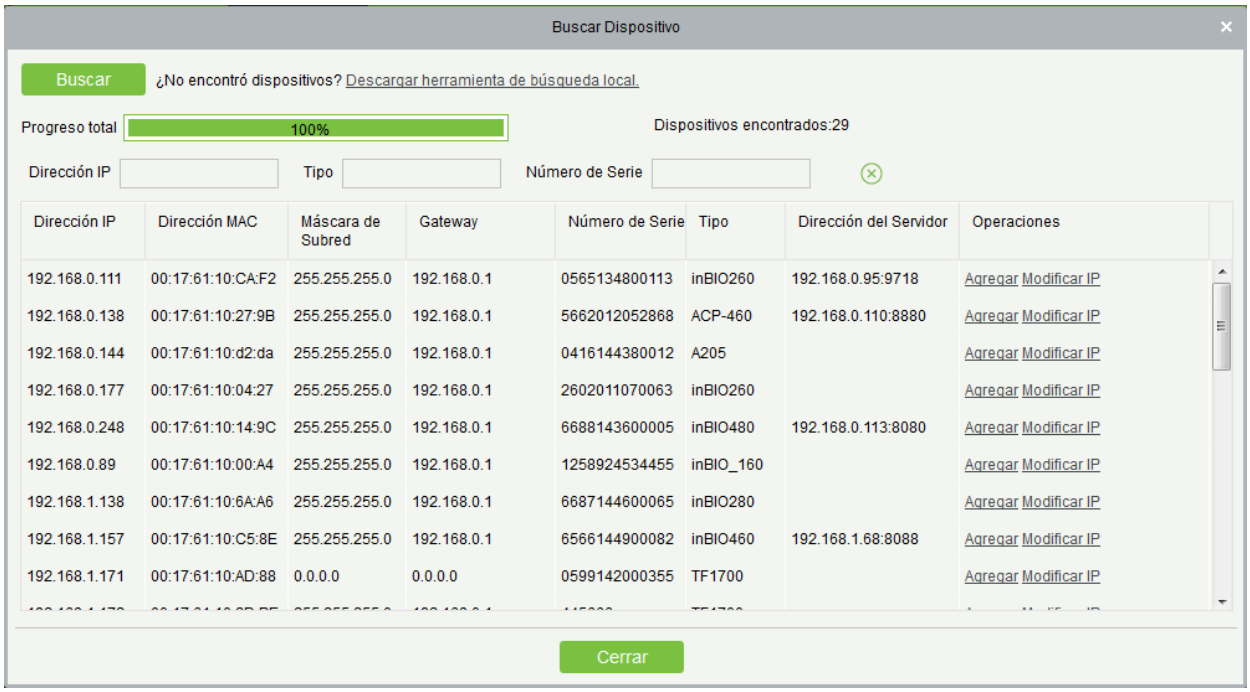
2. Agregar dispositivos por búsqueda

Buscar los dispositivos en la red.

(1) De clic en [Dispositivos de Acceso] > [Dispositivos] > [Buscar Dispositivo], para mostrar la interfaz de búsqueda.

(2) De clic en [Buscar] y se mostrará [Buscando…].

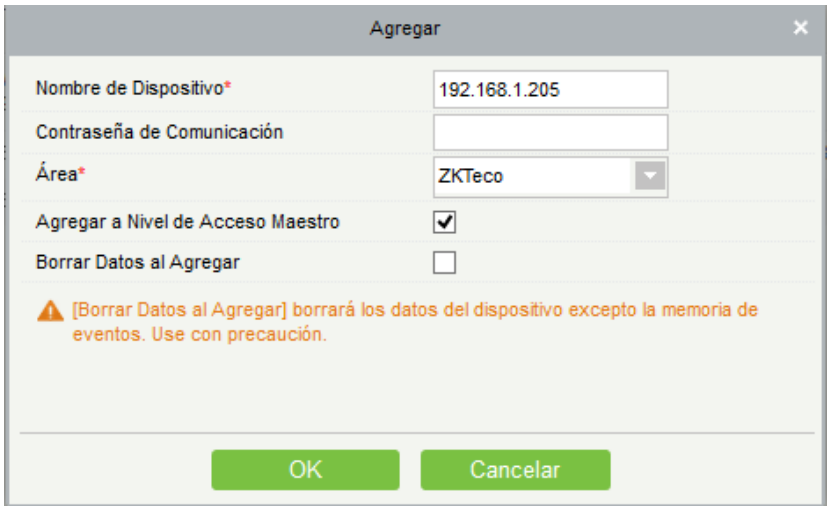
(3) Después la búsqueda se mostrarán los dispositivos encontrados como se muestra a en la imagen.



✍Nota: El modo de transmisión UDP se utilizará para buscar los dispositivos de acceso y solo funciona en la red local. Los dispositivos requieren configurarse dentro del mismo segmento de red.

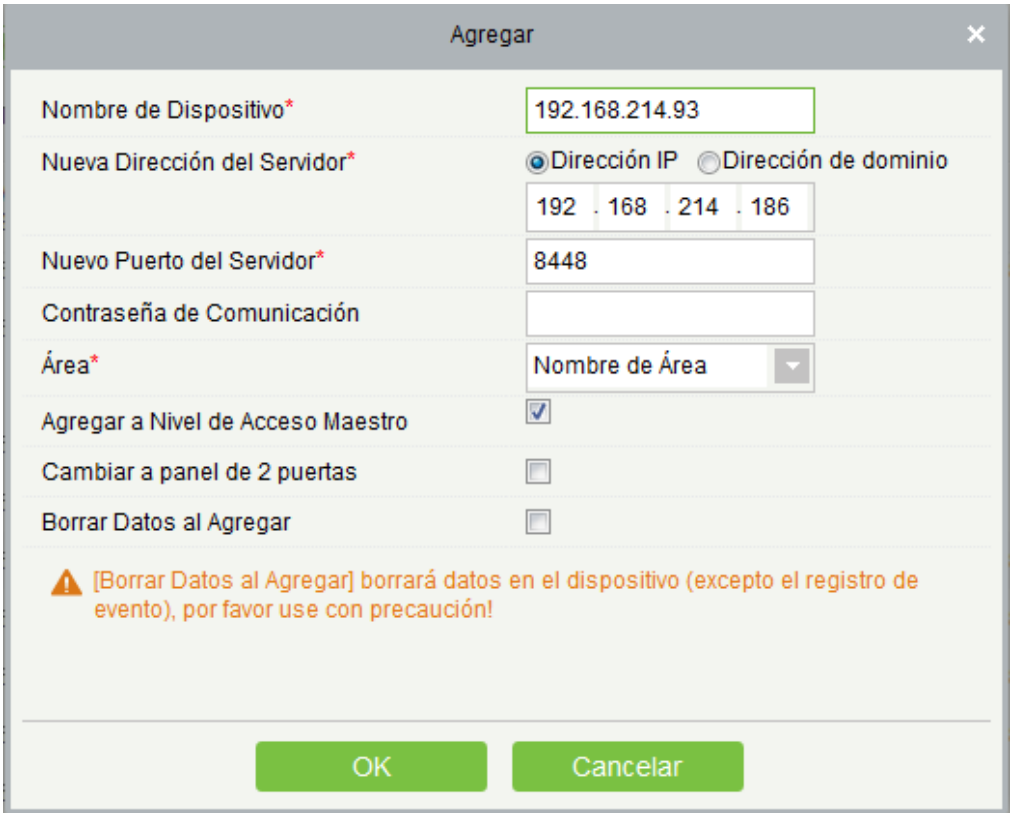
(4) De clic en [Agregar] a un lado del dispositivo.

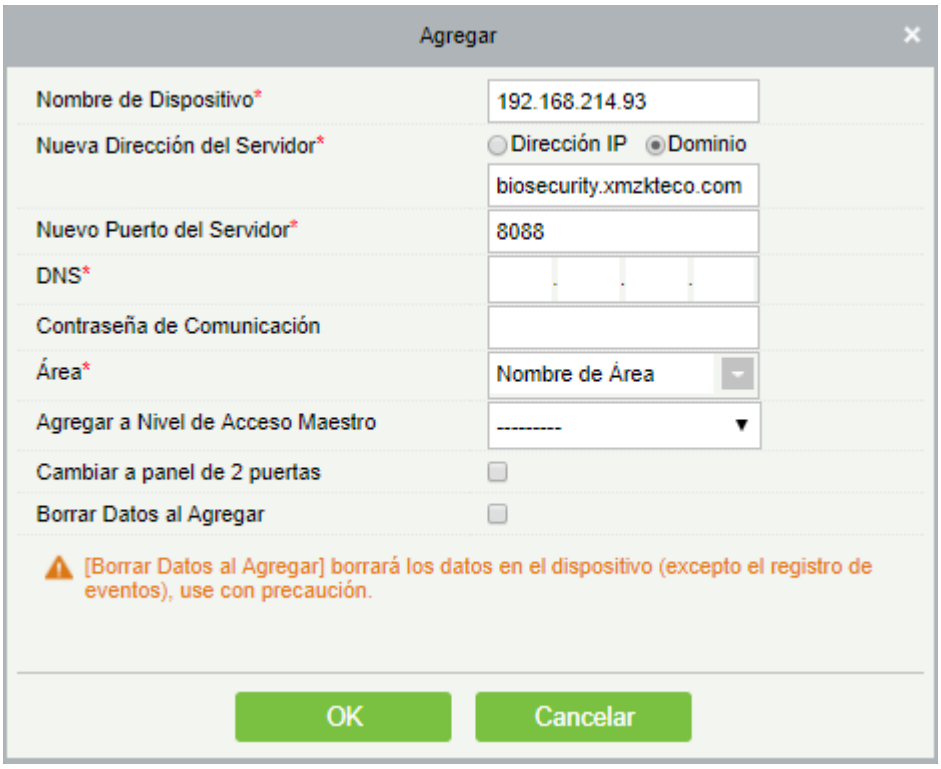
Si el dispositivo opera con firmware PULL, introduzca los datos del dispositivo en el sistema y de clic en [OK] para agregar.



Borrar Datos al Agregar: Seleccione esta opción después de dar clic en agregar y el sistema eliminará todos los datos del dispositivo (excepto los eventos).

Si el dispositivo opera con firmware PUSH, al dar clic en [Agregar] se mostrará la siguiente ventana para introducir los datos del servidor. Introduzca la dirección IP del servidor y el número de puerto y el dispositivo será agregado automáticamente.





Nueva Dirección del Servidor: Introduzca la dirección IP de la PC con el sistema actual.

Nuevo Puerto del Servidor: Introduzca el puerto del servidor. El puerto por defecto es 8080.

Borrar Datos al Agregar: Al marcar esta opción, después de agregar el dispositivo, el sistema borrará todos los datos en el dispositivo (excepto los datos de eventos). Si agrega el dispositivo sólo para demostración o pruebas no requiere marcar la opción.

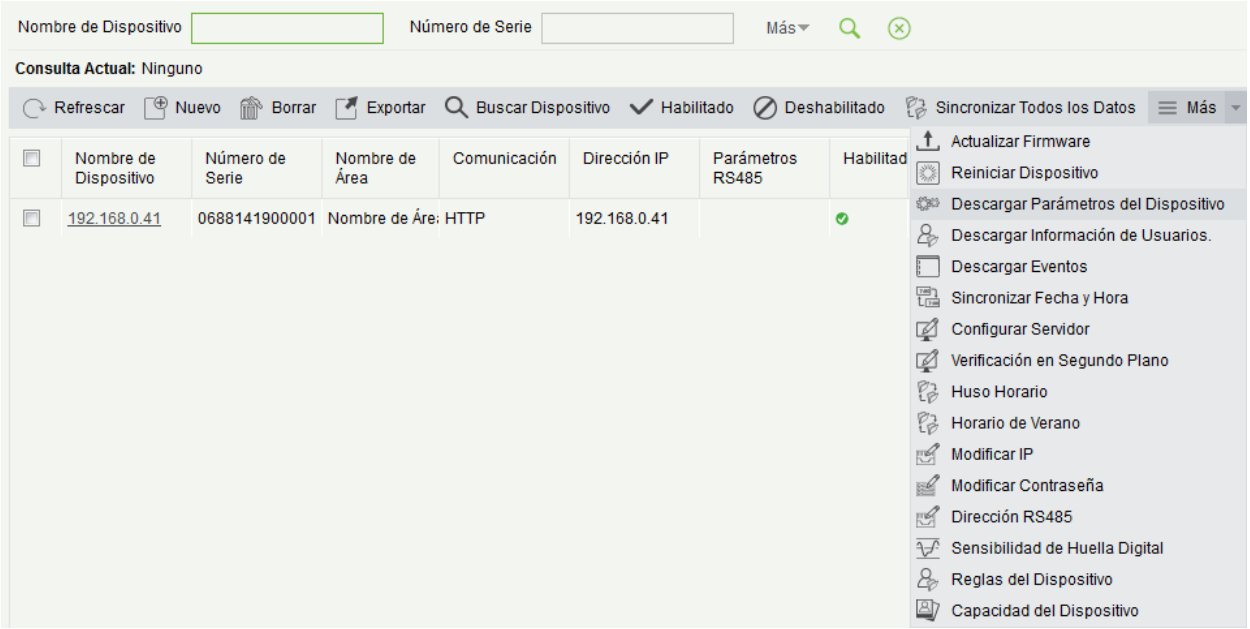
✍**Nota**: Al agregar un dispositivo utilizando alguno de los tres métodos anteriores, si existen datos inconsistentes en alguno de los equipos, sincronice la información dando clic en [Dispositivos] > [Sincronizar Datos a Todos los Equipos].

(5) La dirección IP por defecto del dispositivo pudiera tener conflicto con algún otro dispositivo en la red. En este caso puede modificar la dirección IP dando clic en [Modificar IP]. Introduzca la nueva dirección IP y los otros parámetros (Nota: Configure el Gateway y la IP en el mismo segmento de red).

✍**Nota:** Algunos dispositivos PUSH suportan SSL. Para usar esta función, seleccione el puerto HTTPS durante la instalación del software y asegure que el firmware del dispositivo soporta SSL.

4.1.2 Operaciones del Dispositivo

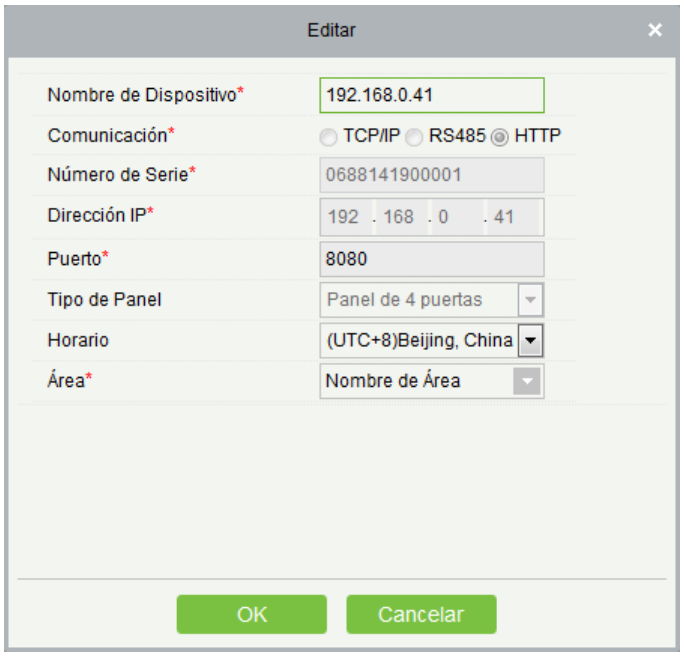
Para la comunicación entre el sistema y el dispositivo, carga y descarga de datos, sincronizar fecha y hora, ajustar parámetros, entre otras. Los usuarios pueden editar, agregar y borrar dispositivos de acuerdo a sus privilegios en el sistema.



- Editar o Borrar un Dispositivo

Editar: De clic en el nombre del dispositivo, o en [Editar] debajo de operaciones para abrir la interfaz de editar.

Borrar: Seleccione el dispositivo, de clic en [Borrar] y luego [OK] para borrar el dispositivo.



Para la configuración y mayor información de los parámetros mostrados anteriormente, consulte los respectivos capítulos. Los objetos mostrados en gris no son editables. El nombre de cada dispositivo debe ser único.

El tipo de panel de acceso no puede ser modificado. Si el tipo es incorrecto, deberá eliminar el dispositivo y agregarlo manualmente de nuevo.

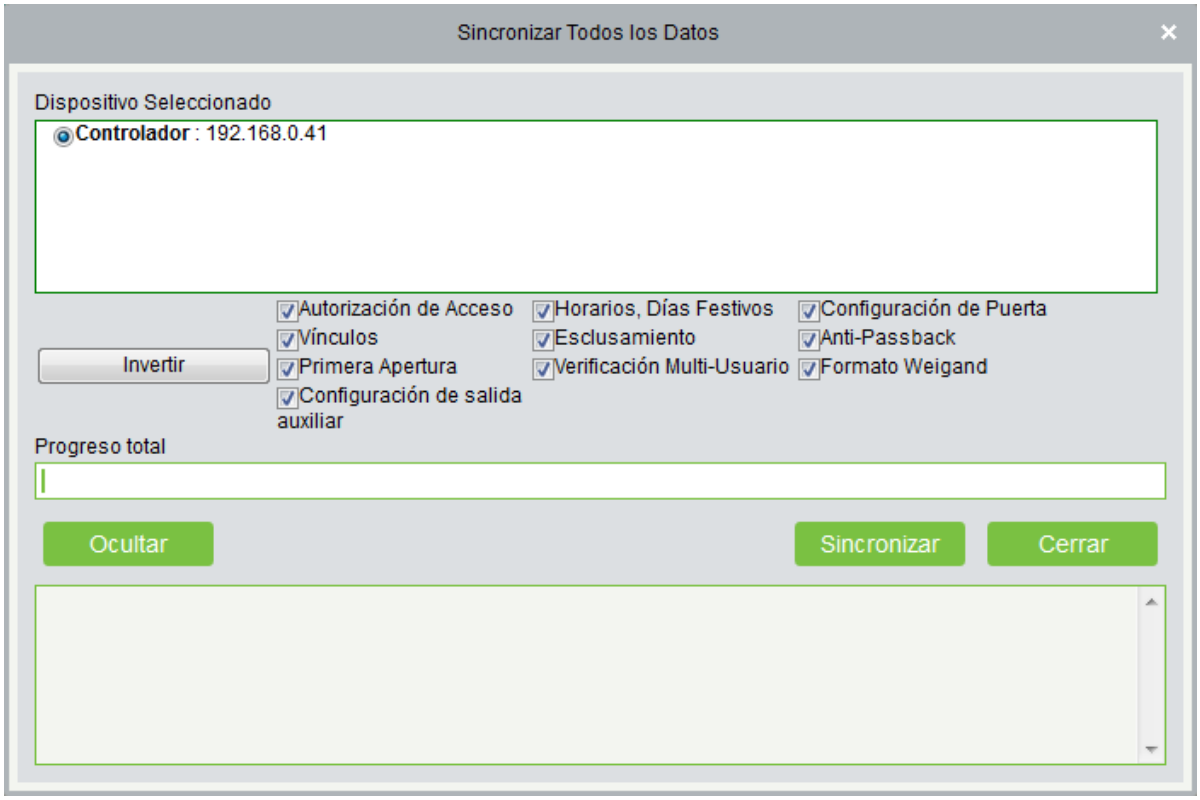
- Deshabilitar/Habilitar

Seleccione el dispositivo y de clic en [Deshabilitar/Habilitar] en la parte superior para iniciar o detener el uso del dispositivo.

Cuando la comunicación entre el dispositivo y el sistema es interrumpida o existe alguna falla, el dispositivo se mostrará deshabilitado automáticamente. Después de solucionar el problema en la red o el dispositivo, de clic en [Habilitar] para reconectar el dispositivo y restablecer la comunicación.

- Sincronizar Datos a los Dispositivos

Para sincronizar los datos del sistema al dispositivo, seleccione el dispositivo y de clic en [Sincronizar Datos al Dispositivo] y de clic en [OK] para realizar la sincronización.



✍**Nota:** [Sincronizar Datos al Dispositivo] primero borrará los datos del dispositivo (excepto los eventos) y descargará los datos y configuraciones de nuevo. Al realizar esta operación, mantenga la conexión de red estable y evite el corte de energía. Si el dispositivo está trabajando normalmente utilice esta función con precaución. Use esta función solo cuando sea necesario.

- Actualizar Firmware

Seleccione el dispositivo que requiera actualizar y de clic en [Actualizar Firmware] para abrir la interfaz y de clic en [Examinar] para seleccionar el archivo de actualización (llamado emfw.cfg) y de clic en [OK] para iniciar la actualización.

✍**Nota:** El usuario no debe actualizar el firmware sin previa consulta. Contacte con su distribuidor antes de realizar la actualización para recibir indicaciones. Realizar actualizaciones sin consultar puede generar problemas y afectar el uso normal del dispositivo.

- Reiniciar Dispositivo

Reiniciará el dispositivo seleccionado.

- Descargar Parámetros del Dispositivo

Descargará los parámetros comunes del dispositivo. Por ejemplo, la versión del firmware después de actualizar el dispositivo.

- Descargar Información de Usuarios

Refresca el número de usuarios actual y las huellas digitales del dispositivo. El valor final se mostrará en la lista de dispositivos.

- Descargar Eventos

Descarga los eventos del dispositivo al sistema. Se muestran dos opciones para esta operación: Descargar Eventos Nuevos y Descargar Todos los Eventos.

Descargar Eventos Nuevos: El sistema solo descargará los eventos nuevos desde la última vez que se descargaron eventos y se guardaron en la base de datos. Los datos repetidos no se rescriben.

Descargar Todos los Eventos: El sistema descargará todos los eventos. Los datos repetidos no se rescriben.

Cuando el estado de la red y la comunicación entre el dispositivo es normal, el sistema obtendrá los eventos del dispositivo en tiempo real y los guardará en la base de datos. Sin embargo, cuando la comunicación es interrumpida por alguna razón y los eventos no pueden ser obtenidos en tiempo real, puede usar la función [Descargar Eventos] para obtener los eventos del dispositivo manualmente. Además, el sistema, por defecto, intentará descargar los eventos de los dispositivos diariamente de manera automática a las 00:00.

✍Nota: Los paneles de acceso pueden almacenar hasta 100mil eventos. Cuando los eventos exceden este número, el dispositivo eliminará los eventos más antiguos (elimina 10mil eventos por defecto).

- Sincronizar Fecha y Hora

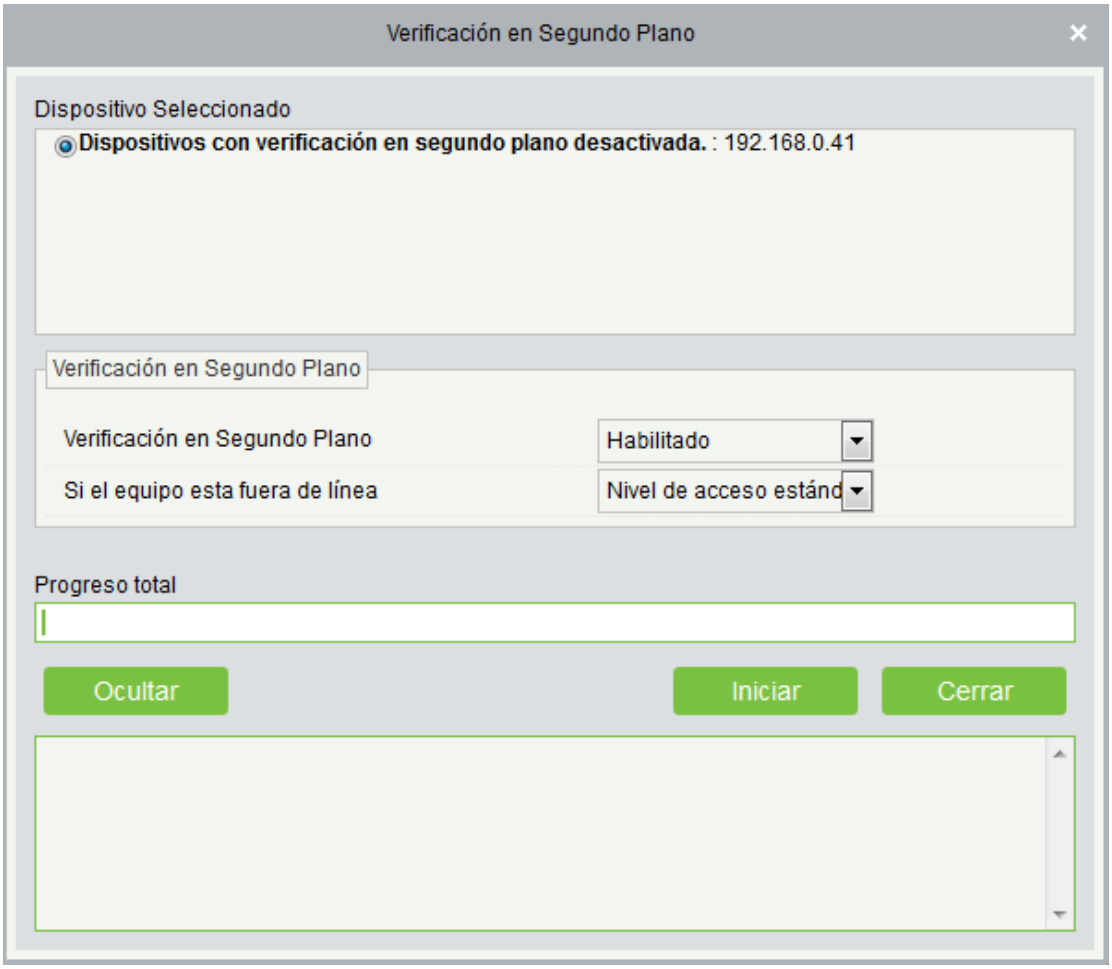
Sincroniza la fecha y hora del dispositivo conforme a la fecha y hora del servidor.

- Configurar Servidor

Configuración de parámetros del dispositivo conectado al servidor.

- Verificación en Segundo Plano

(1) Seleccione el dispositivo que estará en línea y de clic en [Más] > [Verificación en Segundo Plano]:



Verificación en Segundo Plano: Activa o desactiva la función de verificación en segundo plano.

Si el dispositivo está fuera de línea: Si el dispositivo está fuera de línea podrá seleccionar: Niveles de Acceso Estándar o Denegar Acceso.

(2) Después de configurar, de clic en [Iniciar] para cargar los parámetros de verificación en segundo plano.

✍**Nota:** Si requiere utilizar las funciones avanzadas de control de acceso, active la Verificación en Segundo Plano y cargue los parámetros al dispositivo.

- Huso Horario

Si el dispositivo soporta la función de huso horario y no está en el mismo huso horario que el servidor, es necesario establecer el huso horario del dispositivo. Después de configurarse, el dispositivo sincronizará el tiempo automáticamente según el huso horario y la hora del servidor.

- Horario de Verano

Establezca el horario de verano según los requerimientos de cada región.

- Modificar IP

Seleccione el dispositivo y de clic en [Modificar IP] para mostrar la interfaz de modificación. Se obtendrán los datos del dispositivo como IP, máscara de subred y Gateway (si no se pueden obtener los datos la IP no se podrá modificar). Introduzca la nueva IP, mascara de subred y Gateway. De clic en [OK] para guardar los cambios y salir.

Esta función es la misma que [Modificar Dirección IP] en Dispositivos. La diferencia entre ambas es que una función se realiza con los equipos que ya han sido agregados al sistema y la otra con los equipos que no han sido agregados al sistema todavía.

- Modificar Contraseña de Comunicación

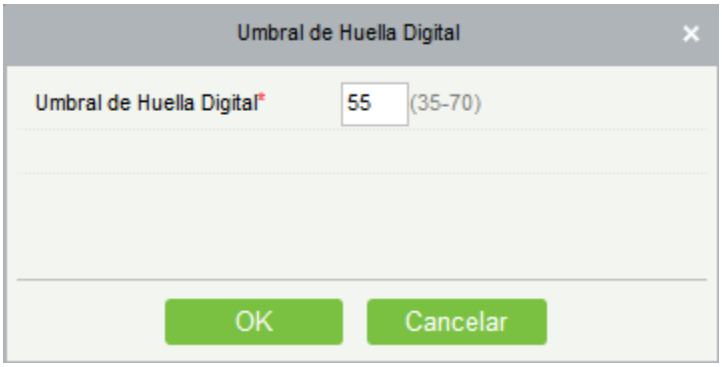
Introduzca la contraseña antigua antes de realizar la modificación. Después de la verificación introduzca la contraseña nueva dos veces y de clic en [OK] para modificar la contraseña de comunicación.

✍**Nota:** La contraseña de comunicación no puede contener espacios; es recomendado usar la combinación de números y letras para incrementar el nivel de seguridad del dispositivo. Es recomendado establecer la contraseña de comunicación para cada dispositivo.

- Modificar Dirección RS485

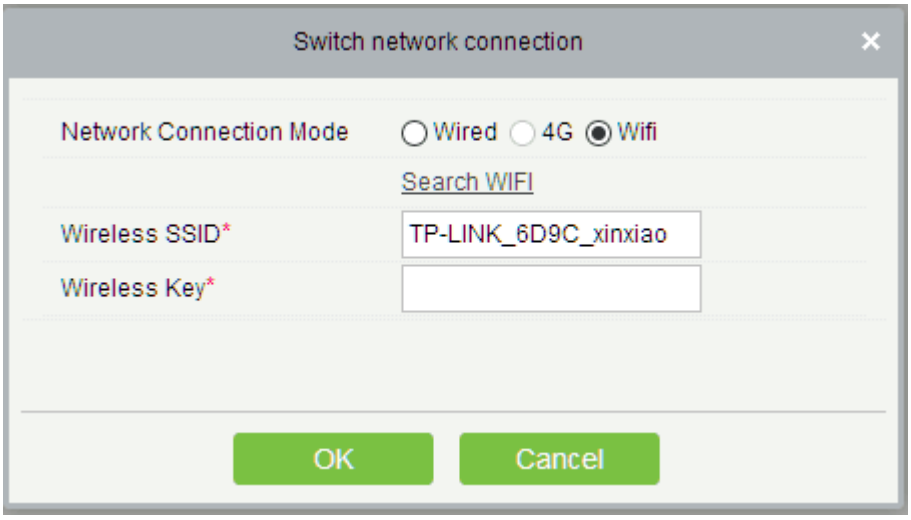
Solo se puede modificar la dirección RS485 a los equipos que no cuentan con DIP Switch.

- Sensibilidad de Huella Digital (Para equipos con función de huella digital)



El usuario puede ajustar la sensibilidad de identificación de huella digital en el dispositivo en una escala de 35 a 70, siendo 55 por defecto. Al agregar el dispositivo, el sistema obtendrá el dato de sensibilidad. El usuario puede ver el nivel de sensibilidad desde la lista de dispositivos. Realizar la operación por lote es permitido.

- Cambiar Conexión de Red



Esta función aplica para la serie de controladores de acceso InBio5, la cual es usada para cambiar el tipo de

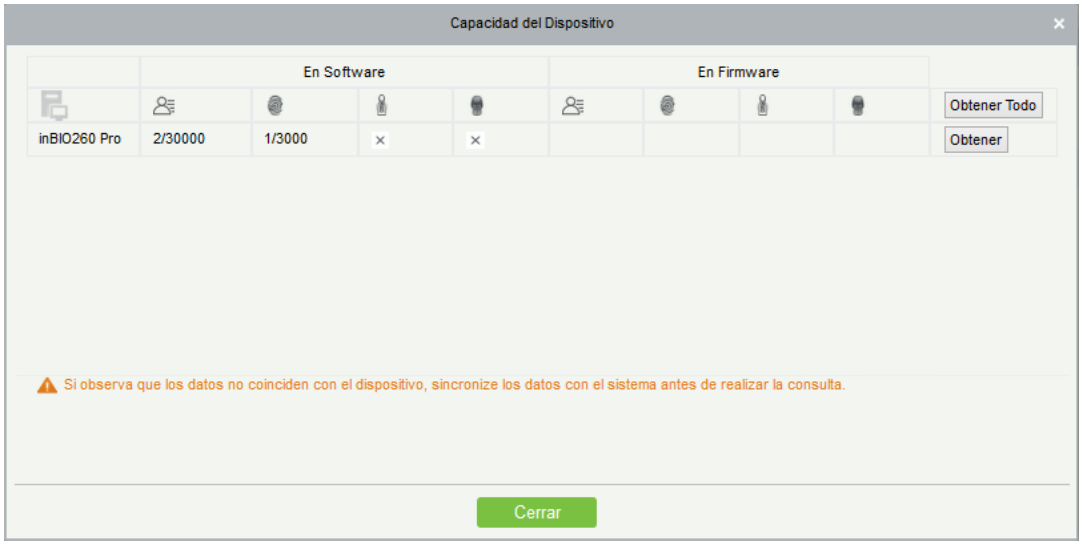
conexión de red del panel.

Reglas del Dispositivo

Se muestran las reglas de acceso del dispositivo.

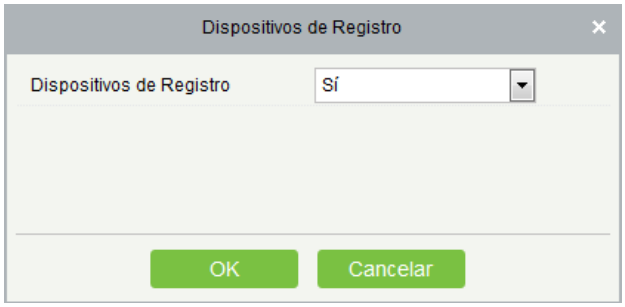
Capacidad del Dispositivo

Comprueba la capacidad de huellas digitales del dispositivo.



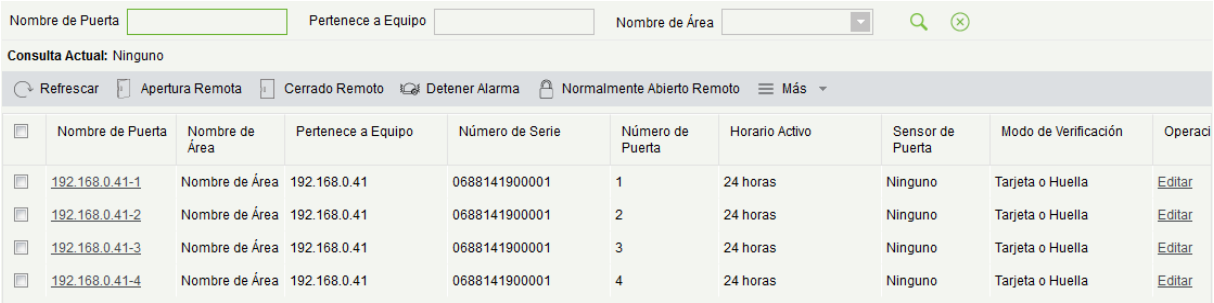
Establecer Dispositivo de Registro

Solo cuando se establece una terminal standalone como dispositivo de registro puede cargar los datos de los usuarios automáticamente.



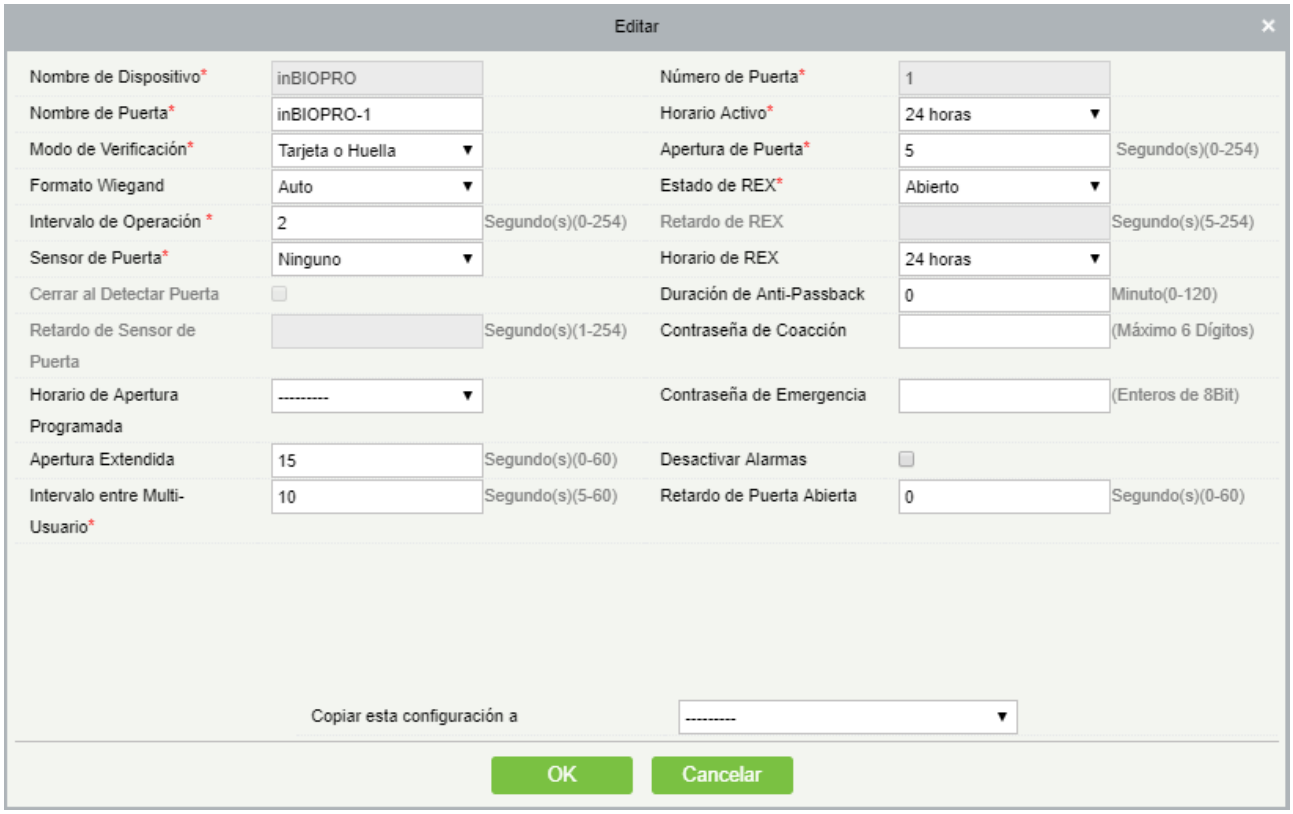
4.1.3 Puertas

1. De clic en [Dispositivos de Acceso] > [Dispositivos] > [Puertas] para acceder a la interfaz de gestión de puertas (de clic en el "Nombre de Área" y el sistema filtrará automáticamente mostrando solo los dispositivos del área seleccionada).



- Configuración de Parámetros de Puertas:

Seleccione la puerta que será configurada y de clic en el nombre de la puerta o en botón de [Editar] debajo de operaciones para mostrar la interfaz de Editar:



Descripción de los campos:

Nombre del Dispositivo: No es editable.

Número de Puerta: El sistema nombra las puertas automáticamente según la cantidad de puertas del dispositivo. Este número será relacionado con el número de puerta del equipo.

✍**Nota:** En la configuración de anti-passback y esclusamiento hace referencia al número de puerta en vez del número en el nombre de la puerta y no necesariamente están relacionados.

Nombre de Puerta: Está compuesto: "nombre de la puerta-número de puerta". El campo permite al usuario modificar el nombre hasta un máximo de 30 caracteres.

Horario Activo, Horario de Apertura Programada: Por defecto se asigna el horario de 24 horas. El Horario de Apertura Programada debe establecerse dentro del Horario Activo.

✍**Nota:** Cuando una puerta se encuentra en estado normalmente abierto y un usuario con nivel de acceso para la puerta realiza la verificación correcta en 5 ocasiones consecutivas (con intervalo de 5 segundos) puede liberar el estado de normalmente abierto y cerrar la puerta. La próxima verificación será una verificación normal y esta función solo será efectiva durante el horario de puerta activa. Otros intervalos de normalmente abierto y/o primer apertura normalmente abierta configurados el mismo día perderán efecto.

Apertura de Puerta: Retardo de tiempo para la apertura de la puerta después de una verificación. La unidad son segundos con un rango de 0 a 254 y un tiempo por defecto de 5 segundos.

Intervalo de Operación: Intervalo entre dos verificaciones. La unidad son segundos con un rango de 0 a 254 y un tiempo por defecto de 2 segundos.

Duración de Anti-Passback: Solo una entrada es permitida con un lector en esta duración. La unidad son minutos con un rango de 0 a 120 y un tiempo por defecto de 0 minutos.

Sensor de Puerta: Ninguno (sin sensor de puerta), Normalmente Abierto, Normalmente Cerrado. El defecto es ninguno. Al seleccionar normalmente abierto o normalmente cerrado, debe establecer el tiempo sensor de puerta y si desea cerrar al detectar la puerta, siendo el tiempo por defecto de 15 segundos y cerrar al detectar puerta deshabilitado.

Retardo de Sensor de Puerta: Es el tiempo de detección después de que la puerta es abierta. Cuando la puerta no está en un periodo de normalmente abierto y la puerta es abierta, el dispositivo comenzará a contar el tiempo y activará una alarma si retardo de tiempo ha expirado y detendrá la alarma al cerrar la puerta. El retardo de sensor de puerta es de 15s con un rango de 1 a 254 segundos. El retardo sensor de puerta debe ser mayor que la duración de apertura de puerta.

Cerrar al Detectar Puerta: Bloquea la cerradura al detectar la puerta cerrada.

Modo de Verificación: Seleccione el modo de verificación que incluye tarjeta, huella, contraseña y combinaciones, siendo por defecto tarjeta o huella. Si selecciona tarjeta y contraseña, asegure que la puerta esté equipada con un lector con teclado.

Formato Wiegand**:** Seleccione el formato de tarjeta Wiegand que puede ser identificado por el lector Wiegand de la puerta. Si el formato es diferente con respecto al formato configurado la puerta no podrá ser abierta. El software incluye 9 formatos, siendo por defecto el automático que realiza la comparación automática. (Excepto para el formato de tarjeta con a, b o c).

Estado de REX: Cerrado indica que la cerradura será bloqueada después de presionar el botón de salida. Abierto (por defecto) indica que la cerradura será desbloqueada después de presionar el botón de salida.
Retardo de REX (Modo de REX): Indica el retardo de tiempo de alarma para la detección de la puerta después de que el botón de salida es bloqueado. Cuando la puerta es abierta forzadamente, el sistema detecta el estado de la puerta después de un periodo de tiempo. El valor defecto es 10s y el rango es de 1 a 254 segundos. El botón de salida tiene que estar bloqueado antes de configurar esta opción.

Horario de REX: El botón de salida estará disponible solo en el horario especificado.

Duración de la Entrada: Basado en el tiempo de duración de la apertura de la cerradura, el retardo de sensor de puerta y el retardo de salida, la duración de la entrada es el límite de tiempo extra. Para usar esta función, es necesario marcar la opción [Apertura Extendida] al agregar o editar personal. Puede usar esta función para extender el tiempo para personas con alguna discapacidad física.

Retardo de Apertura de Puerta: Periodo de tiempo para completar la verificación para abrir la puerta. El rango es de 1 a 60 segundos.

Tiempo de Retardo de Intervalo: Periodo de tiempo durante la verificación entre 2 usuarios ya sea con tarjeta o con huella digital. El rango es de 1 a 60 segundos.

Contraseña de Coacción / Contraseña de Emergencia: En caso de coacción, utilice una contraseña para abrir la puerta, generando una alerta en el software. En caso de emergencia, utilice una contraseña (llamada Super Contraseña) para abrir la puerta, siendo efectiva en cualquier horario y cualquier modo de verificación, normalmente usado por el administrador.

- ✧ Contraseña de coacción (con tarjeta): La contraseña no debe exceder de 6 dígitos. Cuando se configura el modo de verificación de Solo Tarjeta deberá presionar primero el botón ESC en el teclado seguido de la contraseña y el botón [OK] y finalmente presentar la tarjeta. La puerta se abrirá normalmente y se generará una alerta en el software. Cuando se usa la verificación Tarjeta + Contraseña, primero presente la tarjeta

seguido de la contraseña y el botón [OK] (igual que una apertura normal en una verificación tarjeta + contraseña). La puerta se abrirá y genera la alerta.

- Contraseña de Emergencia: La contraseña debe ser de 8 dígitos. Presione la tecla [ESC] antes de introducir la contraseña seguida de la tecla [OK] para ejecutar.

Cuando se utiliza la contraseña de coacción o emergencia, el intervalo para introducir cada número no debe exceder de 10 segundos y las dos contraseñas no deben ser iguales.

Desactivar Alarmas: marque la casilla para desactivar las notificaciones de alarma en la interfaz de monitoreo en tiempo real.

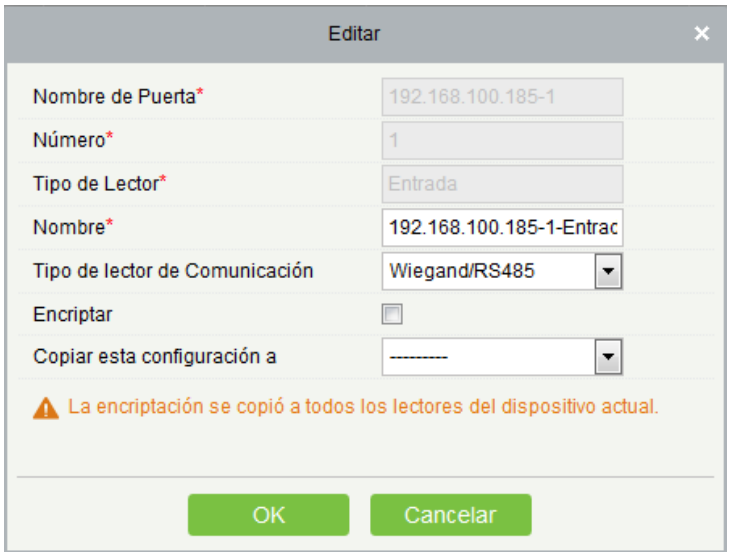
Copiar esta configuración a: Se muestran dos opciones:

- Todas las puertas de este dispositivo: Copia los parámetros a las puertas del dispositivo actual.
- Todas las puertas de todos los dispositivos: Copia los parámetros a todos los dispositivos del nivel del usuario actual.

2. Después de editar los parámetros, de clic en [OK] para guardar y salir.

4.1.4 Lectores

1. De clic en [Dispositivos de Acceso] > [Lectores], seleccione un lector y de clic en [Editar]:



Nombre: El nombre del lector que se muestra en la página de la lista.

Tipo de Comunicación del Lector: Están disponibles las opciones Wiegand/RS485, Wiegand, RS485 y deshabilitado. Cuando se selecciona un tipo de comunicación, la interfaz del dispositivo solo recibirá datos del tipo especificado (incluyendo tarjetas y huellas).

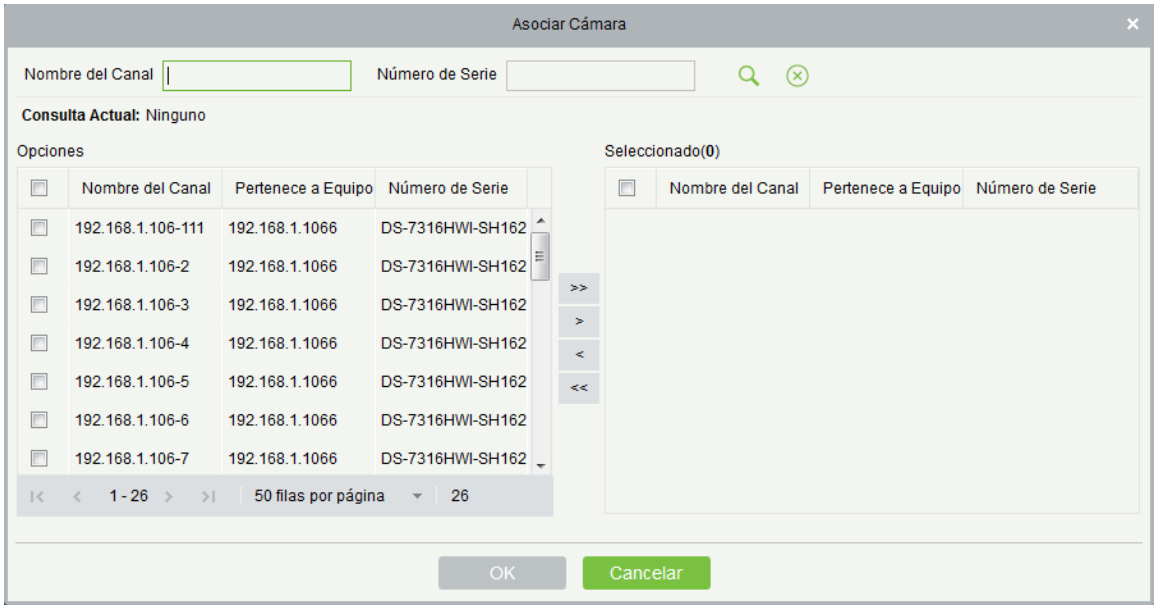
Encriptar: Si habilita ésta opción, el dispositivo solo podrá usar lectores encriptados tales como el SF10 y el FR1300.

- Asociar / Desasociar Cámara

Se realiza la asociación del lector con la cámara para establecer vínculos y poder generar pop up de video, grabar

video o capturar una imagen cuando ocurra un evento específico.

De clic en [Asociar/Desasociar Cámara] para seleccionar uno o varios canales:



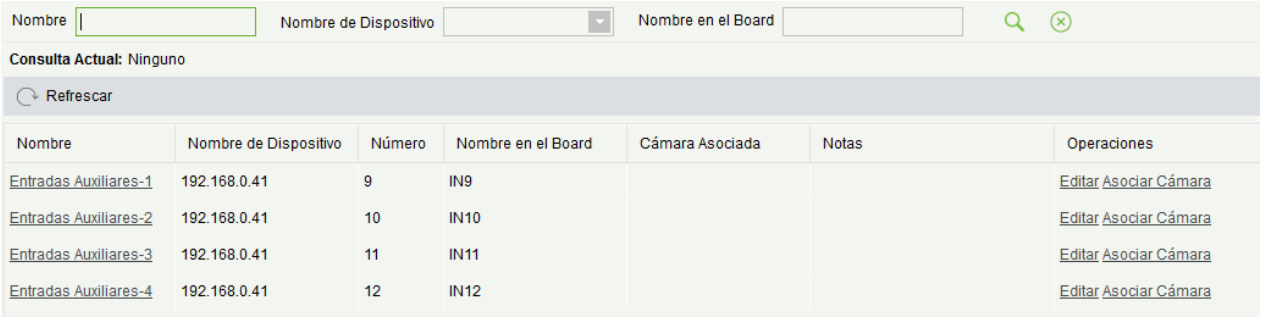
De clic en [OK] para guardar y salir.

✍Nota: Un lector se puede asociar con más de un canal de video.

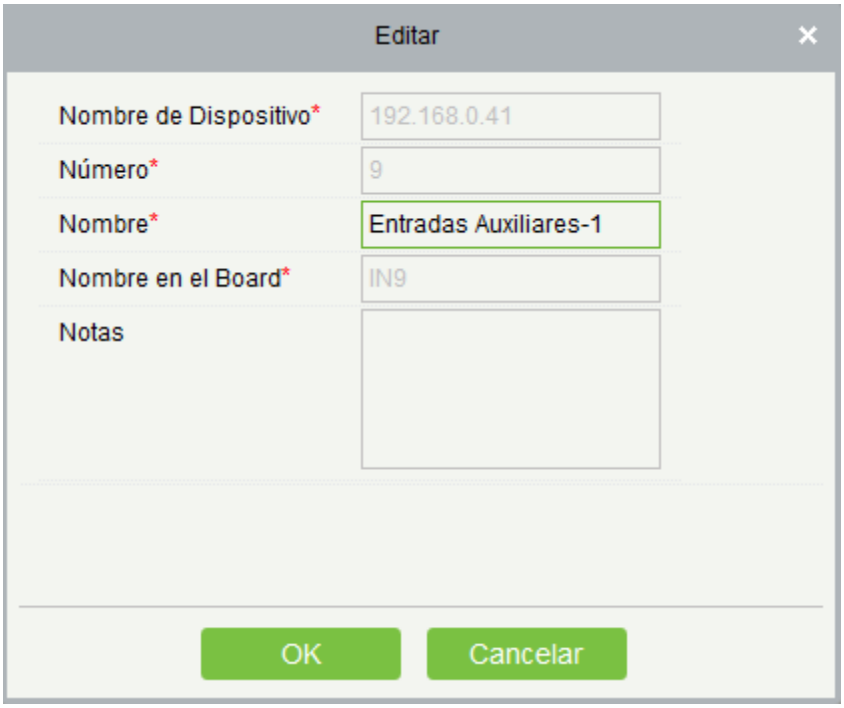
4.1.5 Entradas Auxiliares

Se utilizan principalmente para conectar dispositivos, como sensores infrarrojos o sensores de humo.

1. De clic en [Dispositivos de Acceso] > [Entradas Auxiliares], accederá a la siguiente interfaz:



2. De clic en [Editar] para modificar los parámetros:



Descripción de los campos:

Nombre: Puede editar el nombre.

Nombre en el Board: El nombre como se muestra en el hardware, por ejemplo, IN5.

3. De clic en [Editar] para modificar el nombre y las notas. Otros campos no se pueden editar aquí.

- Asociar / Desasociar Cámara

Se realiza la asociación con la cámara para establecer vínculos y poder generar pop up de video, grabar video o capturar una imagen cuando ocurra un evento específico. Para más información consulte Lectores: Asociar / Desasociar Cámara.

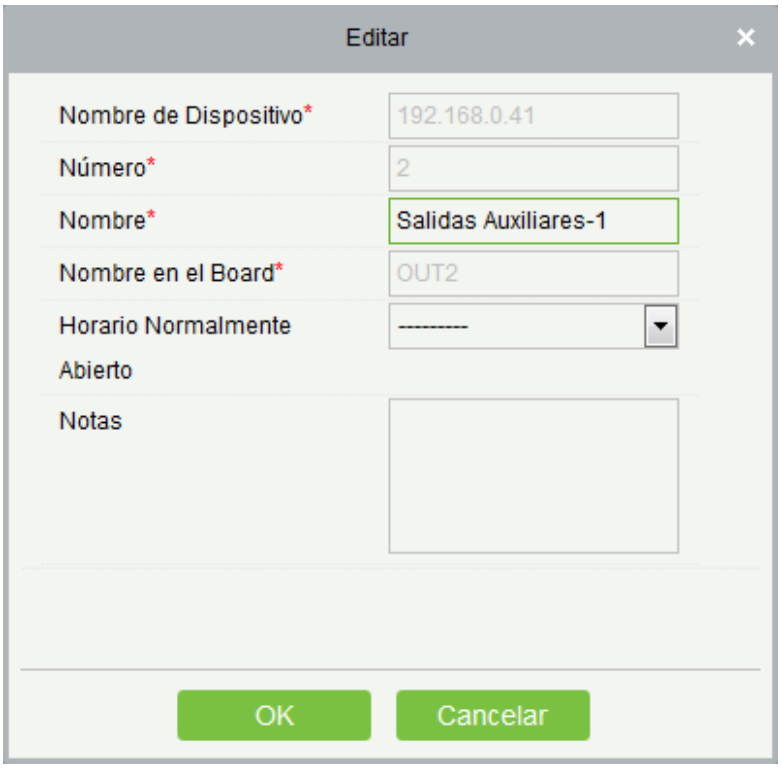
✍Nota: Una entrada auxiliar se puede asociar con más de un canal de video.

4.1.6 Salidas Auxiliares

Utilizadas para generar vínculos, principalmente relacionados con alarmas.

1. De clic en [Dispositivos de Acceso] > [Salidas Auxiliares] para acceder a la siguiente interfaz:

2. De clic en [Editar] para modificar los parámetros:



Descripción de los campos:

Nombre: Puede editar el nombre.

Nombre en el Board: El nombre como se muestra en el hardware, por ejemplo, OUT2.

Horario Normalmente Abierto: La salida auxiliar será normalmente abierta durante este horario.

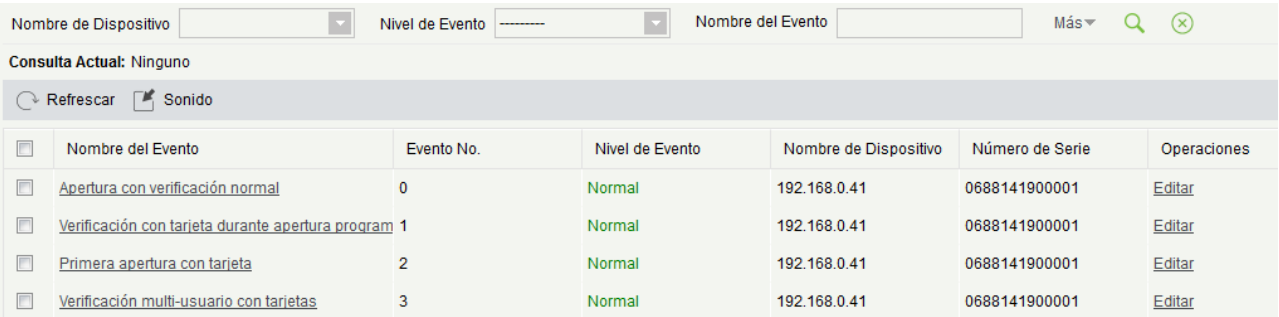
✍Nota: Solo los campos de Nombre, Horario de Apertura Programada y notas pueden ser modificados.

3. De clic en [Editar] para modificar el nombre y las notas. Otros campos no se pueden editar aquí.

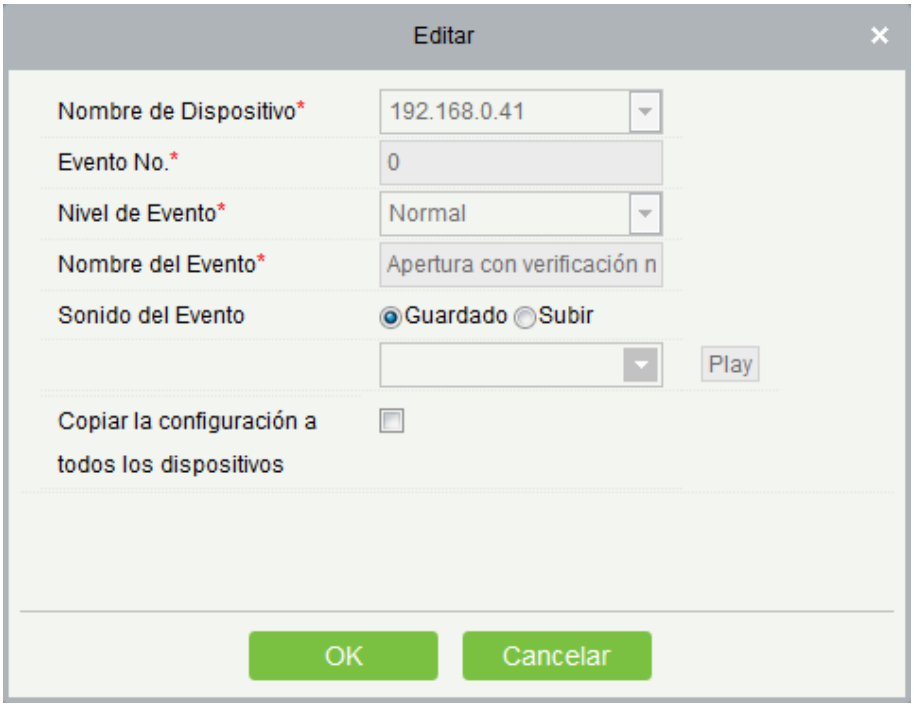
4.1.7 Tipo de Evento

Muestra los tipos de eventos de los dispositivos de acceso.

1. De clic en [Dispositivos de Acceso] > [Tipo de Evento] para acceder a la siguiente interfaz:



2. De clic en [Editar] o de clic en el nombre del evento para editar:



Descripción de los campos:

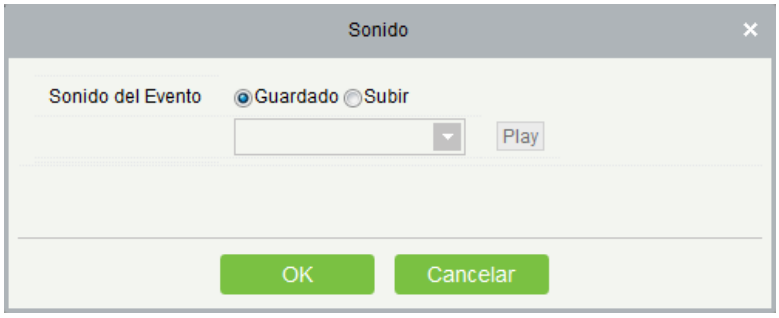
Nivel del Evento: Se muestra Normal, Excepción y Alarma,

Nombre del Evento: No es posible editar el nombre.

Sonido del Evento: Seleccione un sonido personalizado para reproducir durante el monitoreo en tiempo real.

Copiar la configuración a todos los dispositivos: Se copian los parámetros de los eventos a todos los dispositivos.

Sonido: Igual que Sonido del Evento. De clic en [Sonido]:



Puede subir un sonido del disco local de formato wav o mp3 menor de 10Mb.

Para más detalles sobre Tipo de Evento, consulte Tipo de Evento de Acceso.

4.1.8 Horario de Verano

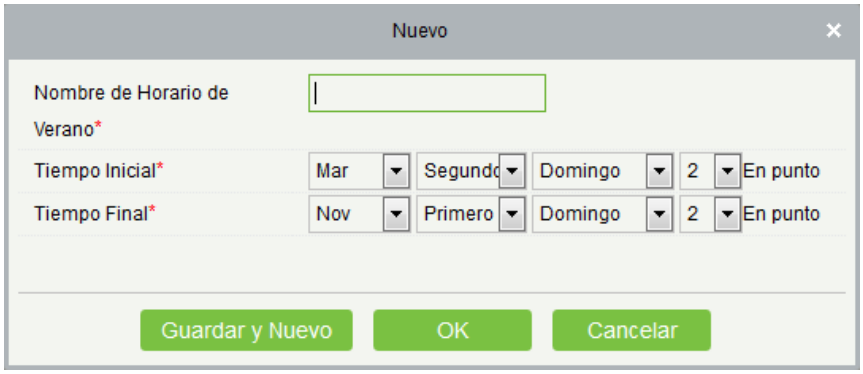
El Horario de Verano, es un sistema para prescribir la hora local con el fin de ahorrar energía. El tiempo unificado adoptado para el sistema es llamado Horario de Verano o DST. Usualmente, el tiempo será una hora adelante en el verano. Las reglas son diferentes en cada país. Actualmente, casi 110 países adoptan el horario de verano.

Para satisfacer el requerimiento de horario de verano, es posible personalizar una opción especial para adelantar

una hora en un día y hora específico (XX hora, XX día, XX mes) y atrasar una hora en un día y hora específico si es necesario.

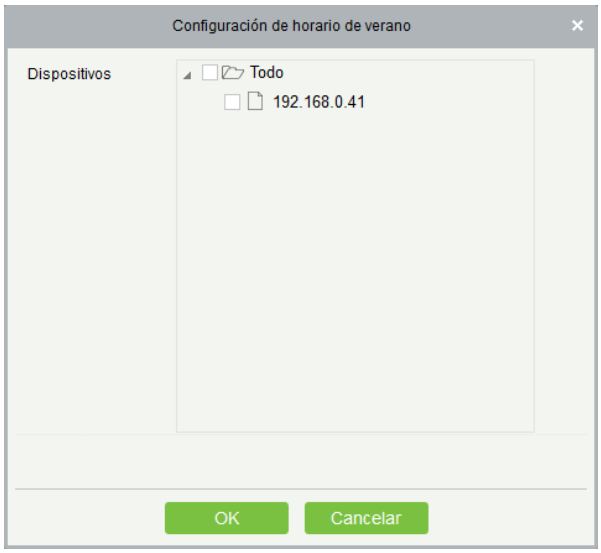
- Agregar Horario de Verano

1. De clic en [Dispositivos de Acceso] > [Horario de Verano] > [Nuevo]:



El formato se establece como "Mes-Número-Día-Hora". Se debe introducir el tiempo inicial y final. Por ejemplo, el tiempo inicial puede ser "Segundo Lunes de Marzo a las 00:00". Cuando llegue esta hora, el sistema adelantará una hora y cuando llegue el tiempo final se atrasará una hora.

- Aplicar Horario de Verano



El usuario puede habilitar o aplicar el horario de verano en un dispositivo: En la interfaz de horario de verano, seleccione uno de los horarios y de clic en [Aplicar Horario de Verano], seleccione los dispositivos y de clic en [OK] para confirmar.

✍ Nota:

1) Si un horario de verano se encuentra en uso no puede ser eliminado. Detenga el uso para eliminar.

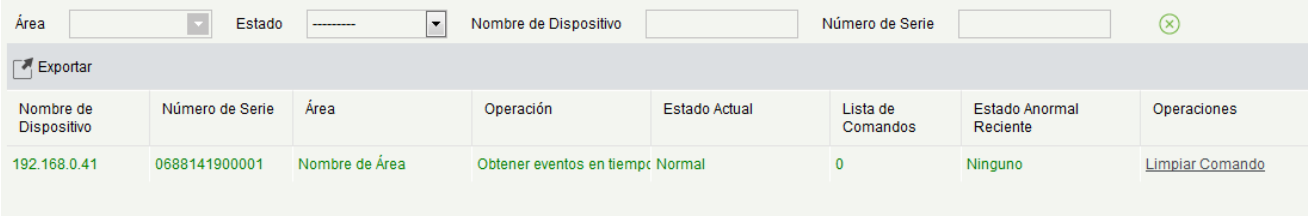
2) Si un horario de verano se encuentra en uso, se enviará la última modificación al dispositivo. Si se interrumpe la comunicación se continuará la transmisión en la siguiente conexión.

3) En el módulo de gestión de puertas del sistema de control de acceso es posible habilitar o deshabilitar la función

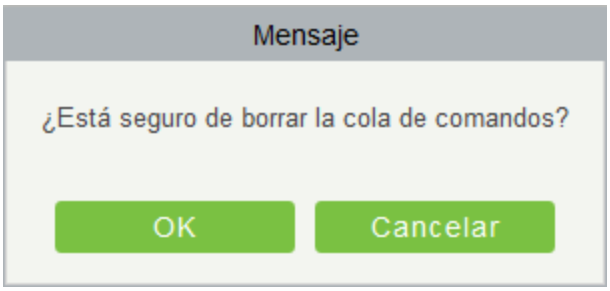
de horario de verano. Si habilita la función, cuando llegue el tiempo inicial, el sistema adelantará una hora. Cuando llegue el tiempo final el sistema atrasará una hora a la hora original. Si no se ha establecido un horario de verano en el dispositivo, al deshabilitarlo se mostrará el mensaje "No se ha configurado horario de verano en este dispositivo".

4.1.9 Monitoreo de Dispositivos

Por defecto se monitorea todos los dispositivos dentro del nivel actual del usuario. De clic en [Dispositivos de Acceso] > [Monitoreo de Dispositivos] y se mostrará la información y operaciones de los dispositivos: Nombre de Dispositivo, No. de Serie, Área, Operación, Estado Actual, Lista de Comandos y operaciones relacionadas.



Es posible limpiar la lista de comandos dando clic en [Limpiar Comando] en el dispositivo correspondiente:



De clic en [OK] para limpiar.

✍Nota:

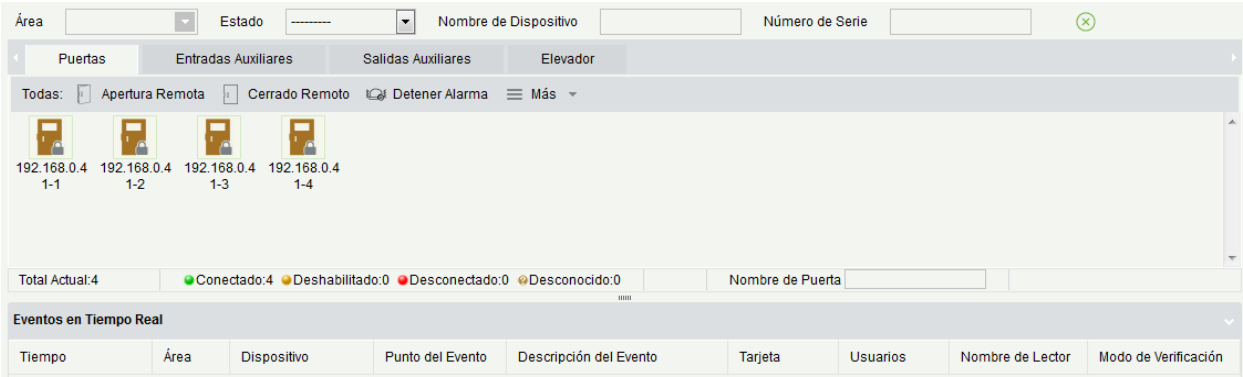
(1 Después de ejecutar Limpiar Comando, puede realizar Sincronizar Todos los Datos para volver a sincronizar la información del software a los dispositivos, pero esta operación no puede realizarse cuando la capacidad de usuarios y huellas digitales se encuentra al máximo en el equipo. Una vez que la capacidad es insuficiente, será necesario reemplazar el dispositivo actual por otro de mayor capacidad o eliminar el privilegio de acceso al dispositivo y después realizar la operación de Sincronizar Todos los Datos.

(2) Estado de Operación es el contenido de las comunicaciones del dispositivo actual, usado principalmente para depuración.

(3) Si el número de comandos para realizar es mayor de 0, esto indica que existen datos que no se han sincronizado con el dispositivo, en este caso, espere un momento.

4.1.10 Monitoreo en Tiempo Real

De clic en [Dispositivos de Acceso] > [Monitoreo en Tiempo] para monitorear el estado y los eventos en tiempo real de las puertas de los paneles de control de acceso, incluyendo eventos normales, anormales, alarmas, vínculos, etc. La interfaz de monitoreo en tiempo real se muestra a continuación:



Descripción de los estados de los íconos:

Íconos	Estado	Íconos	Estado
	Dispositivo deshabilitado		Puerta fuera de línea
/	Puerta sin sensor, Relevador cerrado /Estado sin relevador	/	Puerta sin sensor, Relevador abierto /Estado sin relevador
/	Estado en línea puerta cerrada, Relevador cerrado/ Edo. sin relevador	/	Estado en línea puerta cerrada, Relevador abierto/ Edo. sin relevador
/	Estado en línea puerta abierta, Relevador cerrado/ Edo. sin relevador	/	Estado en línea puerta abierta, Relevador abierto/ Edo. sin relevador
	Puerta abierta, con alarma, Relevador cerrado		Puerta abierta, con alarma, Relevador abierto
/	Tiempo de puerta abierta agotado, Relevador cerrado /Edo. sin Relevador, Sensor de puerta abierto	/	Tiempo de puerta abierta agotado, Relevador abierto /Edo. sin Relevador
	Tiempo de puerta abierta agotado, Relevador cerrado/ Sensor cerrado		Tiempo de puerta abierta agotado, Relevador abierto/ Sensor cerrado
/	Puerta cerrada, con alarma, Relevador cerrado/Edo. sin Relevador	/	Puerta cerrada, con alarma, Relevador abierto/Edo. sin Relevador
	Puerta sin sensor, con alarma, Relevador cerrado		Puerta sin sensor, con alarma, Relevador abierto
	Tiempo de espera agotado, sin Relevador/Sensor de puerta cerrado		Puerta bloqueada

✍Nota: "Estado sin Relevador" indica que el firmware del dispositivo no soporta la detección del estado del relevador.

1. Puerta

- Monitorear Todos

Por defecto la página de inicio muestra todas las puertas de los paneles del nivel del usuario. El usuario puede monitorear una o varias puertas estableciendo el Área, Panel de Acceso o Puerta.

Apertura/Cerrado Remoto: controla una o todas las puertas. Para controlar una sola puerta, posicione el mouse sobre el ícono de la puerta y de clic en [Apertura/ Cerrado Remoto] en el cuadro de diálogo. Para controlar todas las puertas de clic directamente en [Apertura/ Cerrado Remoto] a un lado de "Todas".

En apertura remota, puede definir la duración de la apertura de la puerta (por defecto 15s). Puede seleccionar [Activar Horario de Apertura Programada] para habilitar la función o establecer la puerta en modo normalmente abierto y así la puerta no será limitada por ningún horario y se mantendrá abierta por 24 horas.

Para cerrar una puerta, primero seleccione [Desactivar Horario de Apertura Programada] para evitar que otros horarios normalmente abierto puedan abrir la puerta y luego seleccione [Cerrado Remoto].

✍**Nota:** Si [Apertura/ Cerrado Remoto] falla, revise la conexión de red y que los dispositivos estén en línea.

Detener la Alarma: Cuando se muestra una puerta con alarma en la interfaz, el sonido permanecerá sonando hasta que se detenga la alarma. Esta operación puede realizarse para una puerta o todas las puertas. Para una puerta posicione el mouse en el ícono de la puerta y de clic en [Detener Alarma]. Para todas las puertas, de clic en [Detener todas las Alarmas]. Si la operación es exitosa, la alarma se detendrá automáticamente.

✍**Nota:** Si [Detener la Alarma] falla, revise la conexión de red y que los dispositivos estén en línea.

Normalmente Abierto Remoto: Establece la puerta en normalmente abierto.

Activar Bloqueo: Establece la puerta en un estado de bloqueo. En ese estado, la puerta no recibirá ninguna operación tal como lectura de tarjeta u operaciones remotas. Esta función solo es soportada por ciertos dispositivos.
Desactivar Bloqueo: Desbloquea una puerta bloqueada. Esta función solo es soportada por ciertos dispositivos.
Mostrar Fotos: Si está activado se mostrará la foto registrada del usuario al ocurrir una verificación correcta (si no tiene foto registrada, se muestra la imagen defecto). También se muestra el nombre del evento, fecha, hora y nombre.

Reproducir Audio: Si está activado, reproduce un sonido al ocurrir un evento de alarma.

- Gestión Rápida de Puertas

Mueva el cursor encima del ícono de la puerta y se mostrarán las operaciones que puede realizar. Puede consultar los eventos más recientes de la puerta.

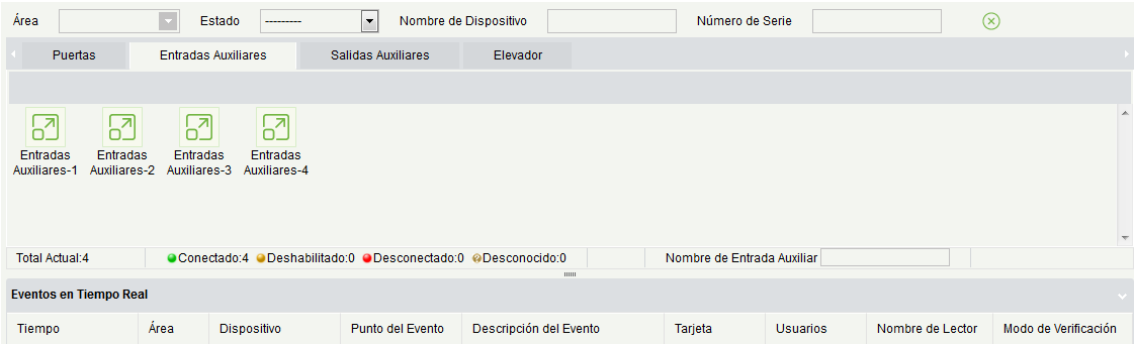
Consultar los Últimos Eventos: De clic para consultar rápidamente los últimos eventos de la puerta.

- Monitoreo de Eventos

El sistema obtiene automáticamente los eventos de los dispositivos (por defecto muestra 200 eventos), incluyendo eventos de acceso normales y anormales (incluyendo alarmas). Los eventos normales se muestran en color verde, los eventos de alarma en rojo y otros eventos anormales en naranja.

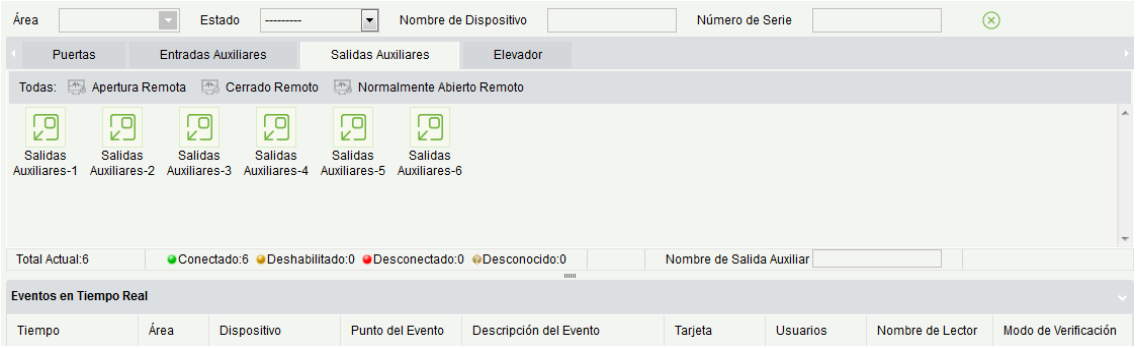
2. Entradas Auxiliares

Monitorea en tiempo real los eventos de las entradas auxiliares.



3. Salidas Auxiliares

Puede realizar Apertura Remota, Cerrado Remoto y Normalmente Abierto Remoto.



4. Elevador

Sobre el monitoreo en tiempo real de elevador consulte Monitoreo en Tiempo Real.

4.1.11 Monitoreo de Alarmas

Monitorea los eventos de alarma de las puertas. Si una puerta envía una alarma y no se confirma, la página siempre mostrará los eventos de alarma.

Confirmar Alarma

Tiempo	Dispositivo	Punto del Evento	Descripción del Evento	Usuarios	Estado
2015-06-19 11:45:40	192.168.0.41		Desconectado		Ninguno

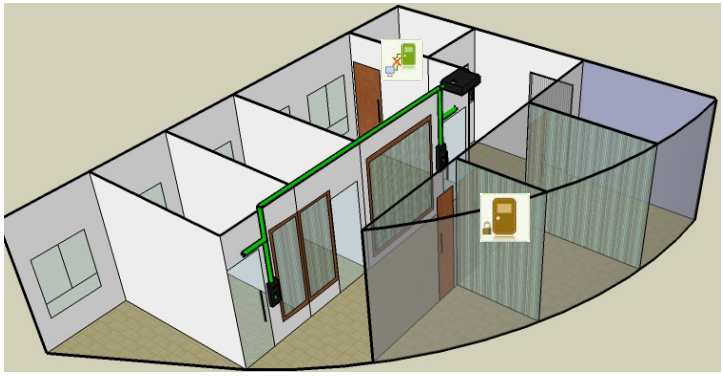
✍**Nota:** La descripción del tipo de alarma se mostrará sólo cuando es compatible con la versión del firmware del dispositivo, de lo contrario sólo se mostrará "alarma" sin mayor detalle.

Detener Alarma: Seleccione la puerta en estado de alarma y de clic en [Detener Alarma]. El sistema enviará un correo electrónico al monitorista de alarmas configurado en el sistema (el correo electrónico debe ser configurado en Parámetros)

✍**Nota:** Cuando una puerta tiene múltiples estados de alarma, solo mostrará la descripción de un tipo de alarma el orden descendente de gravedad. El orden se realiza así: alarma de tamper > alarma de coacción (contraseña + huella digital) > alarma de coacción con huella o contraseña > apertura de puerta inesperada > alarma de puerta mantenida abierta > alarma de dispositivo desconectado.

4.1.12 Mapa Virtual

Antes de usar mapa, primero de clic en [Dispositivos de Acceso] > [Mapa Virtual] > [Agregar] para agregar un mapa. Después de agregarlo, el usuario puede agregar puertas, acercar y alejar el mapa (incluyendo las puertas), etc. Si requiere cambiar la posición de los íconos en el mapa, de clic en [Guardar Posiciones] para guardar los cambios actuales.



Agregar / Borrar Mapa: Es posible agregar o borrar mapas como sea necesario.

Editar Mapa: Es posible editar el nombre del mapa, cambiar el mapa o el área al que pertenece.

Ajustar Mapa: Puede agregar una puerta al mapa o borrar una existente (de clic derecho sobre el ícono de la puerta y seleccione [Borrar Puerta], ajustar el mapa o la posición de la puerta o cámara (arrastrando el ícono) o ajustar el tamaño del mapa (clic en [Acercar] o [Alejar] o de clic en [Pantalla Completa]).

Operaciones de la Puerta: Mueva el cursor a una puerta y el sistema filtrará automáticamente y mostrará la operación de acuerdo al estado de la puerta. Puede abrir o cerrar remotamente, detener alarma, etc.

Control de niveles:

(1) En el proceso de agregar, los usuarios deben seleccionar el área correspondiente del mapa. El área es relevante a los niveles de acceso del usuario y solo podrá ver o gestionar el mapa dentro de los niveles. Si se modifica el área de pertenencia de un mapa, todas las puertas del mapa se borrarán y será necesario agregarlas manualmente otra vez.

(2) Cuando el administrador agrega un nuevo usuario, puede gestionar los privilegios de operación en la configuración de privilegios, tales como guardar posiciones, agregar puerta, agregar cámara, etc.

✍Notas:

(1) En la edición de mapa, es posible modificar el nombre del mapa, pero no la ruta, sólo necesita cancelar la selección antes de modificar la ruta.

(2) El sistema soporta agregar múltiples puertas al mismo tiempo. Después de agregar las puertas, es necesario fijar la posición de las puertas en el mapa y dar clic en [guardar].

(3) Al modificar el ícono de puerta, especialmente al alejar el mapa, el margen hacia arriba y hacia la izquierda no debe ser menor de 5 píxeles o el sistema mostrará el error.

(4) Se recomienda agregar un mapa menor de 1120 x 380 píxeles. Si acceden múltiples PC-clientes al servidor, se mostrará el mapa de diferente forma en cada uno según la resolución de pantalla y la configuración del navegador.

4.2 Gestión de Control de Acceso

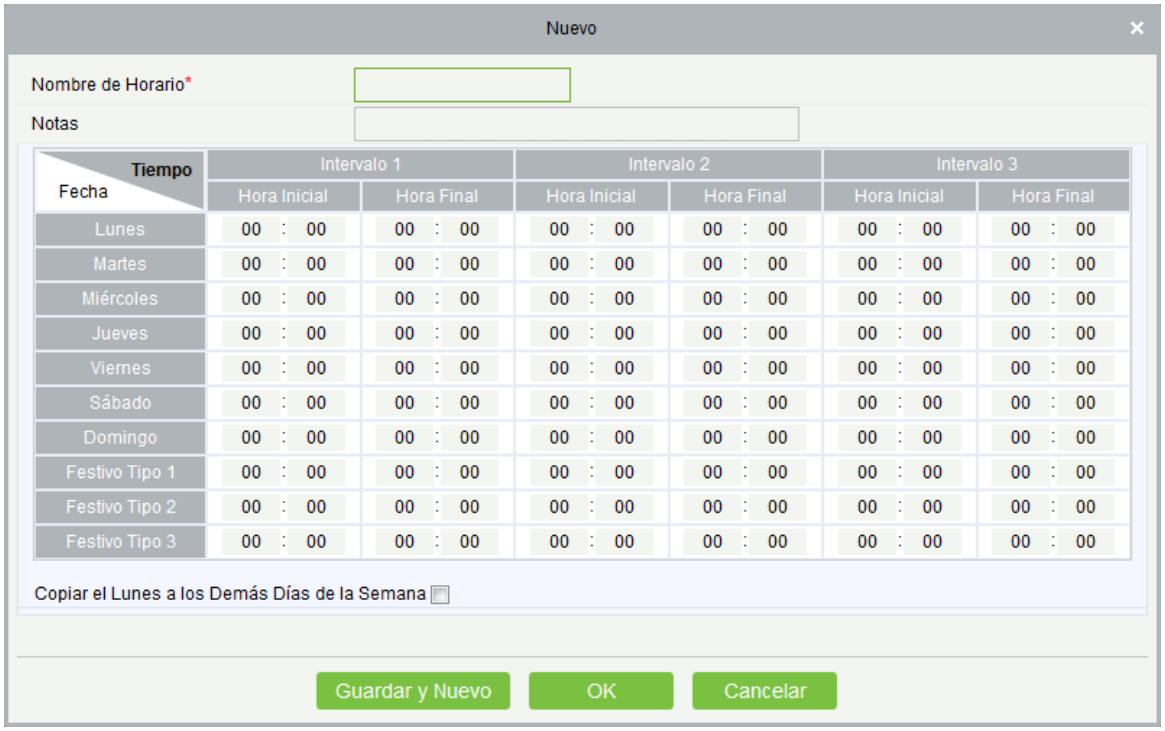
4.2.1 Horarios

Los horarios pueden habilitar o deshabilitar el uso de lectores durante tiempos específicos. También pueden establecer periodos de apertura normalmente abierto o para definir los niveles de acceso para que los usuarios tengan acceso en periodos de tiempo y puertas específicas (incluyendo primera apertura normalmente abierto).

El sistema controla el acceso de acuerdo a los horarios (máx. 255 horarios). El formato de cada intervalo para un horario es: HH: MM. Por defecto, el sistema cuenta con un horario de control de acceso llamado [24 horas]. Este horario no puede ser modificado o borrado. Es posible agregar nuevos horarios que puedan ser modificados o borrados.

1. Agregar Horario

(1) De clic en [Control de Acceso] > [Horarios] > [Nuevo] para acceder a la interfaz de horario:



Descripción de los campos:

Nombre de Horario: Cualquier caracter, hasta 30 caracteres.

Notas: Descripción detallada del horario actual, incluyendo la explicación y aplicación del horario. El campo es de 50 caracteres.

Intervalos, Tiempo Inicial y Final: Un horario puede incluir hasta 3 intervalos para cada día de la semana y 3 intervalos para cada uno de los días festivos. Configure la hora inicial y final de cada intervalo.

Configuración: Si el intervalo es normalmente abierto, solo introduzca 00:00-23:59 como el intervalo 1 y 00:00-00:00 como el intervalo 2/3. Si el intervalo es normalmente cerrado: todos son 00:00-00:00. Si solo se usa un intervalo, el usuario solo necesita introducir el campo del intervalo 1y el intervalo 2/3 mantiene el valor defecto. De igual manera, si solo se usan los primeros dos intervalos, el tercer intervalo se mantiene con el valor defecto. Cuando se usan dos o tres intervalos el usuario requiere asegurar que los intervalos no tienen intersección de tiempo y que el tiempo no abarque días, de lo contrario se mostrará un error.

Tipo de Día Festivo: Los tres tipos de días festivos no están relacionados con los días de la semana. Si una fecha se establece a un día festivo, los tres intervalos del día festivo se usarán para acceso. El tipo de día festivo es opcional. Si no ingresa ninguno el sistema usará el valor defecto.

Copiar el Lunes: Puede copiar rápidamente el horario del lunes a los demás días de la semana.

(2) Después de configurar, de clic en [OK] para guardar, y el horario se mostrará en la lista.

2. Mantenimiento de los Horarios

Editar: De clic en [Editar] para acceder a la interfaz de editar. De clic en [OK] para guardar los cambios.

Borrar: De clic en [Borrar] y luego clic en [OK] para borrar, o de clic en [Cancelar] para cancelar la operación. Un horario en uso no puede ser eliminado. Puede borrar múltiples horarios seleccionando las casillas y dando clic en [Borrar] arriba de la lista y [OK] para borrar o clic en [Cancelar] para cancelar.

4.2.2 Días Festivos

El control de acceso de un día festivo puede ser diferente que de un día normal. El sistema proporciona la configuración de los días festivos. La gestión incluye Agregar, Editar y Borrar.

- Agregar

(1) De clic en [Control de Acceso] > [Días Festivos] > [Agregar] para acceder a la interfaz de editar:

Descripción de los campos:

Nombre de Día Festivo: Cualquier caracter hasta 30 caracteres.

Tipo de Día Festivo: Festivo Tipo 1, 2 ó 3. Un día festivo pertenece a uno de los tipos y cada tipo puede incluir hasta 32 días festivos.

Fecha Inicial / Final: El formato de fecha es: 2010-1-1. La fecha inicial no puede ser posterior a la fecha final, de lo contrario se mostrará un error. El año de la fecha inicial no puede ser anterior al año actual y no puede abarcar años diferentes.

Recurrente: Indica si la fecha de un día festivo es igual todos los años. Por ejemplo, el día de año siempre es el 1 de enero y puede establecerlo como Si, pero, por ejemplo, el día del padre se celebra el tercer domingo de junio y por lo tanto no es fijo. En casos como este se establecería como No.

(2) Después de editar, de clic en [OK] para guardar y se mostrará en la lista de días festivos.

- Editar

De clic en el nombre del día festivo o en [Editar] para acceder a la interfaz. Después de realizar la modificación, de clic en [OK] para guardar y salir.

- Borrar

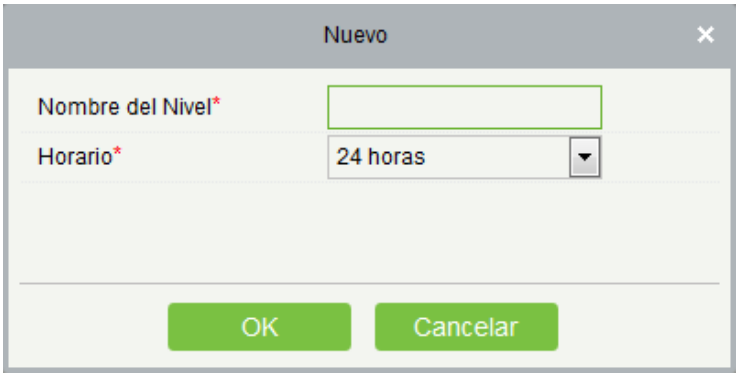
En la lista de días festivos, de clic en [Borrar]. De clic en [OK] para borrar o de clic en [Cancelar] para cancelar la operación. Un día festivo en uso no puede ser borrado.

4.2.3 Niveles de Acceso

Los niveles de acceso indican si una o varias puertas seleccionadas pueden ser abiertas por usuarios mediante la verificación y una combinación de horario.

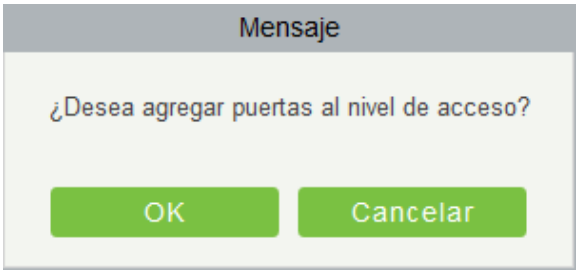
- Agregar

1. De clic en [Control de Acceso] > [Niveles de Acceso] > [Agregar] para acceder a la interfaz de agregar.



2. Ingrese los parámetros: Nombre del Nivel (no repetir) y Horario.

3. De clic en [OK] y el sistema mostrará "¿Desea agregar puertas al nivel de acceso?", de clic en [OK] to para agregar puertas o en [Cancelar] para regresar a la lista de niveles de acceso. El nivel de acceso agregado se mostrará en la lista.



✍Nota: Es posible seleccionar y agregar puertas de diferentes paneles en un nivel de acceso.

- Acceso Por Niveles

Agregar/Borrar personal de los niveles seleccionados:

(1) De clic en [Control de Acceso] > [Niveles de Acceso] > [Por Niveles] para acceder a la interfaz de edición, de clic en el nivel de acceso de la lista de la izquierda y el personal que tiene el privilegio para abrir la puerta en este nivel será mostrado en la lista de la derecha.

(2) En la lista de la izquierda, de clic en [Agregar Usuarios] debajo de operaciones para emerger la ventana de agregar de agregar personal; seleccione el personal (múltiple) de clic en > para mover a la lista de la derecha, después de clic en [OK] para guardar y salir.

(3) De clic en el nivel para ver el personal en la lista de la derecha. Seleccione el personal y de clic en [Borrar Personal] arriba de la lista de la derecha y de clic en [OK] para borrar.

- Acceso Por Usuario

Agregar/borrar personal de los niveles de acceso seleccionados:

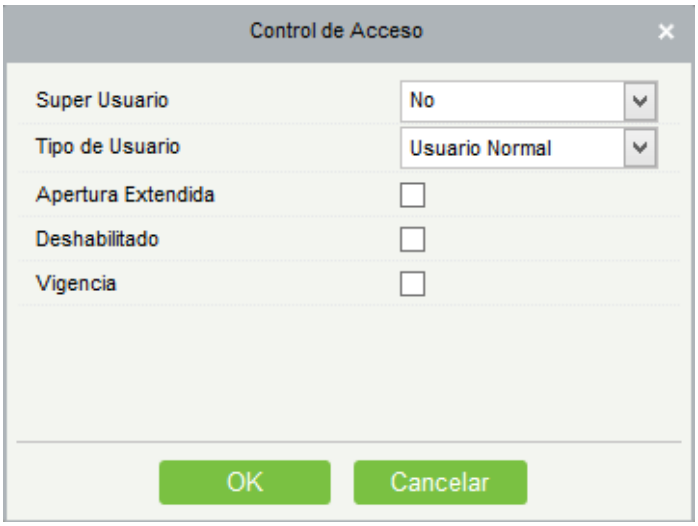
(1) De clic en [Control de Acceso] > [Niveles de Acceso] > [Por Usuario], de clic en el usuario para ver sus respectivos niveles en la lista de la derecha.

(2) De clic en [Agregar a los Niveles] debajo de Operaciones para emerger la ventana de Agregar a los Niveles, seleccione el nivel (múltiple) y de clic en > para mover los seleccionados a la lista de la derecha; de clic en [OK] para guardar y salir.

(3) Seleccione el nivel (múltiple) de la lista de la derecha, y de clic en [Borrar de los Niveles] arriba de la lista y de clic en [OK] para borrar el personal de los niveles seleccionados.

Configurar Control de Acceso para el Personal Seleccionado:

（1） Seleccione un usuario de la lista de la izquierda y de clic en el botón [Control de Acceso].



（2） Configure los parámetros de control de acceso y de clic en [OK] para guardar los ajustes.

- Acceso por Departamento

Agregar los departamentos a los niveles de acceso seleccionados, o eliminar los departamentos de los niveles de acceso. Los parámetros de acceso del personal en el departamento serán cambiados.

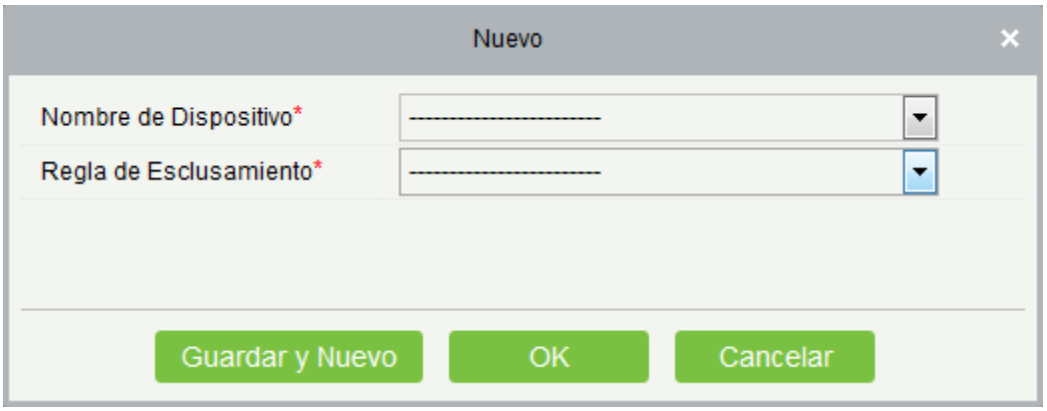
4.2.4 Esclusamiento

El esclusamiento puede establecerse para dos o más puertas que pertenecen a un panel de acceso. Cuando una puerta es abierta, las otras no podrán abrirse hasta que la puerta abierta sea cerrada.

Antes de configurar el esclusamiento, asegure que el panel de acceso tenga conectados los sensores de puerta correspondientes, ya sean N.C. o N.A.

- Agregar Esclusamiento

1. De clic en [Control de Acceso] > [Esclusamiento] > [Nuevo] para acceder a la interfaz de edición:



2. Seleccione el nombre del dispositivo. Al agregar, los dispositivos ya esclusados no se mostrarán en la lista hasta después de borrar su respectiva configuración de esclusamiento. Las opciones de configuración de esclusamiento varían según el número de puertas del dispositivo seleccionado:

- Panel de una puerta no tiene opciones de esclusamiento.
- Panel de dos puertas: esclusar puertas 1 y 2.
- Panel de cuatro puertas: esclusar puertas 1 y 2, esclusar puertas 3 y 4, esclusar puertas 1, 2 y 3, esclusar puertas 1, 2, 3 y 4.

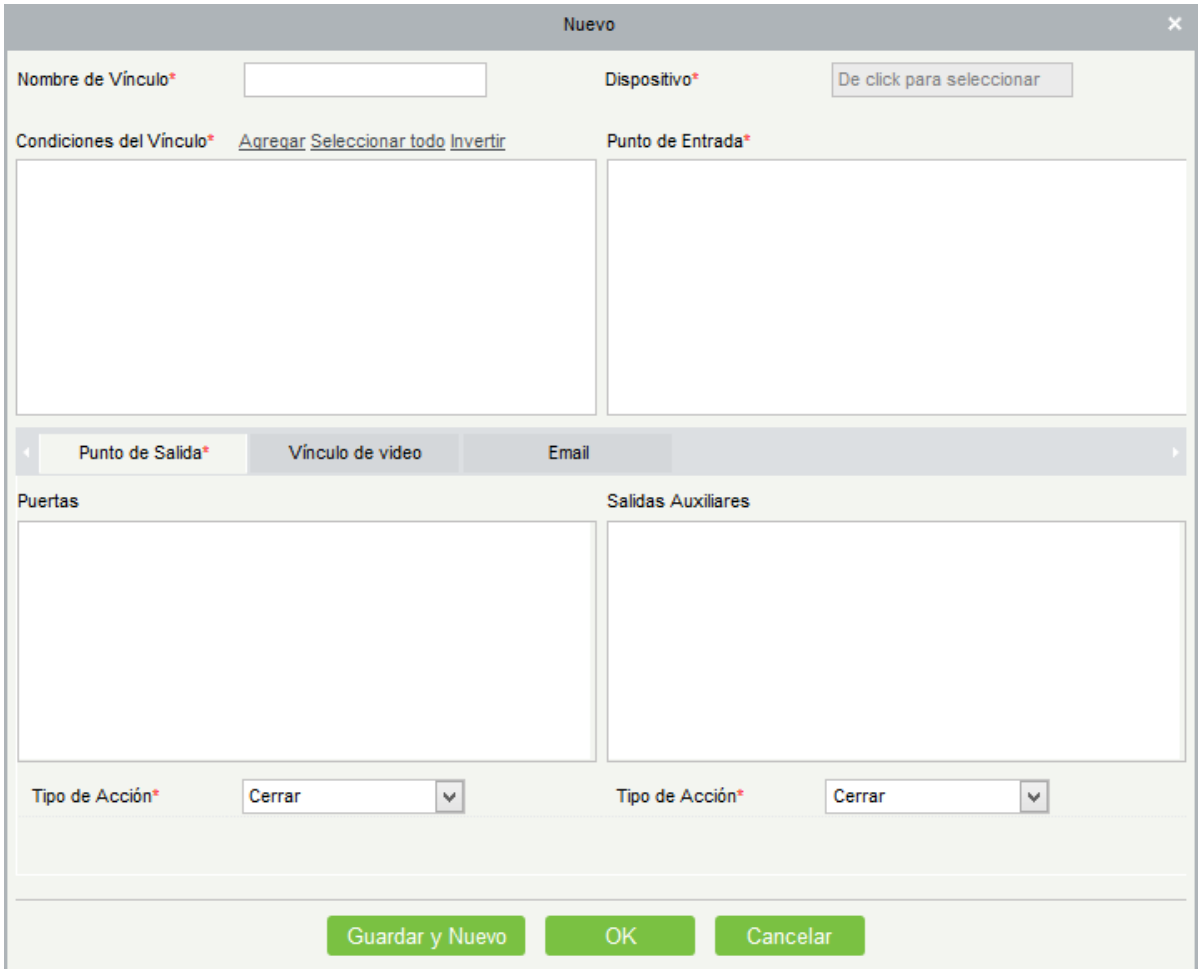
3. Seleccione la opción y de clic en [OK] para completar. La nueva lista de opciones se mostrará en la lista.

✍Nota: Al editar, el dispositivo no puede ser modificado pero la configuración de esclusamiento si puede ser modificado. Si ya no requiere realizar ajustes para el dispositivo el registro de configuración de esclusamiento puede ser eliminado. Cuando se elimina el registro de un dispositivo, si cuenta con registro de configuración de esclusamiento, también será eliminado.

4.2.5 Vínculos

Un vínculo significa que cuando ocurre un evento en un punto de entrada del sistema de control de acceso, se desencadenará o vinculará una acción en un punto de salida especificado tal como una apertura, salida de alarma, etc.

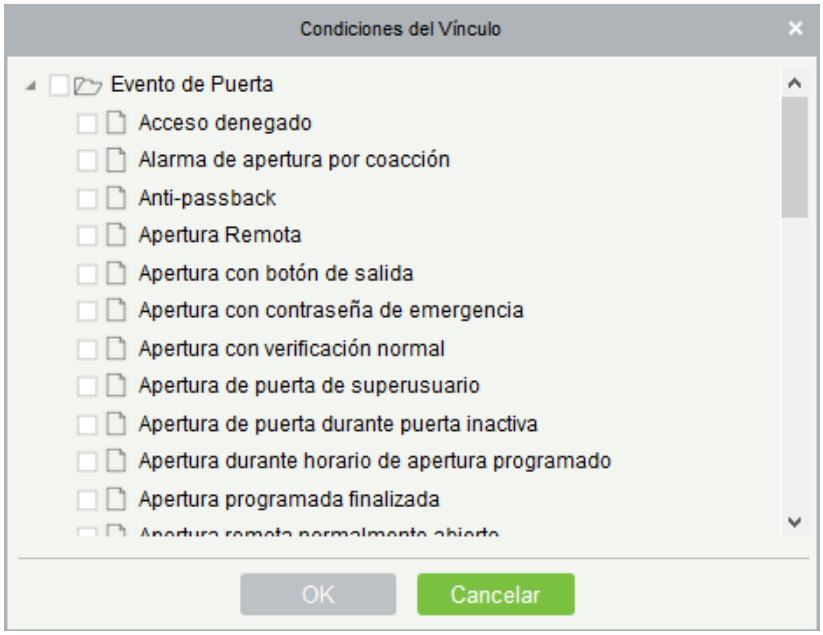
Agregar vínculo:



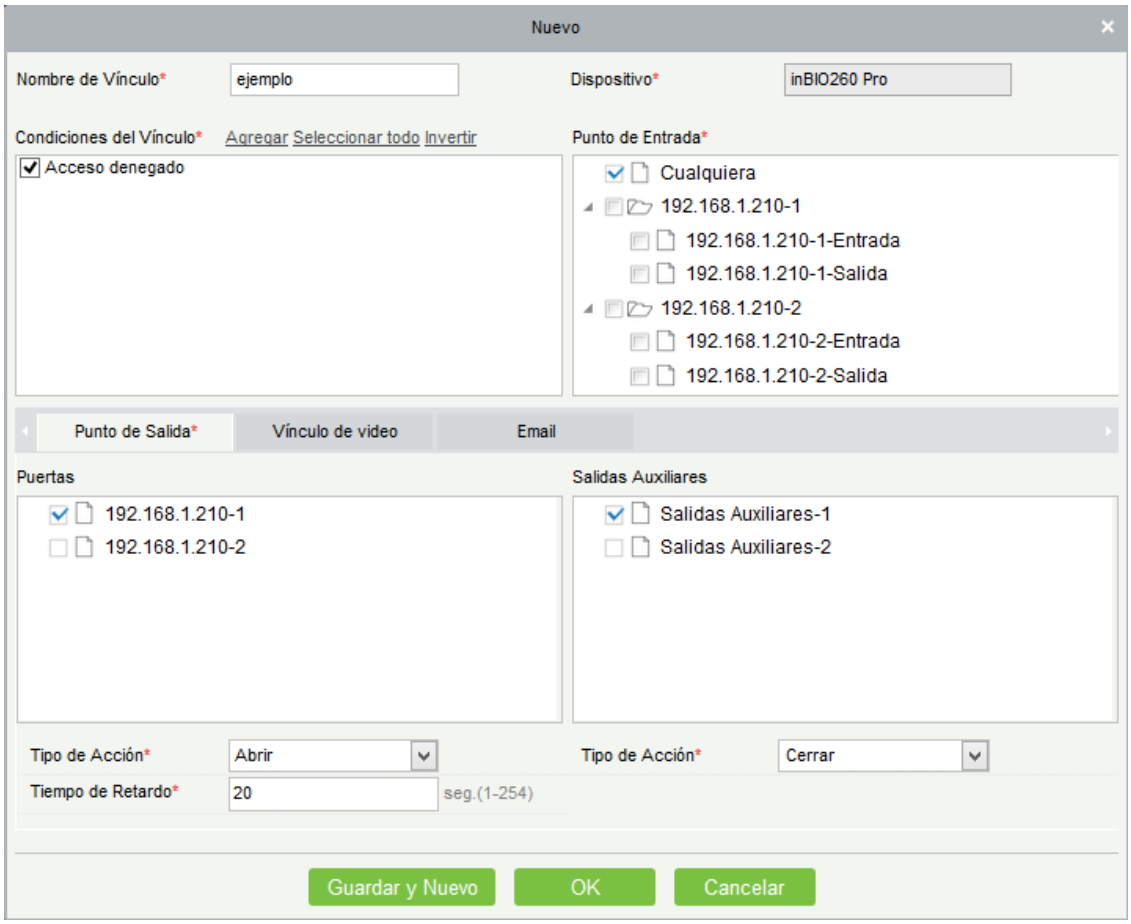
1. De clic en [Control de Acceso] > [Vínculos] > [Agregar]

2. Introduzca el nombre del vínculo, seleccione el dispositivo, seleccione las condiciones del vínculo, seleccione el punto de inicio, seleccione el punto de salida, seleccione la acción, el vínculo de video y otros parámetros.

3. Después de seleccionar el dispositivo, los ajustes de vínculos correspondientes se mostrarán (el Sistema primero confirmará que el dispositivo está conectado correctamente y que ha podido leer los parámetros extendidos, de lo contrario el sistema no podrá configurar los vínculos y solo mostrará los ajustes de vínculos de acuerdo a la cantidad de puertas y entradas y salidas auxiliares del dispositivo seleccionado actualmente):



✍Nota: Las condiciones de vínculo contienen eventos de puerta y entrada auxiliar. Falla de conexión al servidor, recuperar conexión y dispositivo desconectado serán filtrados de los eventos de puerta.



4. Seleccione el punto de inicio y de salida, acción, vínculo de video y dirección de email.

Descripción de los campos:

Nombre del Vínculo: Introduzca el nombre del vínculo.

Condición del Vínculo: La condición del vínculo es el tipo de evento del dispositivo seleccionado. Todos los eventos pueden ser condiciones de vínculo excepto detener alarma, habilitar/deshabilitar salida auxiliar y dispositivo inicializado.

Punto de Entrada: Puede ser, Puerta 1, 2, 3 y 4, Entrada Auxiliar 1, 2, 3, 4, 9, 10, 11, 12 (los puntos de entrada varían según el modelo y especificaciones de cada dispositivo).

Punto de Salida: Puerta 1, 2, 3, y 4, Salida Auxiliar 1, 2, 3, 4, 6, 8, 9, 10 (los puntos de salida varían según el modelo y especificaciones de cada dispositivo).

Acción del Vínculo: Abrir, Cerrar, Normalmente Abierto. El defecto es Cerrar. Para Abrir, deberá introducir el tiempo de retardo o seleccionar Normalmente Abierto.

Vínculo de Video:

- Pop-Up de Video: Si se habilita, emergerá una ventana de vista previa de video en la interfaz de monitoreo en tiempo real. Deberá introducir el tiempo de retardo.
- Video: Si se habilita, se guarda el video de la cámara asociada. Deberá introducir el tiempo de duración de la grabación.
- Captura: Si se habilita, se guarda la captura del evento.

Retardo: El rango es de 1 a 254s (este campo es válido cuando la acción es Abrir).

5. Después de la edición, de clic en [OK] para guardar y salir. El vínculo agregado se mostrará en la lista.

Por ejemplo: si selecciona Apertura con Verificación Normal como condición del vínculo, el punto de entrada "Puerta 1", punto de salida "Salida Auxiliar 1" y la acción del vínculo es Abrir, con retardo de 60s, entonces, cuando ocurra una verificación normal en la puerta 1 entonces se accionará la Salida Auxiliar 1 por 60s.

✍Nota: Al editar, no es posible modificar el dispositivo, pero puede modificar el nombre del vínculo y su configuración. Cuando un dispositivo es eliminado, si cuenta con algún vínculo configurado, será también eliminado.

Si el dispositivo y la condición del vínculo es el mismo, y el sistema tiene una configuración de vínculo donde el punto de entrada es una puerta específica o entrada auxiliar, no permitirá al usuario agregar o editar la configuración del vínculo donde el punto de entrada es Cualquiera.

Al contrario, si el dispositivo y la condición del vínculo es el mismo, y el sistema tiene una configuración de vínculo donde el punto de entrada es Cualquiera, no permitirá al usuario agregar o editar la configuración del vínculo donde el punto de entrada es una puerta específica o entrada auxiliar.

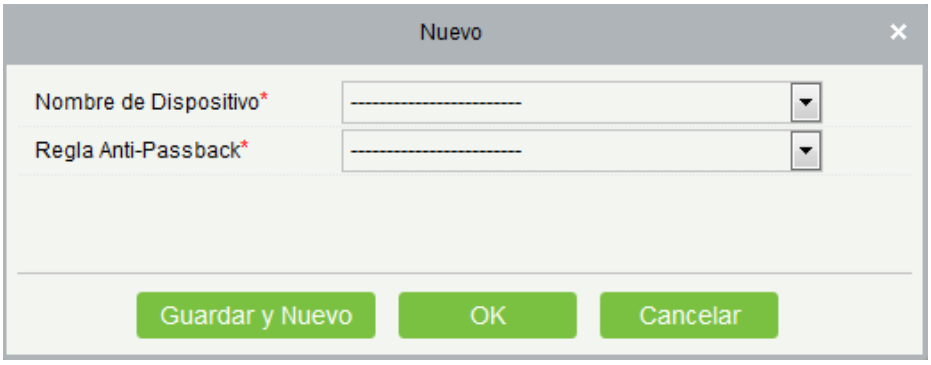
Adicionalmente, no es permitido configurar el vínculo para el mismo punto de entrada y de salida. El mismo dispositivo permite ajustes consecutivos de vinculación lógica. El sistema permite establecer varias condiciones de vínculo al mismo tiempo.

4.2.6 Anti-Passback

Actualmente la función Anti-Passback se soporta en la entrada y salida. En algunos casos es necesario que el titular de una tarjeta de acceso que entró por una puerta deba generar un evento de salida con la misma tarjeta y de esta manera los registros de entrada y salida son consistentes. Es posible realizar esta función configurando los ajustes de Anti-Passback. Esta función es utilizada en prisiones, bancos, bóvedas, ejército, defensa nacional, etc.

Agregar configuración de Anti-Passback:

1. De clic en [Control de Acceso] > [Anti-Passback] > [Agregar] para acceder a la interfaz de edición:



2. Seleccione el dispositivo (los dispositivos que ya cuentan con configuración de anti-passback no serán mostrados en la lista). Se mostrarán las opciones según el número de puertas de cada dispositivo:

- Panel de una puerta: Anti-passback entre los lectores.
- Panel de dos puertas: Anti-passback entre los lectores de la puerta 1, anti-passback entre los lectores de la puerta 2 y anti-passback de puerta 1 y puerta 2.
- Panel de cuatro puertas: Anti-passback de puerta 1 y puerta 2, anti-passback de puerta 3 y puerta 4, anti-passback de puertas 1/2 y puertas 3/4, anti-passback de puerta 1 y puertas 2/3, anti-passback de puerta 1 y puertas 2/3/4 y anti-passback entre lectores de puertas 1/2/ 3/ 4.

✍Nota: Los lectores de puerta mencionados anteriormente incluye los lectores Wiegand y lectores inBIO conectados a los paneles de acceso. El panel de 1 y 2 puertas con lectores Wiegand incluye lector de entrada y salida. Los paneles de 4 puertas solo tienen un lector por puerta. Los números de lector 1, 2 (ya sea Wiegand o dirección RS485) corresponden a la puerta 1, los números de lector of 3, 4 son para la puerta 2, etc. No es necesario considerar si es un lector Wiegand o InBIO para la configuración de anti-passback entre puertas o entre lectores, solo asegure la correcta distribución de lectores de entrada y salida según los requerimientos reales. Respecto al número de los lectores, los números nones son considerados entrada y los números pares son considerados salida.

3. Seleccione la regla de anti-passback y de clic en [OK] para completar. La configuración de anti-passback se mostrará en la lista.

✍**Nota:** Al editar, no es posible modificar el dispositivo, pero puede modificar la configuración de anti-passback. Cuando un dispositivo es eliminado, si cuenta con alguna configuración de anti-passback, será también eliminada.

4.2.7 Primera Apertura Normalmente Abierto

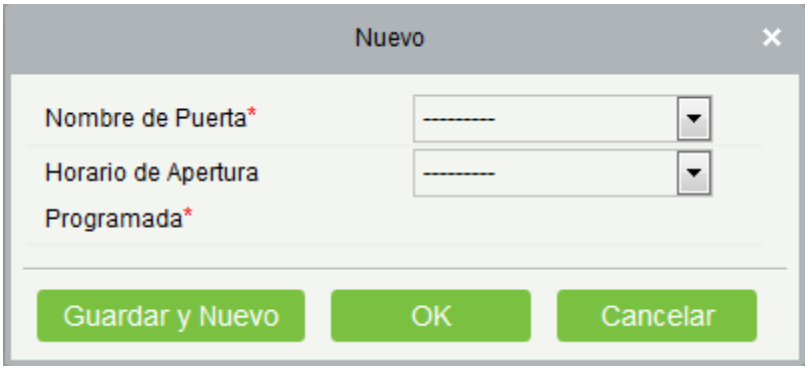
Durante un horario especificado, después de la verificación de un usuario con nivel de primera apertura normalmente abierto, la puerta se abrirá con estado normalmente abierto y se restaurará al estado cerrado automáticamente cuando haya transcurrido el horario.

Es posible establecer esta función para una puerta específica (la configuración incluye puerta, horario y personal con la función o nivel asignado). Es posible establecer múltiples horarios para esta función. La interfaz para cada puerta mostrará el número existente de primera apertura normalmente abierto.

Al agregar o editar primera apertura normalmente abierto seleccione la puerta y el horario. Después de agregar exitosamente, agregue el personal que pueda abrir la puerta con esta función. Es posible examinar y borrar el personal en el lado derecho de la interfaz.

Descripción de los pasos:

1. De clic en [Control de Acceso] > [Primera Apertura] > [Nuevo], seleccione el nombre de la puerta y horario de apertura programada y de clic en [OK] para guardar la configuración.

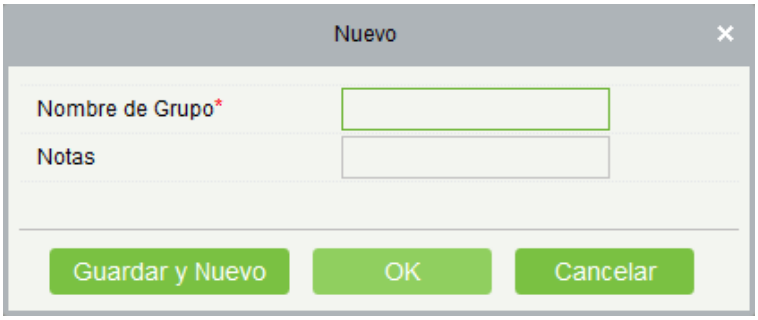


2. De clic en [Agregar Personal] debajo de Operaciones para agregar personal a este nivel (este personal debe tener nivel de acceso asignado), luego de clic en [OK] para guardar.

4.2.8 Grupos Multi-Usuario

La puerta solo se abrirá solamente después de la verificación consecutiva de un grupo específico de usuarios. Cualquier usuario que intente verificar que no esté dentro de esta combinación o grupo interrumpirá el procedimiento y será necesario esperar 10 segundos para reintentar la verificación. En esta función la puerta no se abrirá por la verificación de un solo usuario del grupo.

(1) De clic en [Control de Acceso] > [Grupos Multi-Usuario] > [Nuevo] para acceder a la interfaz de edición:



Nombre de Grupo: Cualquier combinación de hasta 30 caracteres. El nombre debe ser único.

Después de editar, de clic en [OK] para guardar y regresar. El grupo agregado se mostrará en la lista.

(2) De clic en [Agregar Personal] debajo de Operaciones para agregar personal al grupo.

(3) Después de seleccionar y agregar personal, de clic en [OK] para guardar y regresar.

✍Nota: Un usuario puede pertenecer a un solo grupo.

4.2.9 Verificación Multi-Usuario

Establece los niveles para el personal en el grupo multi-usuario.

Es una combinación de personal en uno o más grupos multi-usuario. Al establecer el número de personas en cada grupo, se puede configurar un grupo (como la apertura de puerta por la combinación de dos personas en un grupo) o múltiples grupos (como la apertura de puerta de cuatro usuarios, incluyendo dos personas del grupo 1 y dos personas del grupo 2), y al menos un grupo debe contener un número de usuario diferente a 0, y el número total no debe ser mayor de 5. Adicionalmente, si el número de usuarios ingresados es mayor que en el grupo actual, la verificación multi-usuario será deshabilitada.

Configuración de verificación multi-usuario:

(1) De clic en [Control de Acceso] > [Verificación Multi-Usuario] > [Nuevo]:

(2) Seleccione el Nombre de Puerta e introduzca el Nombre de Combinación. Seleccione el número de usuarios para la verificación multi-usuario de un grupo (el máximo número de usuarios para la verificación multi-usuario es 5)

y de clic en [OK] para completar.

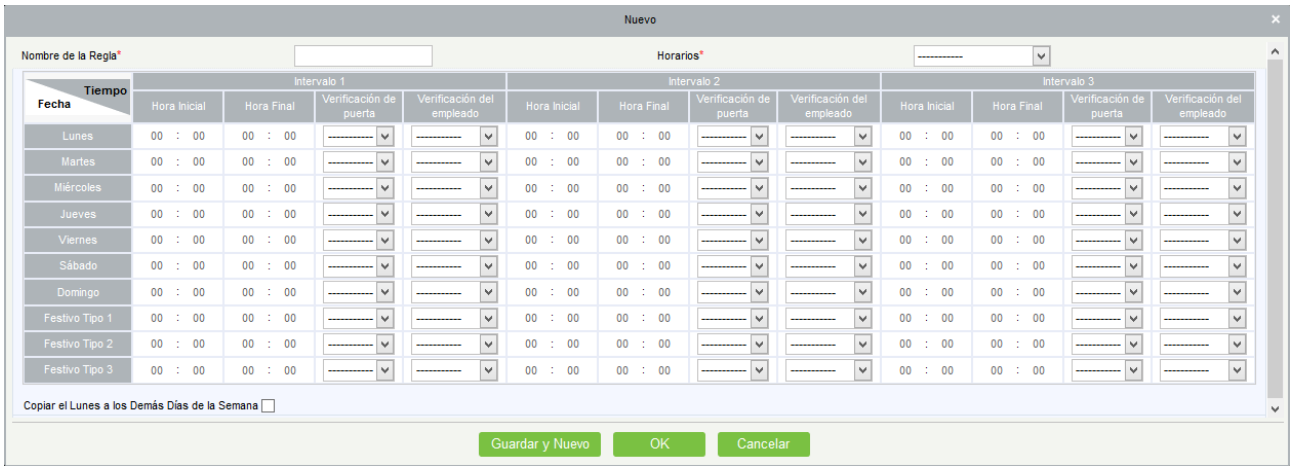
✍Nota: El intervalo de verificación entre usuarios por defecto es de 10 segundos. Puede modificar en intervalo si el dispositivo lo soporta.

4.2.10 Modo de Verificación

Modo de Verificación: Puede configurar el modo de verificación independiente para las puertas y para el personal durante un horario de tiempo definido.

- Agregar

1. De clic en [Control de Acceso] > [Modo de Verificación] > [Nuevo] para ir a la ventana de agregar regla de modo de verificación.



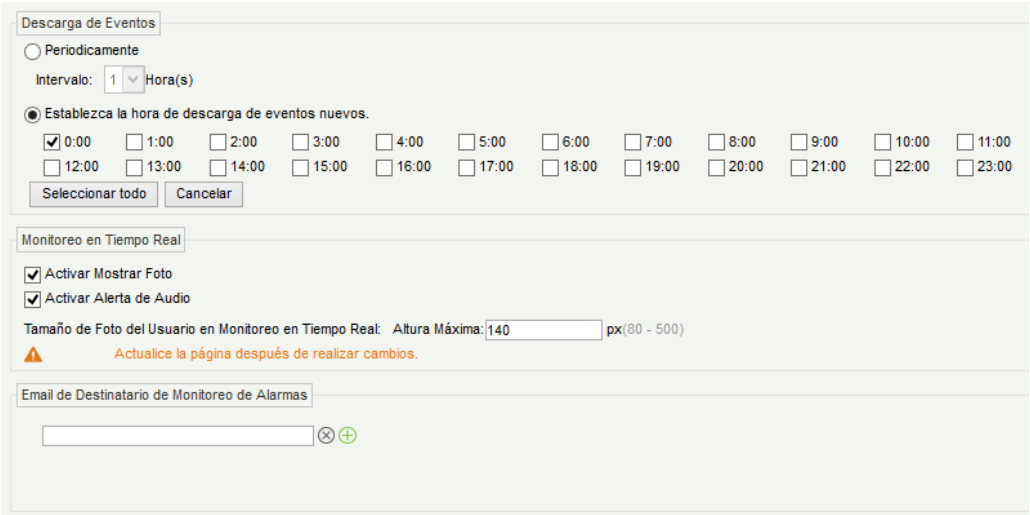
2. Configure los siguientes parámetros: Seleccione un nombre para la regla (no repetible), el segmento de tiempo y el modo de verificación para la puerta o usuario en cada segmento de tiempo.
3. De clic en [OK] para terminar.
4. En la página con la lista, puede agregar o eliminar puertas en la regla de modo de verificación.

✍**Nota**: Si una regla incluye el modo de verificación para personal, no puede seleccionar puertas con lectores RS485 al agregar puertas. Solo puede modificar la configuración en la página de ajustes de los lectores antes de agregar las puertas.

Grupo de Modo de Verificación: Configure el personal apropiado para la regla de modo de verificación.

4.2.11 Parámetros

De clic en [Control de Acceso] > [Parámetros] para acceder a la interfaz de configuración de parámetros:



Descarga de Eventos

- Periódicamente

El sistema intentará descargar los eventos cada intervalo de tiempo. Comienza a partir de la hora en que se establece la configuración.

- Establezca la hora de descarga de eventos nuevos

Si se selecciona la hora, el sistema intentará descargar los eventos nuevos automáticamente.

Tamaño de Imagen Pop-up de Personal en Monitoreo en Tiempo Real: Cuando un evento de control de acceso ocurre, la foto del personal emergerá y es posible ajustar el tamaño, el rango es 80-500 pixeles.

Email de Destinatario de Monitoreo de Alarmas: El sistema enviará un correo electrónico al motorista de alarmas cuando ocurra un evento de alarma.

4.3 Funciones Avanzadas de Control de Acceso

Las funciones avanzadas de control de acceso es una función opcional del sistema. Si requiere estas funciones, contacte a su representante comercial o Ingeniero de soporte. Estas funciones pueden utilizarse después de obtener y activar una licencia.

✍Nota: A excepción de los vínculos globales, para poder utilizar las funciones avanzadas es necesario activar la verificación en segundo plano. Para más información, consulte Operaciones del Dispositivo.

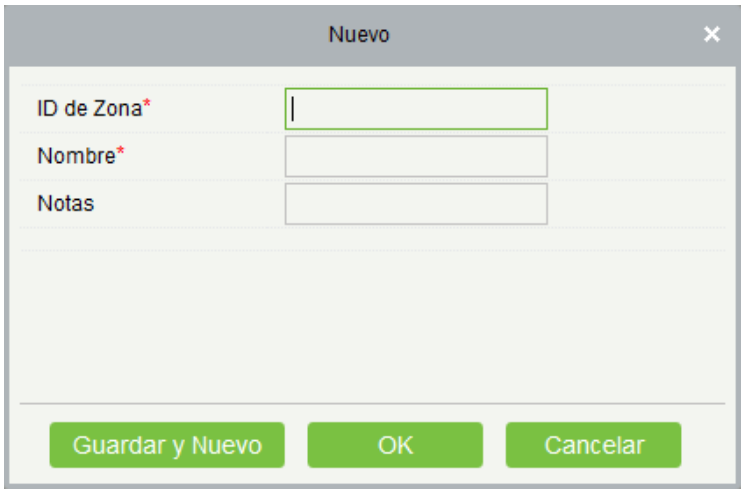
4.3.1 Zona

Para el uso de las funciones avanzadas de control de acceso como el Anti-Passback Global es necesario definir las zonas de acceso.

- Agregar

1. De clic en [Control de Acceso] > [Funciones Avanzadas] > [Zona] > [Nuevo] para acceder a la interfaz de Agregar

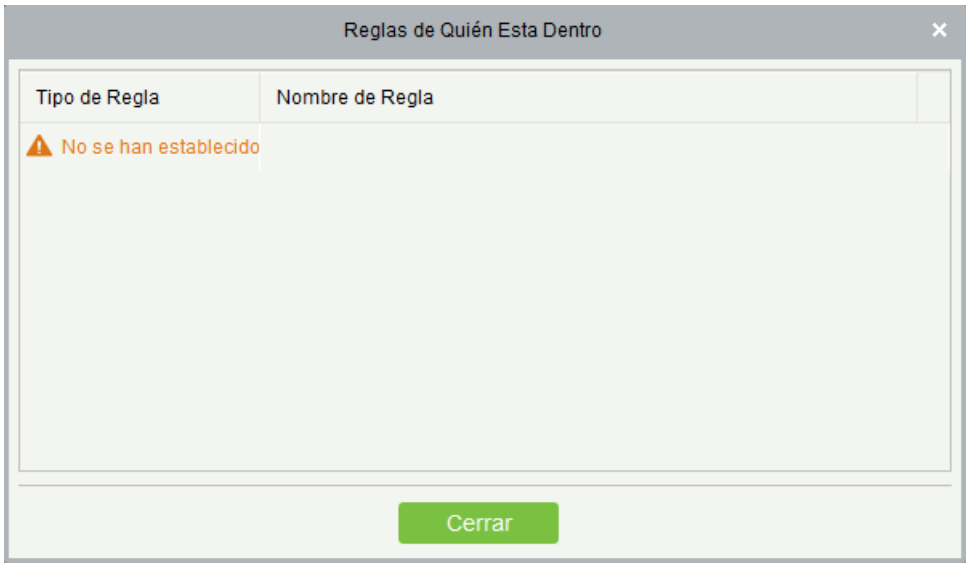
Zona:



2. Introduzca el ID de Zona, Nombre y Notas si es necesario.

3. De clic en [OK] para guardar y salir. La zona agregada se mostrará en la lista.

Reglas Dentro de:

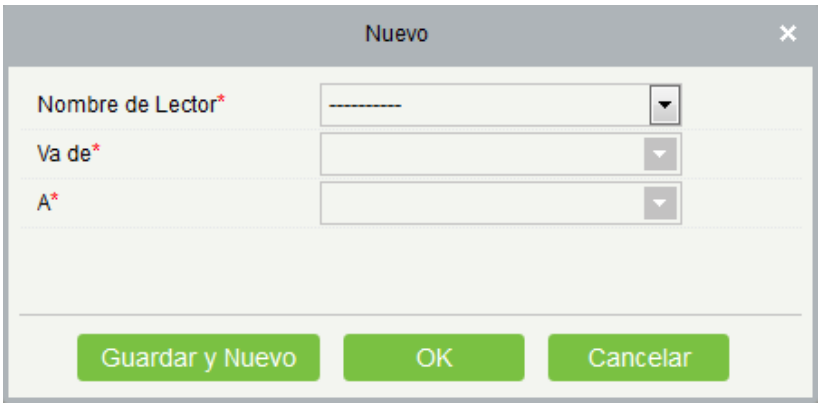


4.3.2 Definir Lectores

Definir Lectores indica el control de lectores para acceder de una zona a otra, basado en la zona de acceso. Si requiere utilizar las funciones avanzadas, es necesario definir los lectores.

- Agregar

1. De clic en [Control de Acceso] > [Funciones Avanzadas] > [Definir Lectores] > [Nuevo] para acceder a la interfaz de agregar:

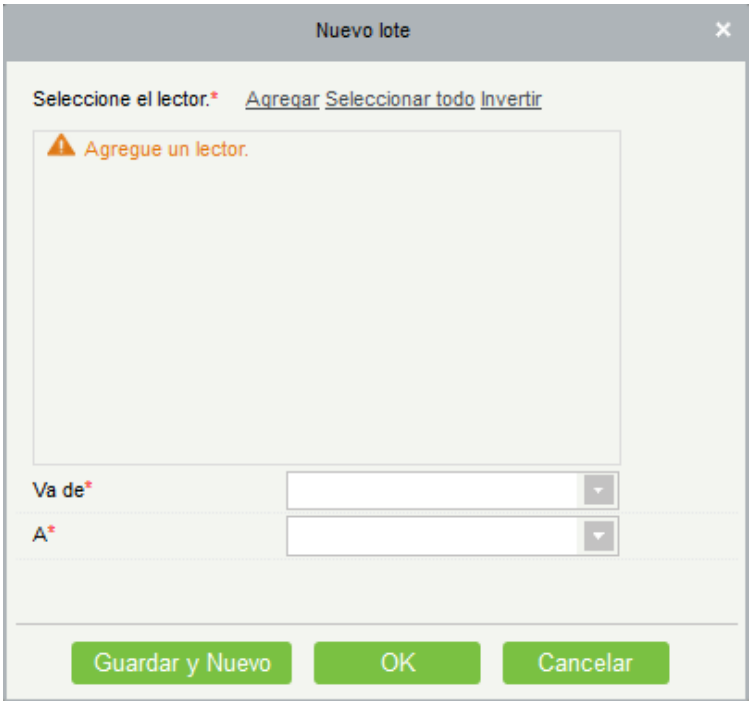


2. Seleccione el Nombre de Lector, Va de y A, como sea necesario.

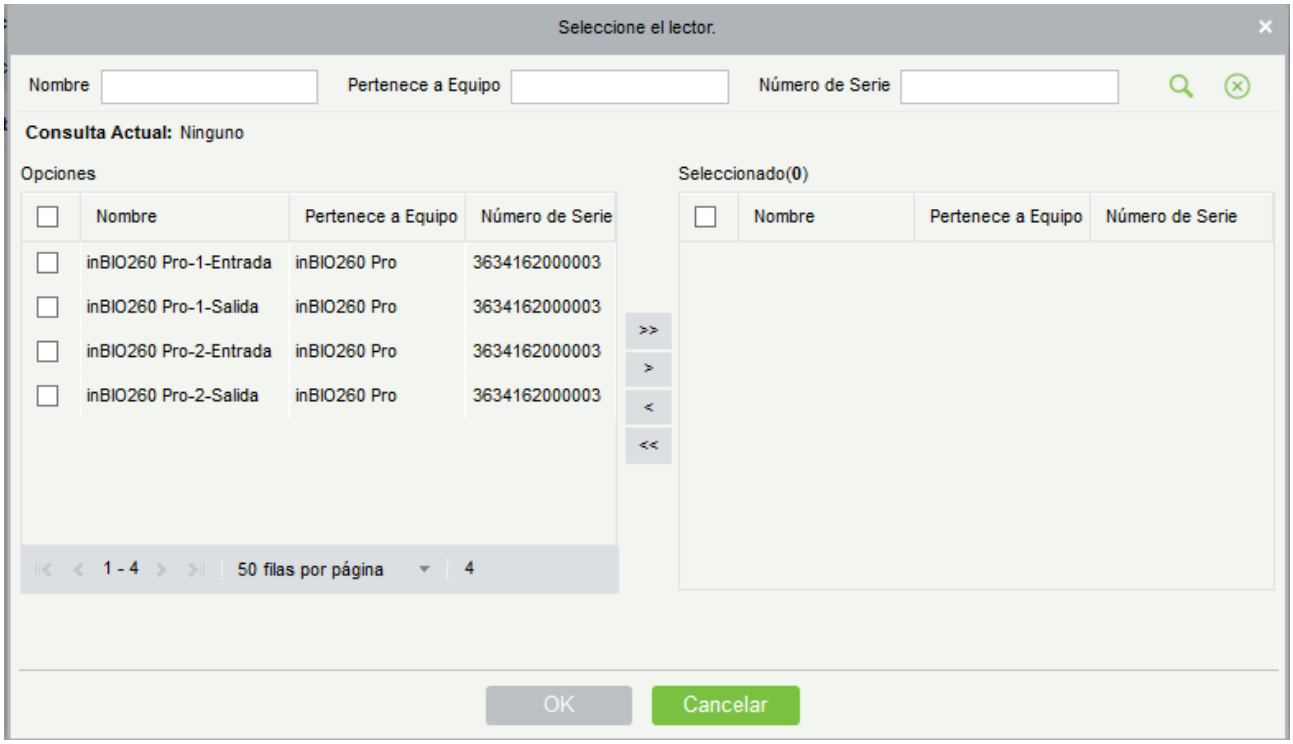
3. De clic en [OK] para guardar y salir. La definición de lectores se mostrará en la lista.

- Lote Nuevo

1. Clic en [Control de Acceso] > [Funciones Avanzadas] > [Definir Lectores] > [Lote Nuevo] para acceder a la interfaz de lote nuevo:



2. De clic en [Agregar], seleccione el Lector y de clic en [OK]



3. Configure los parámetros como sea requerido.

4.3.3 Quién Está Dentro

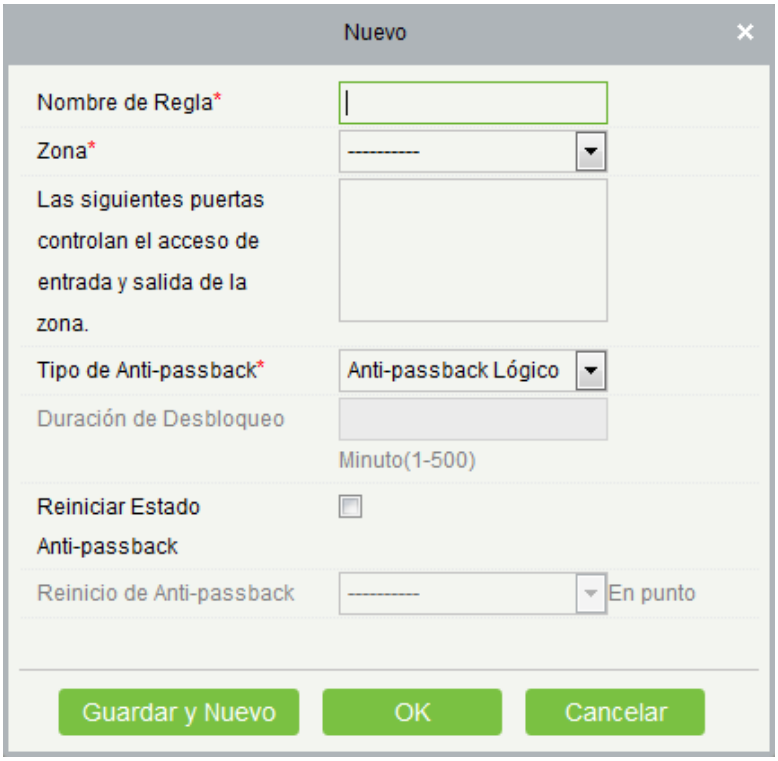
Después de introducir la zona, es posible ver el estado del personal en la zona en el árbol de zonas.

4.3.4 Anti-Passback Global

Anti-Passback Global entre zonas puede establecer Anti-Passback entre dispositivos. Para usar esta función, es necesario establecer las Zonas de Acceso, Definir Lectores y activar la verificación en segundo plano para el dispositivo con esta función.

- Agregar

1. De clic en [Control de Acceso] > [Funciones Avanzadas] > [Anti-Passback Global] > [Nuevo] para acceder a la interfaz de agregar:



2. Introduzca el Nombre de Regla, (nombre único), seleccione la zona, tipo de anti-passback, duración de desbloqueo, Reinicio de estado Anti-passback y cuando reiniciar Anti-passback como sea necesario.

Zona: Seleccione una opción de la lista. Las puertas correspondientes se mostrarán con el texto "Las siguientes puertas controlan el acceso de entrada y salida de la zona". Al mismo tiempo, las puertas obedecen la regla de una puerta no puede ser el límite de dos Anti-passback independientes.

Tipo de Anti-passback: Anti-passback lógico, temporizado y lógico temporizado.

- Anti-passback Lógico: Requiere los registros de entrada y salida estrictamente consistentes en la zona de Anti-passback, de lo contrario la puerta no se abrirá.
- Anti-passback Temporizado: En un periodo de tiempo específico, un usuario puede entrar a la zona Anti-passback solo una vez. Cuando el periodo se termina, el estado del usuario se reinicia y el usuario puede acceder a ésta zona otra vez.
- Anti-passback Lógico Temporizado: En un periodo de tiempo específico, los usuarios que entren a la zona de Anti-passback deben obedecer la regla del Anti-passback Lógico. Si excede el periodo de tiempo, el sistema contará el tiempo otra vez.

Duración de Desbloqueo: Solo se puede establecer en Anti-passback Temporizado y Anti-passback Lógico Temporizado.

Reiniciar Estado Anti-Passback: Seleccione para reiniciar o borrar el estado Anti-passback del personal en el sistema y recuperar el estado inicial. Cuando haya expirado el tiempo de Anti-passback, el sistema reiniciará el estado Anti-passback del personal en la zona.

Reinicio de Anti-Passback: Seleccione la hora para el reinicio del Anti-passback.

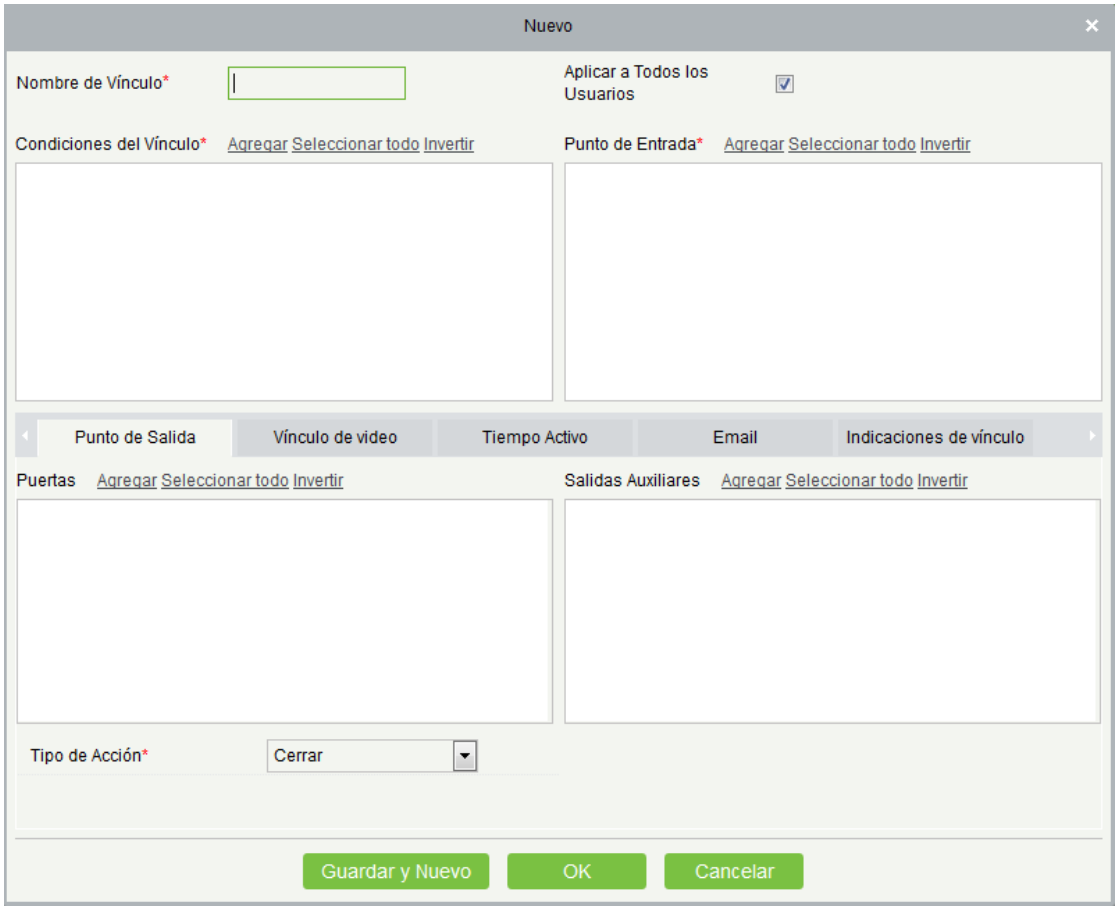
3. De clic en [OK] para guardar y salir. La zona de APB Global se mostrará en la lista.

4.3.5 Vínculos Globales

Los vínculos globales permiten configurar datos entre dispositivos. Solo los dispositivos con firmware PUSH soportan esta función.

- Agregar

1. De clic en [Control de Acceso] > [Funciones Avanzadas]> [Vínculos Globales] > [Nuevo]:



Aplicar a Todos los Usuarios: Si se habilita esta opción, el vínculo será efectivo para todos los usuarios.
Tiempo Activo: Configure el tiempo activo del vínculo.

2. Seleccione las condiciones del vínculo global, el punto de inicio (el sistema filtrará los dispositivos según la selección del primer paso), el punto de salida y la acción del vínculo. Para más detalles acerca de estos parámetros, consulte Vínculos.

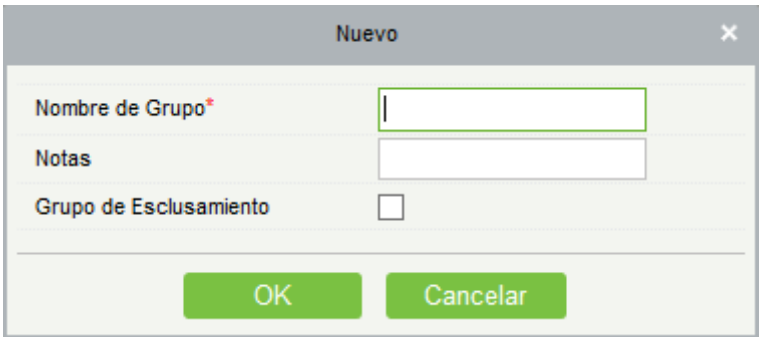
✍**Nota:** Es posible seleccionar múltiples eventos de puerta, pero los eventos "Falla al conectar al servidor", "Recuperar conexión" y "Conexión de dispositivo apagado" serán filtrados de los eventos de puerta.

3. De clic en [OK] para guardar y salir. El vínculo global agregado se mostrará en la lista.

4.3.6 Grupo Esclusamiento Global

Los grupos de esclusamiento global permiten agrupar puertas para la función de esclusamiento global y para usar esta función el dispositivo debe estar habilitado con verificación en segundo plano.

1. De clic en [Control de Acceso] > [Grupo Esclusamiento Global]> [Nuevo]:



Nombre de Grupo:

(1) Cualquier combinación de hasta 30 caracteres. El nombre no puede repetirse.

(2) Después de editar, de clic en [OK] para guardar. Después de confirmar el agregar la puerta inmediatamente, la información de la puerta agregada se mostrará en la lista.

(3) De clic en [Agregar Puerta] debajo de Operaciones Relacionadas para agregar la puerta al grupo.

(4) Después de seleccionar y agregar el personal, de clic en [OK] para guardar y regresar.

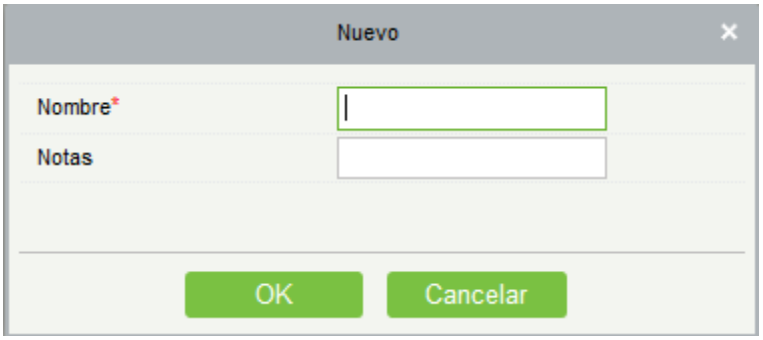
Grupo de Esclusamiento: Si se habilita la opción, se establece la regla de esclusamiento global al grupo.

4.3.7 Esclusamiento Global

La función de esclusamiento global permite configurar datos a través de dispositivos. Esta función solo es compatible con dispositivos de protocolo PUSH.

Configuración de Esclusamiento Global:

1. De clic en [Control de Acceso] > [Esclusamiento Global]> [Nuevo]:



Nombre:

(1) Cualquier combinación de hasta 30 caracteres. El nombre no puede repetirse.

(2) Después de editar, de clic en [OK] para guardar. Después de confirmar el agregar la puerta inmediatamente, la información de la puerta agregada se mostrará en la lista.

(3) De clic en [Agregar Puerta] debajo de Operaciones Relacionadas para agregar la puerta al grupo.

(4) Después de seleccionar y agregar los usuarios, de clic en [OK] para guardar y regresar.

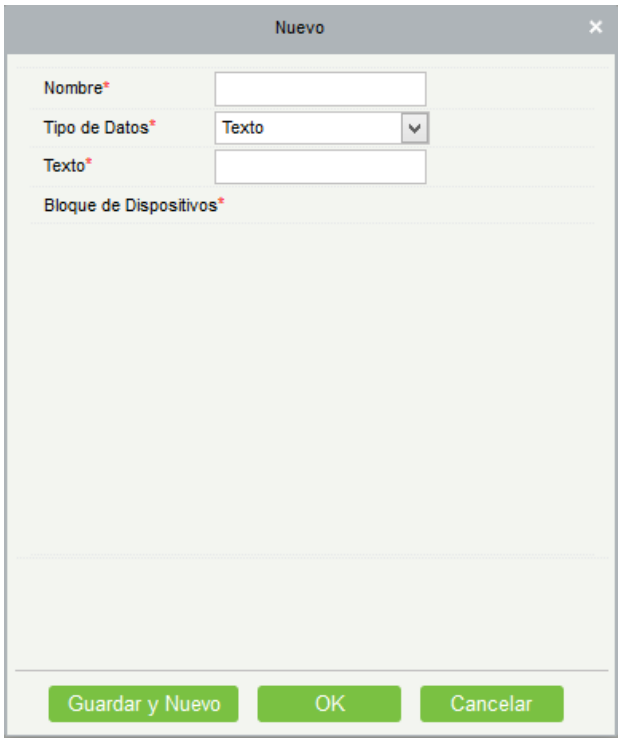
Grupo de Esclusamiento: Si se habilita la opción, se establece la regla de esclusamiento global al grupo.

✍ **Notas:**

1. En el mismo esclusamiento, no se pueden duplicar las puertas.
2. Cuando existe esclusamiento asignado a un grupo, no puede ser eliminado directamente.

4.3.8 Datos LED

- Agregar



Nombre: Nombre de los Datos LED.

Tipo de Datos:

Texto: Enviar textos autodefinidos a los bloques.

Zona de Datos: Número total de usuarios en la zona a ser enviada y estadísticas del personal en los departamentos de la zona.

✍**Notas:**

1. La zona de control de acceso es la que se encuentra en las funciones avanzadas.
2. Si el contenido para enviar es el departamento, seleccione el departamento del cual se recolectarán las estadísticas.

Cambiar datos: Información en tiempo real del personal entrando y saliendo. Puede seleccionar el contenido que será enviado.

4.4 Reportes de Acceso

Incluye reportes de: Todos los Eventos, Eventos de Hoy, Última Posición Registrada, Eventos de Excepción, Eventos por Puerta y Eventos por Usuario. Es posible exportar después de buscar los datos.

Puede generar estadísticas de datos relevantes de los dispositivos y generar reportes, incluyendo información de verificación con tarjetas, información de operación de puertas, accesos, etc.

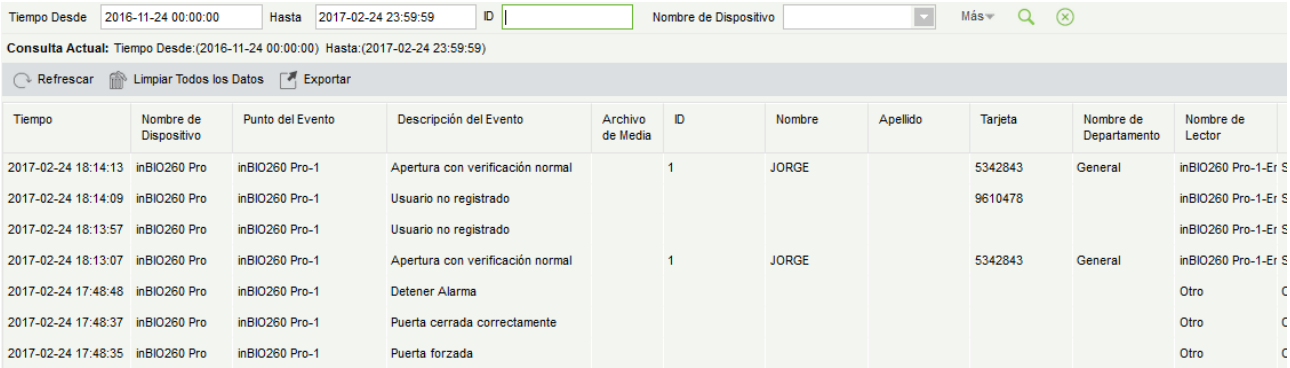
Acerca de los eventos normales y anormales, consulte Monitoreo en Tiempo Real para los detalles.

Modo de Verificación: Solo Tarjeta, Solo Huella, Solo Contraseña, Tarjeta y Contraseña, Tarjeta y Huella, Tarjeta o Contraseña, etc.

✍**Nota:** Solo los eventos generados cuando el usuario usa la contraseña de emergencia para abrir las puertas incluirán modo de verificación Solo Contraseña.

4.4.1 Todos los Eventos

Dado que el tamaño de los datos de acceso puede ser muy grande, es posible ver los eventos de control de acceso después de filtrar condiciones específicas. Por defecto, el sistema mostrará los eventos de los últimos tres meses. De clic en [Reportes] > [Todos los Eventos] para ver todos los eventos:



Tiempo	Nombre de Dispositivo	Punto del Evento	Descripción del Evento	Archivo de Media	ID	Nombre	Apellido	Tarjeta	Nombre de Departamento	Nombre de Lector
2017-02-24 18:14:13	inBIO260 Pro	inBIO260 Pro-1	Apertura con verificación normal		1	JORGE		5342843	General	inBIO260 Pro-1-Er S
2017-02-24 18:14:09	inBIO260 Pro	inBIO260 Pro-1	Usuario no registrado					9610478		inBIO260 Pro-1-Er S
2017-02-24 18:13:57	inBIO260 Pro	inBIO260 Pro-1	Usuario no registrado							inBIO260 Pro-1-Er S
2017-02-24 18:13:07	inBIO260 Pro	inBIO260 Pro-1	Apertura con verificación normal		1	JORGE		5342843	General	inBIO260 Pro-1-Er S
2017-02-24 17:48:48	inBIO260 Pro	inBIO260 Pro-1	Detener Alarma							Otro
2017-02-24 17:48:37	inBIO260 Pro	inBIO260 Pro-1	Puerta cerrada correctamente							Otro
2017-02-24 17:48:35	inBIO260 Pro	inBIO260 Pro-1	Puerta forzada							Otro

Archivo de Media: Puede ver o descargar las fotos capturadas o los videos creados en el sistema.

Limpiar Todos los Datos: De clic en [Limpiar Todos los Datos] para emerger una ventana y de clic en [OK] para limpiar todos los datos.

4.4.2 Eventos de Hoy

Consulta los eventos de hoy.

De clic en [Acceso] > [Reportes] > [Eventos de Hoy] para ver los eventos de hoy.

ID | Nombre de Dispositivo | Más

Consulta Actual: Ninguno

Refrescar | Limpiar Todos los Datos | Exportar

Tiempo	Tarjeta	ID	Nombre	Apellido	Nombre de Departamento	Nombre de Dispositivo	Punto del Evento	Descripción del Evento	Archivo de Media	Nombre de Lector	Mo Ve
2017-02-24 18:14:13	5342843	1	JORGE		General	inBIO260 Pro	inBIO260 Pro-1	Apertura con verificación normal		inBIO260 Pro-1-Er	Solo
2017-02-24 18:13:07	5342843	1	JORGE		General	inBIO260 Pro	inBIO260 Pro-1	Apertura con verificación normal		inBIO260 Pro-1-Er	Solo
2017-02-24 17:40:25	5342843	1	JORGE		General	inBIO260 Pro	inBIO260 Pro-1	Apertura con verificación normal		inBIO260 Pro-1-Er	Solo
2017-02-24 17:38:46	5342843	1	JORGE		General	inBIO260 Pro	inBIO260 Pro-1	Apertura con verificación normal		inBIO260 Pro-1-Er	Solo

4.4.3 Última Posición Registrada

Consulta la última ubicación o posición donde un usuario realizó una verificación de acceso. Es útil para localizar a un usuario específico.

De clic en [Acceso] > [Reportes] > [Última Posición Registrada] para consultar.

Tiempo Desde 2016-11-24 00:00:00 | Hasta 2017-02-24 23:59:59 | ID | Nombre de Dispositivo | Más

Consulta Actual: Tiempo Desde:(2016-11-24 00:00:00) Hasta:(2017-02-24 23:59:59)

Refrescar | Limpiar Todos los Datos | Exportar

ID	Nombre	Apellido	Tarjeta	Tiempo	Nombre de Departamento	Nombre de Dispositivo	Punto del Evento	Descripción del Evento	Nombre de Lector	Modo de Verificación
1	JORGE		5342843	2017-02-24 18:14:13	General	inBIO260 Pro	inBIO260 Pro-1	Apertura con verificación normal	inBIO260 Pro-1-Er	Solo Tarjeta

Conocer la ubicación del personal: Los usuarios con privilegio de mapa virtual pueden dar clic en el ID de usuario correspondiente para conocer la ubicación específica del personal en el mapa virtual donde se mostrará la puerta parpadeando.

4.4.4 Eventos de Excepción

De clic en [Reportes] > [Eventos de Excepción] para ver los eventos de excepción en las condiciones especificadas. Las opciones son las mismas que en [Todos los Eventos].

Tiempo Desde 2016-11-24 00:00:00 | Hasta 2017-02-24 23:59:59 | ID | Nombre de Dispositivo | Más

Consulta Actual: Tiempo Desde:(2016-11-24 00:00:00) Hasta:(2017-02-24 23:59:59)

Refrescar | Limpiar Todos los Datos | Exportar

Tiempo	Descripción del Evento	Punto del Evento	Nombre de Dispositivo	Tarjeta	ID	Nombre	Apellido	Nombre de Área	Nombre de Departame	Nombre de Lector	Modo de Verificació	Notas
2017-02-24 18:14:09	Usuario no registrado	inBIO260 Pro-1	inBIO260 Pro	9610478				ZKTeco		inBIO260 Pr	Solo Tarjeta	
2017-02-24 18:13:57	Usuario no registrado	inBIO260 Pro-1	inBIO260 Pro					ZKTeco		inBIO260 Pr	Solo Huella	
2017-02-24 17:48:35	Puerta forzada	inBIO260 Pro-1	inBIO260 Pro					ZKTeco		Otro	Otro	

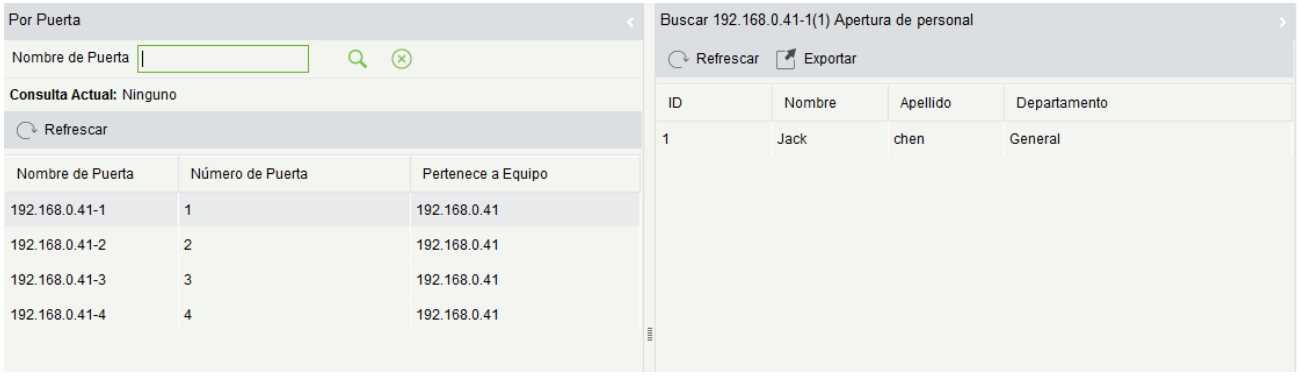
Limpiar Todos Los Eventos: De clic en [Limpiar Todos Los Eventos] para emerger una ventana y de clic en [OK] para limpiar los eventos de excepción.

4.4.5 Privilegios de Acceso

- Por Puerta

Ver los niveles de acceso por puerta. De clic en [Reportes] > [Por Puerta], la lista de datos en la izquierda muestra

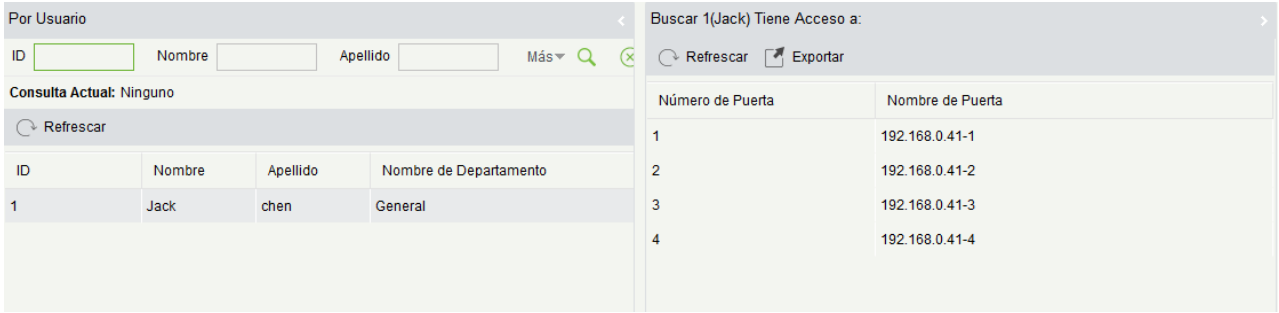
todas las puertas en el sistema, seleccione una puerta y se mostrará el personal que tiene el nivel de acceso a la puerta en la lista de la derecha.



- Por Usuario

Ver los niveles de acceso por personal.

De clic en [Reportes] > [Por Usuario], la lista de datos en la izquierda muestra todos los usuarios, seleccione un usuario y se mostrarán las puertas a las que el personal tiene acceso.



4.4.6 Gráficas

Puede visualizar las gráficas de estadísticas de los eventos de control de acceso.

4.5 Integración VMS

Para los detalles de esta función consulte el manual de usuario correspondiente.

5 Elevador

El sistema de control de elevador es principalmente usado para definir los parámetros del dispositivo (tal como el horario para usar los elevadores y la duración de las teclas), gestionar los privilegios de acceso a los pisos, el tiempo de control del elevador y supervisar los eventos de elevador y control de acceso. Es posible asignar los privilegios de pisos a los usuarios. Solo los usuarios autorizados pueden acceder a ciertos pisos dentro del horario especificado después de haber sido autentificado.

5.1 Dispositivo de Elevador

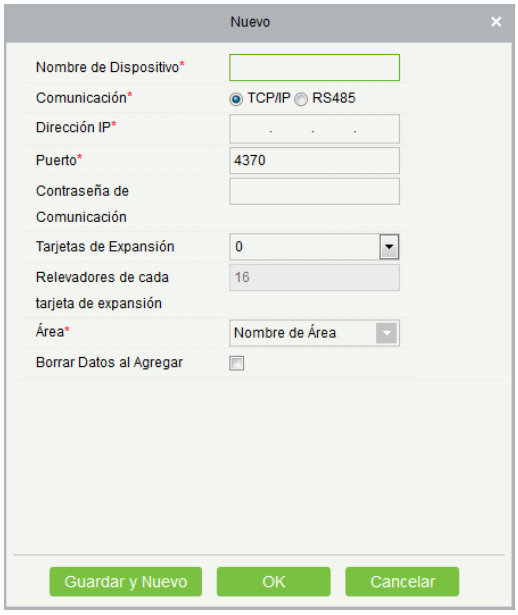
5.1.1 Agregar un Dispositivo de Elevador

Hay dos formas de agregar dispositivos de elevador.

- Agregar manualmente

(1) De clic en [Elevador] > [Dispositivos] > [Dispositivos] > [Nuevo] en el menú y se mostrará la siguiente interfaz:

Modo de comunicación TCP/ IP



Modo de comunicación RS485

Dirección IP: Introduzca la dirección IP del panel de acceso.

Puerto de Comunicación: Por defecto es 4370.

Puerto Serial: COM1 a COM254.

Dirección RS485: El número de dispositivo, rango de 1 a 255. En un lazo de comunicación Serial no se puede repetir la dirección RS485.

Baudios: Velocidad de transmisión de datos. Por defecto es 38400.

Figura de Dirección RS485: Muestra la figura del DIP Switch de la dirección RS485.

Opciones comunes:

Nombre de Dispositivo: Cualquier carácter con un máximo de 20.

Contraseña de Comunicación: La longitud máxima es de 6, con números o letras. Un dispositivo nuevo o inicializado no tiene contraseña de comunicación.

✍ **Nota:** No es necesario introducir este campo si el dispositivo es nuevo o recién inicializado.

Tarjetas de Expansión: Número de tarjetas de expansión del dispositivo de elevador.

Relevadores de cada tarjeta de expansión: Cada tarjeta de expansión tiene 16 relevadores.

Número de Tarjetas de Expansión: La cantidad de tarjetas de expansión que controlará el dispositivo.

Área: Especifica el área del dispositivo. Después de establecer las áreas es posible filtrar por área en el monitoreo en tiempo real.

Borrar Datos al Agregar: Al marcar esta opción, después de agregar el dispositivo, el sistema borrará todos los datos en el dispositivo (excepto los datos de eventos). Si agrega el dispositivo sólo para demostración o pruebas no requiere marcar la opción.

(2) Después de editar de clic [OK] y el sistema tratará de conectarse con el dispositivo actual.

Si la conexión es exitosa, el sistema obtendrá los parámetros extendidos del dispositivo. En este punto, si el sistema no reconoce al equipo con los parámetros correspondientes del dispositivo actual, mostrará una advertencia. Si da clic en [OK], se guardará el tipo de controlador actual.

Parámetros Extendidos del Dispositivo: Estos parámetros incluyen número de serie, tipo de dispositivo, versión de firmware, cantidad de entradas y salidas auxiliares, cantidad de puertas, versión de algoritmo de huella digital, cantidad de lectores, etc.

✍Nota: Al eliminar un nuevo dispositivo, el software borrará toda información de usuarios, horarios, días festivos y configuraciones de control de acceso (incluyendo niveles de acceso, anti-passback, esclusamiento, vínculos, etc.) del dispositivo, excepto los datos de eventos (a menos que la información contenida en el dispositivo no sea útil, se recomienda no borrar el dispositivo para evitar la pérdida de información).

Configuración de Dispositivo de Elevador:

✧ Requisitos de Comunicación TCP/ IP

Para soportar y habilitar la comunicación TCP/ IP, conecte el dispositivo directamente a la PC o a la red local, introduzca la dirección IP y otros datos del dispositivo;

✧ Requisitos de Comunicación RS485

Para comunicación RS485, conecte al dispositivo a la PC mediante un convertidor e introduzca los datos al sistema como el número de puerto, ID RS485 del dispositivo, baudios, etc.

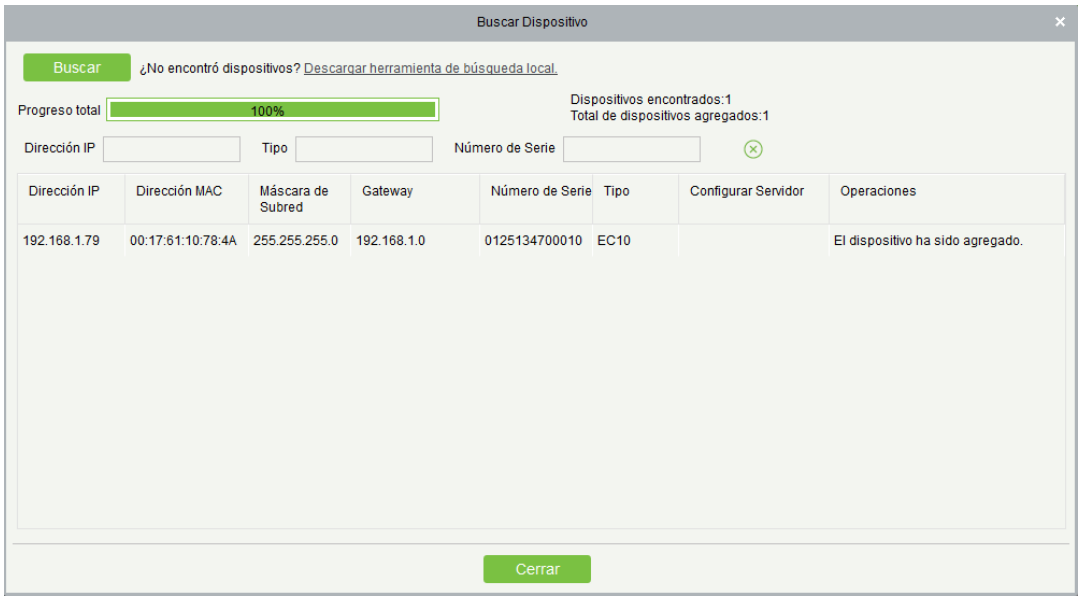
2. Agregar dispositivos por búsqueda

Buscar los dispositivos en la red.

(1) De clic en [Elevador] > [Dispositivos] > [Buscar Dispositivo], para mostrar la interfaz de búsqueda.

(2) De clic en [Buscar] y se mostrará [Buscando…].

(3) Después de realizar la búsqueda se mostrarán los dispositivos encontrados en la red en una lista como se muestra a en la imagen:



✍Nota: El modo de transmisión UDP se utilizará para buscar los dispositivos de elevador y solo funciona en la red local. Los dispositivos requieren configurarse dentro del mismo segmento de red.

(4) De clic en [Agregar] y emergerá una ventana de diálogo. Introduzca el nombre del dispositivo y de clic en [OK] para agregar.

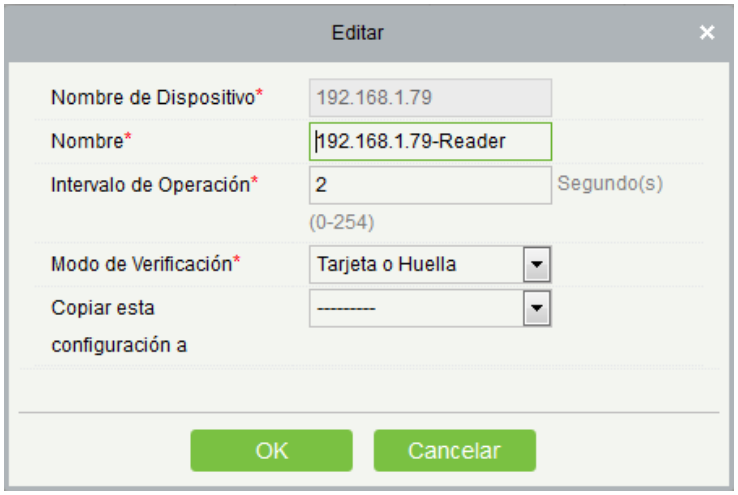
(5) La dirección IP por defecto del dispositivo pudiera tener conflicto con algún otro dispositivo en la red. En este caso puede modificar la dirección IP dando clic en [Modificar IP]. Introduzca la nueva dirección IP y los otros parámetros (Nota: Configure el Gateway y la IP en el mismo segmento de red).

✍Nota: El sistema no puede agregar dispositivos de elevador automáticamente.

5.1.2 Lectores

Cada dispositivo de elevador tiene un lector. Puede establecerse la información del lector.

De clic en [Dispositivo] > [Lectores], seleccione un nombre de lector de la lista:



Descripción de los campos:

Nombre del Dispositivo: No es editable.

Nombre: El formato defecto es "Nombre de Dispositivo - Lector", es editable. Máx. 30 caracteres.

Intervalo de Operación: El intervalo entre dos verificaciones. El valor defecto es 2 segundos y un rango de 0 a 254 segundos.

Modo de Verificación: Seleccione el modo de verificación que incluye tarjeta, huella, contraseña y combinaciones, siendo por defecto tarjeta o huella. Si selecciona tarjeta y contraseña, asegure que la puerta esté equipada con un lector con teclado.

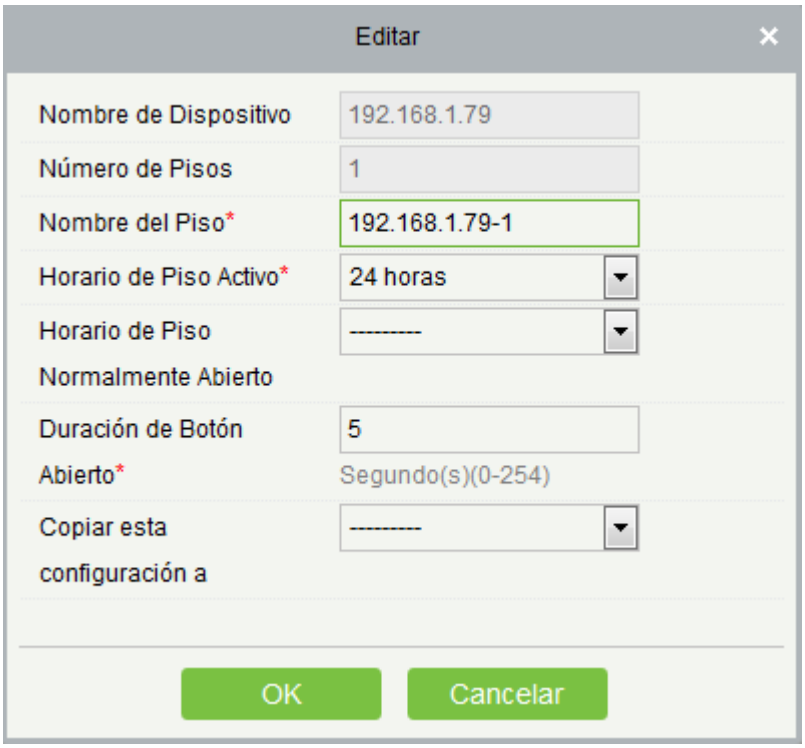
Copiar esta configuración a:

Todos los lectores de todos los dispositivos: Aplicar configuración anterior a todos los lectores de todos los dispositivos del nivel del usuario actual.

De clic en [OK] para guardar y salir.

5.1.3 Pisos

De clic en [Dispositivos] > [Pisos], seleccione el nombre de un piso de la lista y de clic en [Editar]:



Descripción de los campos:

Nombre de Dispositivo: No es editable.

Número de Piso: El sistema los nombrará automáticamente según el número de relevadores.

Nombre de Piso: El formato defecto es "Nombre de Dispositivo – Número de Piso", es editable máx. 30 caracteres.

Horario de Piso Activo, Horario de Apertura Programada: **El valor defecto es Nulo**. Se mostrarán los horarios de piso activo agregados por los usuarios para ser seleccionados. Al editar un piso, el horario de piso activo debe ser. Para cerrar la liberación continua de los pisos se realiza después de especificar el horario efectivo. El horario de apertura programada toma efecto solo en el periodo efectivo. Se recomienda que el periodo de liberación continua sea incluido en el horario de piso activo.

Duración de Liberación de Botón: Es el tiempo que se libera un botón después de una realizar una verificación válida. El valor defecto es 5 segundos con un rango de 0 a 254 segundos.

Copiar la Configuración a: Incluye dos opciones.

- Todos los Pisos del Dispositivo Actual: Aplica la configuración actual a todos los pisos del dispositivo.
- Todos los Pisos de Todos los Dispositivos: Aplica la configuración actual a todos los pisos de todos los dispositivos del nivel del usuario actual.

5.1.4 Entradas Auxiliares

Se utilizan principalmente para conectar dispositivos, como sensores infrarrojos o sensores de humo.

1. De clic en [Elevador] > [Dispositivos] > [Entradas Auxiliares], accederá a la siguiente interfaz:

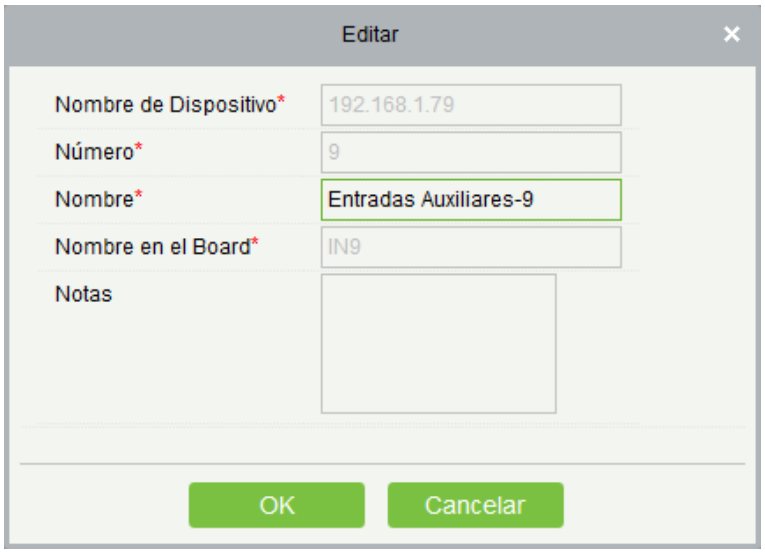
Nombre | Nombre de Dispositivo | Nombre en el Board

Consulta Actual: Ninguno

Refrescar

Nombre	Nombre de Dispositivo	Número	Nombre en el Board	Notas	Operaciones
Entradas Auxiliares-9	192.168.214.47	9	IN9		Editar
Entradas Auxiliares-10	192.168.214.47	10	IN10		Editar
Entradas Auxiliares-11	192.168.214.47	11	IN11		Editar
Entradas Auxiliares-12	192.168.214.47	12	IN12		Editar

2. De clic en [Editar] para modificar los parámetros:



Descripción de los campos:

Nombre: Puede editar el nombre.

Nombre en el Board: El nombre como se muestra en el hardware, por ejemplo, IN9.

3. De clic en [Editar] para modificar el nombre y las notas. Otros campos no se pueden editar aquí.

5.1.5 Tipo de Evento

Muestra los tipos de eventos de los dispositivos de elevador.

1. Clic [Dispositivos] > [Tipo de Evento], para acceder a la siguiente interfaz:

Refrescar

Nombre del Evento	Evento No.	Nivel de Evento	Nombre de Dispositivo	Número de Serie
Apertura con Tarjeta	0	Normal	192.168.1.79	0125134700010
Registro durante zona de tiempo del modo pass	1	Normal	192.168.1.79	0125134700010
Apertura durante zona de tiempo del modo pass	5	Normal	192.168.1.79	0125134700010
Apertura Remota	8	Normal	192.168.1.79	0125134700010
Cerrado Remoto	9	Normal	192.168.1.79	0125134700010
Desactivar Apertura Programada	10	Normal	192.168.1.79	0125134700010
Activar Apertura Programada	11	Normal	192.168.1.79	0125134700010
Apertura con Huella Digital	14	Normal	192.168.1.79	0125134700010
Huella digital durante horario de apertura progra	16	Normal	192.168.1.79	0125134700010
Intervalo de lectura muy corto	20	Excepción	192.168.1.79	0125134700010
Zona de tiempo inactiva en puerta (tarjeta)	21	Excepción	192.168.1.79	0125134700010
Fuera de horario permitido	22	Excepción	192.168.1.79	0125134700010
Acceso denegado	23	Excepción	192.168.1.79	0125134700010

Para más detalles acerca de Tipo de Evento, consulte Tipo de Evento de Elevador.

5.1.6 Monitoreo de Dispositivos

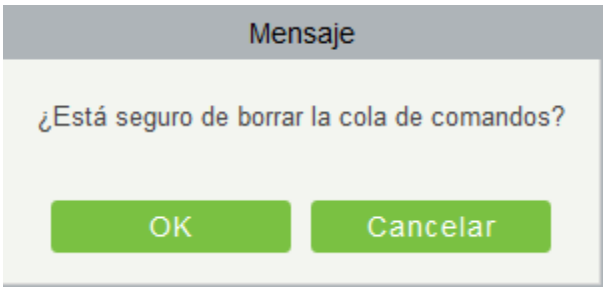
Por defecto se monitorea todos los dispositivos dentro del nivel actual del usuario. De clic en [Elevador] > [Dispositivos] y se mostrará la información y operaciones de los dispositivos: Nombre de Dispositivo, No. de Serie, Área, Operación, Estado Actual, Lista de Comandos y operaciones relacionadas.

Área | Estado --------- | Nombre de Dispositivo | Número de Serie

Exportar

Nombre de Dispositivo	Número de Serie	Área	Operación	Estado Actual	Lista de Comandos	Estado Anormal Reciente	Operaciones
192.168.1.79	0125134700010	Nombre de Área	Obtener eventos en tiempo	Normal	0	Ninguno	Limpiar Comando

Es posible limpiar la lista de comandos dando clic en [Limpiar Comando] en el dispositivo correspondiente:



De clic en [OK] para limpiar.

✍**Notas:**

(1) Después de ejecutar Limpiar Comando, puede realizar Sincronizar Todos los Datos para volver a sincronizar la información del software a los dispositivos, pero esta operación no puede realizarse cuando la capacidad de

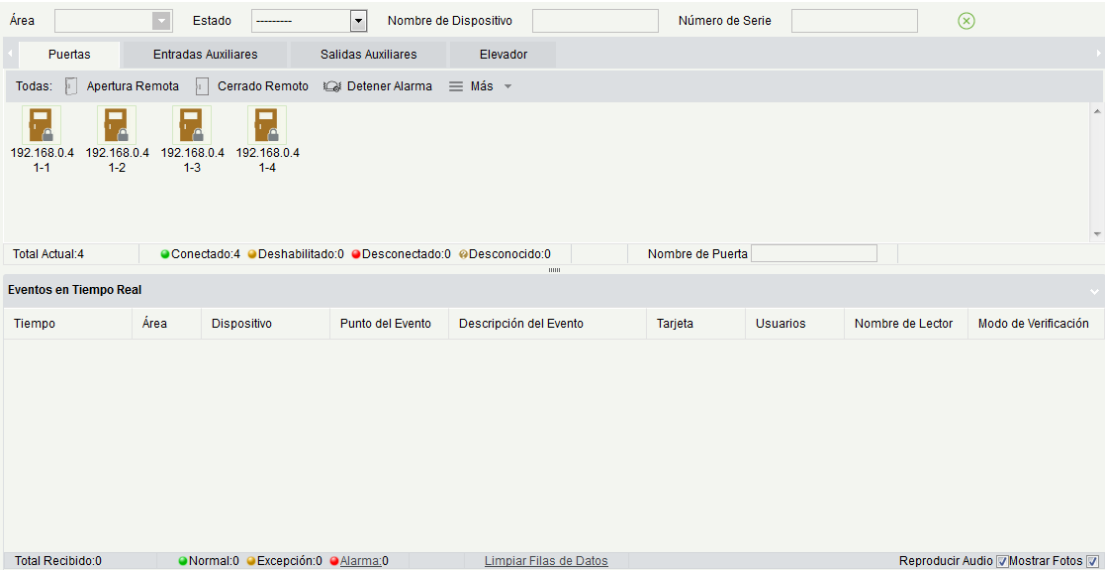
usuarios y huellas digitales se encuentra al máximo en el equipo. Una vez que la capacidad es insuficiente, será necesario reemplazar el dispositivo actual por otro de mayor capacidad o eliminar el privilegio de acceso al dispositivo y después realizar la operación de Sincronizar Todos los Datos.

(2) Estado de Operación es el contenido de las comunicaciones del dispositivo actual, usado principalmente para depuración.

(3) Si el número de comandos para realizar es mayor de 0, esto indica que existen datos que no se han sincronizado con el dispositivo, en este caso, espere un momento.

5.1.7 Monitoreo en Tiempo Real

De clic en [Elevador] > [Dispositivos] > [Monitoreo en Tiempo Real] para monitorear el estado y los eventos en tiempo real de las puertas de los paneles de elevador, incluyendo eventos normales, anormales, alarmas, vínculos, etc. La interfaz de monitoreo en tiempo real se muestra a continuación:



1. Monitoreo De Eventos

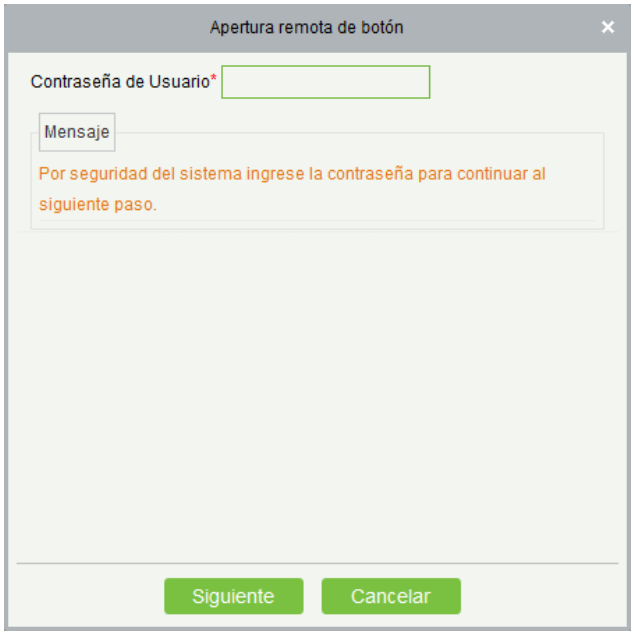
El sistema obtiene automáticamente los eventos de los dispositivos (por defecto muestra 200 eventos), incluyendo eventos de acceso normales y anormales (incluyendo alarmas). Los eventos normales se muestran en color verde, los eventos de alarma en rojo y otros eventos anormales en naranja.

Monitoreo de Áreas: Por defecto, se monitorean todos los pisos del dispositivo de elevador. Es posible filtrar el monitoreo de los pisos por Área, Estado, Nombre de Dispositivo y No. de Serie.

Mostrar Fotos: Si está activado se mostrará la foto registrada del usuario al ocurrir una verificación correcta (si no tiene foto registrada, se muestra la imagen defecto). También se muestra el nombre del evento, fecha, hora y nombre.

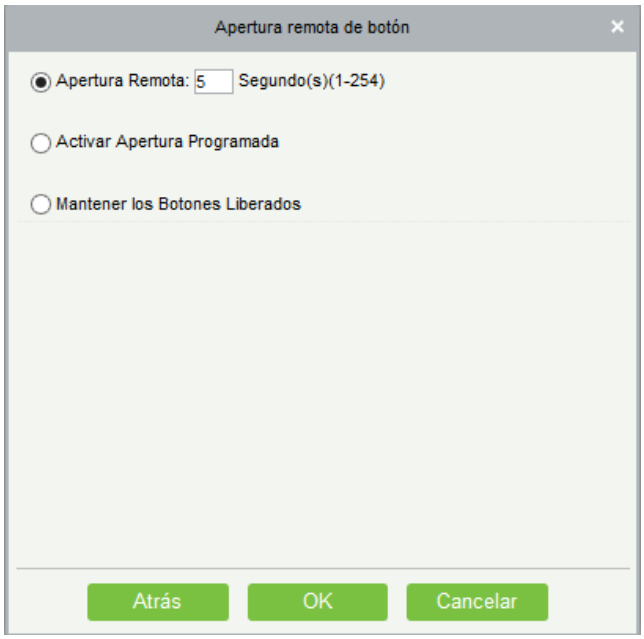
2. Liberación de Botón Remoto

De clic en [Apertura Remota de Botón]:



Introduzca la contraseña de usuario (la contraseña de inicio de sesión), luego de clic en [Siguiente]:

Seleccione el piso y de clic en [Siguiente]:



Descripción de los campos:

Apertura Remota: Determina cuando la tecla correspondiente al piso seleccionado puede ser presionada. Es posible personalizar la duración de la liberación de la tecla (15seg por defecto), o seleccionar el horario de liberación programado. También es posible establecer el estado del piso en liberación continua. En este caso, el piso no estará sujeto a restricciones de horarios, incluyendo el horario de piso activo, horario programado o duración de apertura de botón. En otras palabras, el piso estará liberado continuamente las 24 horas todos los días.

Habilitar Horario de Apertura Programado: Para detener el acceso a un piso, primero debe deshabilitar el horario de apertura programado para prevenir que el piso sea liberado debido a que otros horarios de apertura tomen efecto. Después deberá cerrarlo con Bloqueo de Botón Remoto.

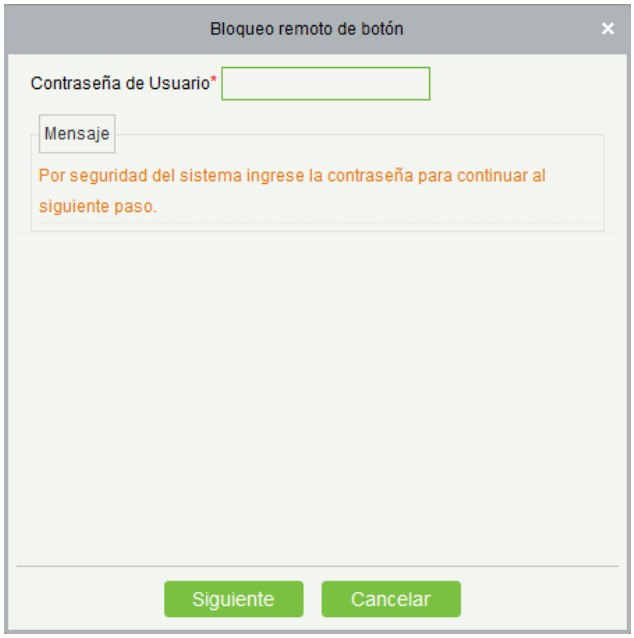
Liberación de Botón Continua: El piso que se mantiene en estado de liberación continua no está sujeto a restricciones de horarios, esto significa que estará continuamente liberado las 24 horas cada día. Para detener la liberación del piso, debe seleccionar Desactivar Horario de Liberación.

✍Nota: Si se muestra continuamente un mensaje de error al liberar remotamente, revise si están los dispositivos desconectados en la lista de dispositivos o la conexión de la red.

Seleccione las opciones y de clic en [Completar] para terminar de habilitar el botón.

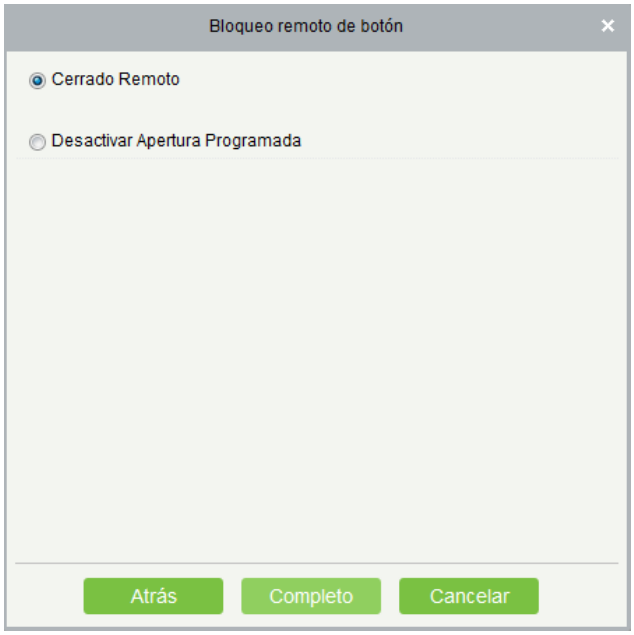
2. Bloqueo Remoto de Botón

De clic en [Bloqueo Remoto de Botón]:



Introduzca la contraseña de usuario (la contraseña de inicio de sesión), luego de clic en [Siguiente]:

Seleccione el piso y de clic en [Siguiente]:



Descripción de los campos:

Bloqueo Remoto de Botón: Bloquea el botón liberado remotamente.

✍Nota: Si un mensaje de falla es devuelto, revise que el dispositivo no se encuentre desconectado o revise la conexión de red.

Seleccione las opciones y de clic en [Finalizar] para completar el bloqueo del botón.

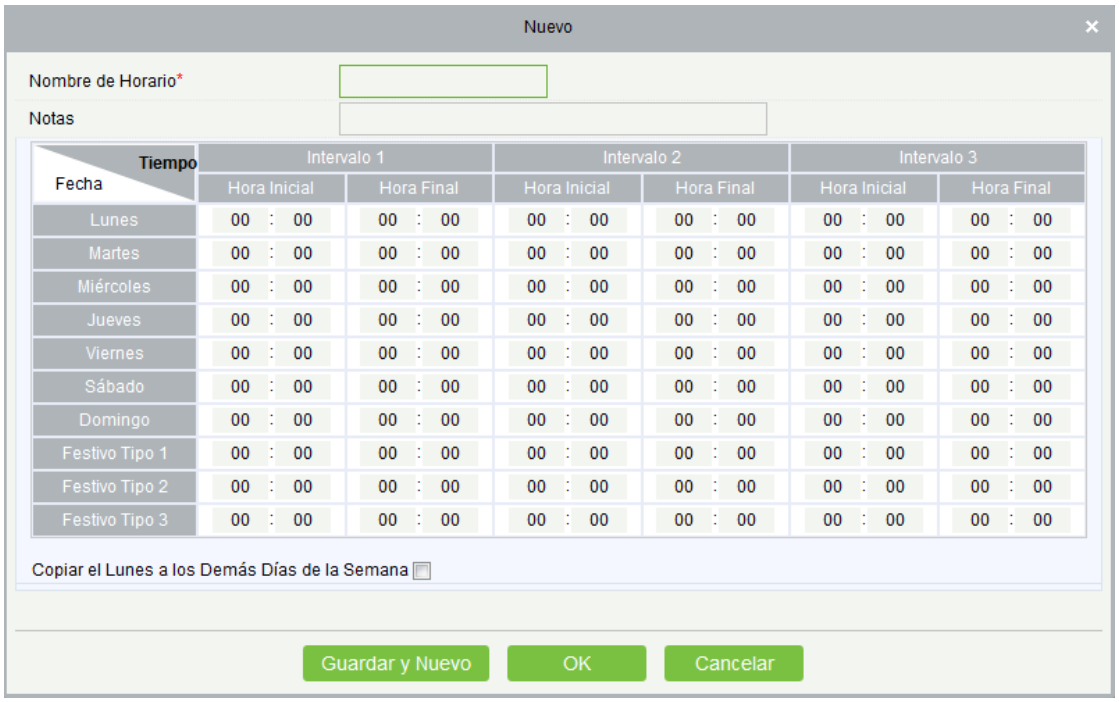
5.2 Reglas de Elevador

Puede controlar los botones de un elevador convencional e implementar la gestión unificada de personas entrando o saliendo de cada piso a través del controlador de elevador. Puede establecer los privilegios del personal registrado para restringir la operación de los botones del elevador.

5.2.1 Horarios de Elevador

1. Agregar Horario de Elevador

(1) De clic en [Elevador] > [Horarios] > [Nuevo] para acceder a la interfaz de edición:



Descripción de los campos:

Nombre de Horario: Cualquier caracter, hasta 30 caracteres.

Notas: Descripción detallada del horario actual, incluyendo la explicación y aplicación del horario. El campo es de 50 caracteres.

Intervalo, Tiempo Inicial y Final: Un horario de control de elevador incluye 3 intervalos para cada día de la semana, y 3 intervalos para cada uno de los días festivos. Configure la hora inicial y final de cada intervalo.

Configuración: Si el intervalo es normalmente abierto, solo introduzca 00:00-23:59 como el intervalo 1 y 00:00-00:00 como el intervalo 2/3. Si el intervalo es normalmente cerrado: todos son 00:00-00:00. Si solo se usa un intervalo, el usuario solo necesita introducir el campo del intervalo 1 y el intervalo 2/3 mantiene el valor defecto. De igual manera, si solo se usan los primeros dos intervalos, el tercer intervalo se mantiene con el valor defecto. Cuando se usan dos o tres intervalos el usuario requiere asegurar que los intervalos no tienen intersección de tiempo y que el tiempo no abarque días, de lo contrario se mostrará un error.

Tipo de Día Festivo: Los tres tipos de días festivos no están relacionados con los días de la semana. Si una fecha se establece a un día festivo, los tres intervalos del día festivo se usarán para acceso. El tipo de día festivo es opcional. Si no ingresa ninguno el sistema usará el valor defecto.

Copiar el Lunes: Puede copiar rápidamente el horario del lunes a los demás días de la semana.

(2) Después de configurar, de clic en [OK] para guardar, y el horario se mostrará en la lista.

2. Mantenimiento de Horarios de Elevador

Editar: De clic en [Editar] para acceder a la interfaz de editar. De clic en [OK] para guardar los cambios.

Borrar: De clic en [Borrar] y luego clic en [OK] para borrar, o de clic en [Cancelar] para cancelar la operación. Un horario en uso no puede ser eliminado. Puede borrar múltiples horarios seleccionando las casillas y dando clic en [Borrar] arriba de la lista y [OK] para borrar o clic en [Cancelar] para cancelar.

5.2.2 Días Festivos de Elevador

El horario de control de elevador puede ser diferente en un día festivo. El sistema permite la configuración de horarios para los días festivos, incluyendo las funciones Agregar, Modificar y Borrar.

- Agregar

(1) De clic en [Elevador] > [Días Festivos] > [Agregar] para acceder a la interfaz de edición:

Descripción de los campos:

Nombre de Día Festivo: Cualquier caracter. Máximo 30.

Tipo de Día Festivo: Festivo Tipo 1, 2 ó 3. Un día festivo pertenece a uno de los tipos y cada tipo puede incluir hasta 32 días festivos.

Fecha Inicial / Final: El formato de fecha es: 2010-1-1. La fecha inicial no puede ser posterior a la fecha final, de lo contrario se mostrará un error. El año de la fecha inicial no puede ser anterior al año actual y no puede abarcar años diferentes.

Recurrente: Indica si la fecha de un día festivo es igual todos los años. Por ejemplo, el día de año siempre es el 1 de enero y puede establecerlo como Si, pero, por ejemplo, el día del padre se celebra el tercer domingo de junio y por lo tanto no es fijo. En casos como este se establecería como No.

(2) Después de editar, de clic en [OK] para guardar y se mostrará en la lista de días festivos.

- Editar

De clic en el nombre del día festivo o en [Editar] para acceder a la interfaz. Después de realizar la modificación, de clic en [OK] para guardar y salir.

- Borrar

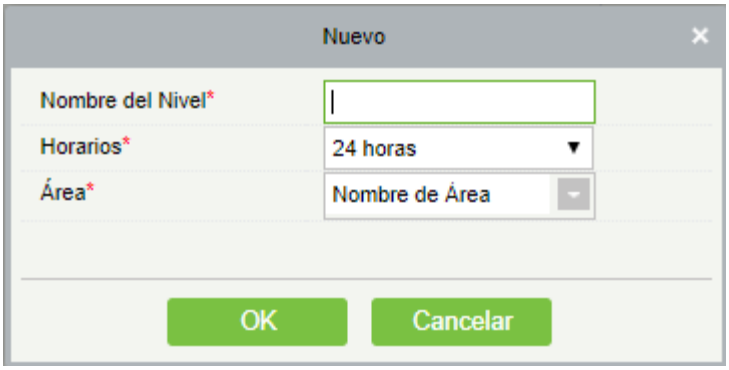
En la lista de días festivos, de clic en [Borrar]. De clic en [OK] para borrar o de clic en [Cancelar] para cancelar la operación. Un día festivo en uso no puede ser borrado.

5.2.3 Niveles de Acceso de Elevador

Los niveles de acceso de elevador indican si los usuarios pueden acceder a uno o varios pisos seleccionados mediante la verificación de acceso y una combinación de horario.

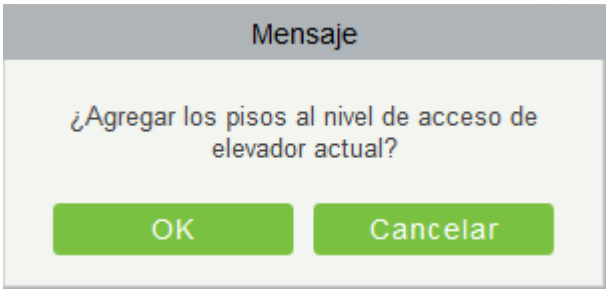
- Agregar

1. De clic en [Elevador] > [Niveles de Acceso de Elevador] > [Agregar] para acceder a la interfaz de edición:



2. Introduzca los parámetros: Nombre del Nivel (no repetir) y Horario.

3. De clic en [OK] y el sistema mostrará "¿Desea agregar puertas al nivel de acceso?", de clic en [OK] to para agregar puertas o en [Cancelar] para regresar a la lista de niveles de acceso. El nivel de acceso agregado se mostrará en la lista.



✍Note: Es posible seleccionar y agregar pisos de diferentes paneles en un nivel de acceso de elevador.

- Por Niveles

Agregar/Borrar personal de los niveles seleccionados:

(1) De clic en [Elevador] > [Por Niveles] para acceder a la interfaz de edición, de clic en el nivel de acceso de la lista de la izquierda y el personal que tiene el privilegio para abrir la puerta en este nivel será mostrado en la lista de la derecha.

(2) En la lista de la izquierda, de clic en [Agregar Usuarios] debajo de operaciones para emerger la ventana de agregar de agregar personal; seleccione el personal (múltiple) de clic en > para mover a la lista de la derecha, después de clic en [OK] para guardar y salir.

(3) De clic en el nivel para ver el personal en la lista de la derecha. Seleccione el personal y de clic en [Borrar Personal] arriba de la lista de la derecha y de clic en [OK] para borrar.

- Por Usuarios

Agregar/borrar personal de los niveles de acceso seleccionados:

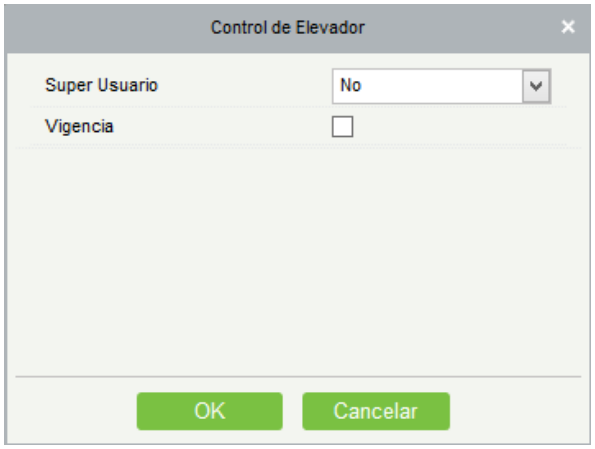
(1) De clic en [Elevador] > [Por Usuario], de clic en el usuario para ver sus respectivos niveles en la lista de la derecha.

(2) De clic en [Agregar a los Niveles] debajo de Operaciones para emerger la ventana de Agregar a los Niveles, seleccione el nivel (múltiple) y de clic en > para mover los seleccionados a la lista de la derecha; de clic en [OK] para guardar y salir.

(3) Seleccione el nivel (múltiple) de la lista de la derecha, y de clic en [Borrar de los Niveles] arriba de la lista y de clic en [OK] para borrar el personal de los niveles seleccionados.

Asignar Nivel de Acceso de Elevador al Personal Seleccionado:

(1) Seleccione un usuario de la lista de la izquierda y de clic en el botón [Control de Elevador]. Se muestra la siguiente ventana:



(2) Establezca los parámetros de control de acceso de elevador y de clic en [OK] para guardar los ajustes.

- Por Departamento

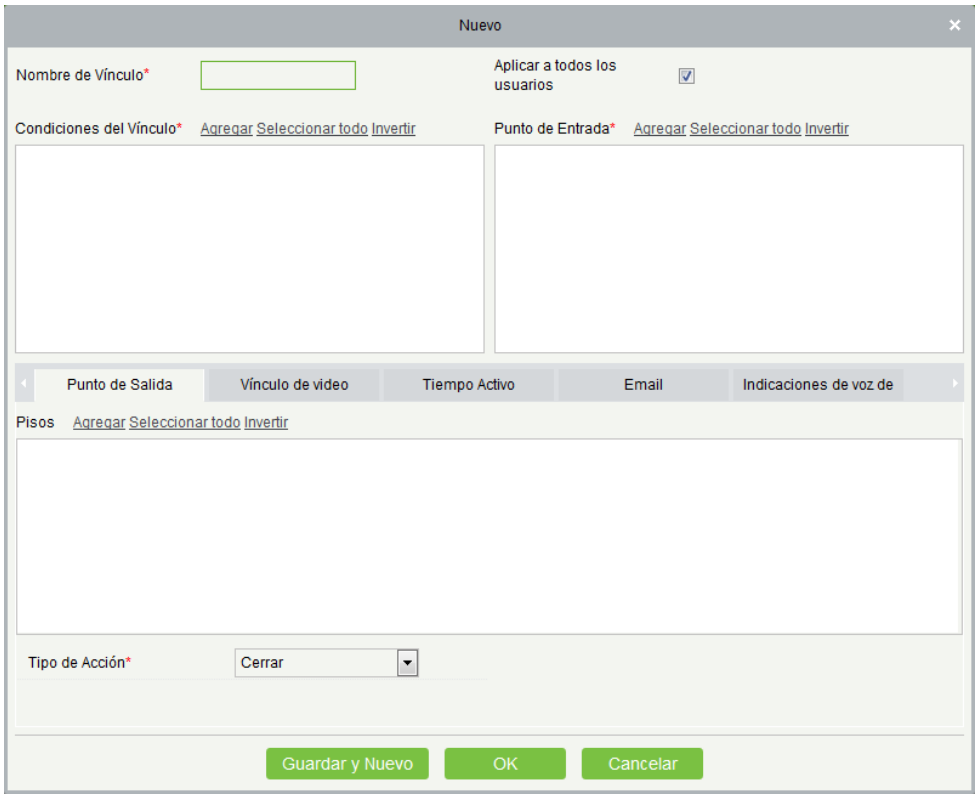
Agregue o remueva el departamento seleccionado de los niveles de acceso o elevador. Los privilegios de acceso del personal del departamento serán modificados.

5.2.4 Vínculos Globales

Los vínculos globales permiten configurar datos entre dispositivos. Solo los dispositivos con firmware PUSH soportan esta función.

- Agregar

1. De clic en [Elevador] > [Elevador] > [Vínculos Globales] > [Nuevo]:



Descripción de los campos:

Nombre del Vínculo: Introduzca el nombre del vínculo.

Condición del Vínculo: La condición del vínculo es el tipo de evento del dispositivo seleccionado. Todos los eventos pueden ser condiciones de vínculo excepto detener alarma, habilitar/deshabilitar salida auxiliar y dispositivo inicializado.

Punto de Entrada: Puede ser, Puerta 1, 2, 3 y 4, Entrada Auxiliar 1, 2, 3, 4, 9, 10, 11, 12 (los puntos de entrada varían según el modelo y especificaciones de cada dispositivo).

Punto de Salida: Puerta 1, 2, 3, y 4, Salida Auxiliar 1, 2, 3, 4, 6, 8, 9, 10 (los puntos de salida varían según el modelo y especificaciones de cada dispositivo).

Acción del Vínculo: Abrir, Cerrar, Normalmente Abierto. El defecto es Cerrar. Para Abrir, deberá introducir el tiempo de retardo o seleccionar Normalmente Abierto.

Vínculo de Video:

✧ Pop-Up de Video: Si se habilita, emergerá una ventana de vista previa de video en la interfaz de monitoreo en

tiempo real. Deberá introducir el tiempo de retardo.

- ✧ Video: Si se habilita, se guarda el video de la cámara asociada. Deberá introducir el tiempo de duración de la grabación.
- ✧ Captura: Si se habilita, se guarda la captura del evento.

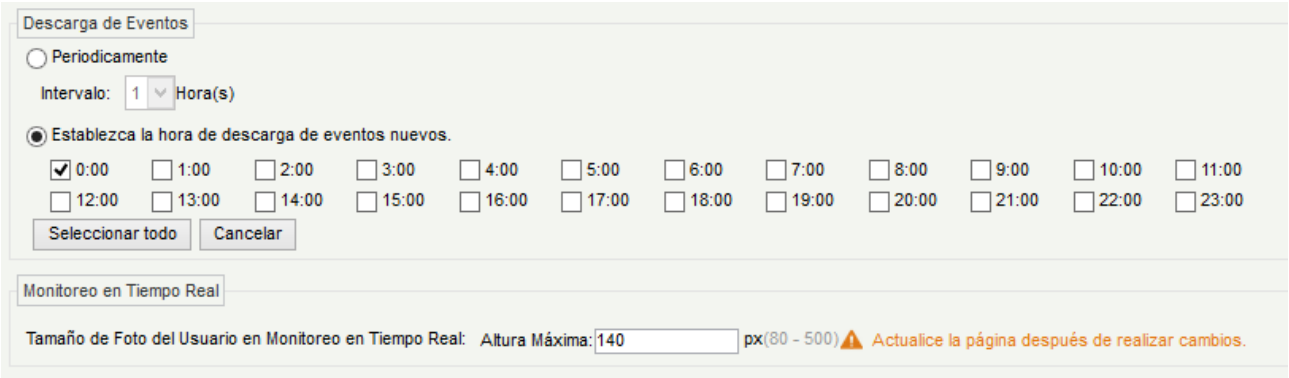
Retardo: El rango es de 1 a 254s (este campo es válido cuando la acción es Abrir).

2. De clic en [OK] para guardar y salir. El vínculo agregado se mostrará en la lista.

✍Nota: No es permitido configurar el vínculo para el mismo punto de entrada y de salida. El mismo dispositivo permite ajustes consecutivos de vinculación lógica. El sistema permite establecer varias condiciones de vínculo al mismo tiempo.

5.2.5 Parámetros

1. De clic en [Elevador] > [Elevador] > [Parámetros]:



Tipos de Descargas de Eventos

- Periódicamente

El sistema intentará descargar los eventos cada intervalo de tiempo. Comienza a partir de la hora en que se establece la configuración.

- Establezca la hora de descarga de eventos nuevos

Si se selecciona la hora, el sistema intentará descargar los eventos nuevos automáticamente.

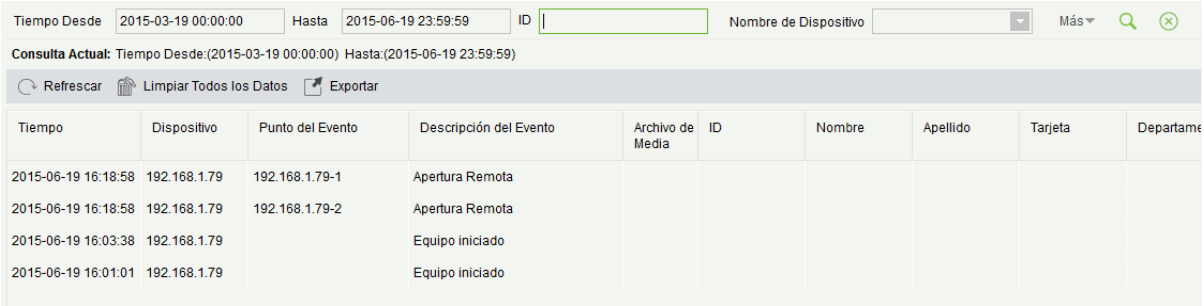
Email de Destinatario de Monitoreo de Alarmas: El sistema enviará un correo electrónico al motorista de alarmas cuando ocurra un evento de alarma.

5.3 Reportes de Elevador

Incluye todos los Eventos y Eventos de Excepción. Es posible exportar los datos después de realizar la consulta.

5.3.1 Todos los Eventos

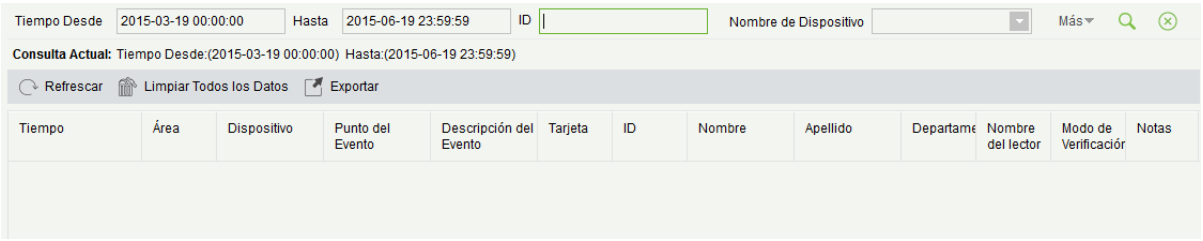
Dado que el tamaño de los datos de acceso puede ser muy grande, es posible ver los eventos de control de acceso después de filtrar condiciones específicas. Por defecto, el sistema mostrará los eventos de los últimos tres meses. De clic en [Reportes] > [Todos los Eventos] para ver todos los eventos:



Limpiar Todos los Datos: De clic en [Limpiar Todos los Datos] para emerger una ventana y de clic en [OK] para limpiar todos los datos del periodo de tiempo seleccionado.

5.3.2 Eventos de Excepción

De clic en [Reportes] > [Eventos de Excepción] para ver los eventos de excepción en las condiciones especificadas. Las opciones son las mismas que en [Todos los Eventos].

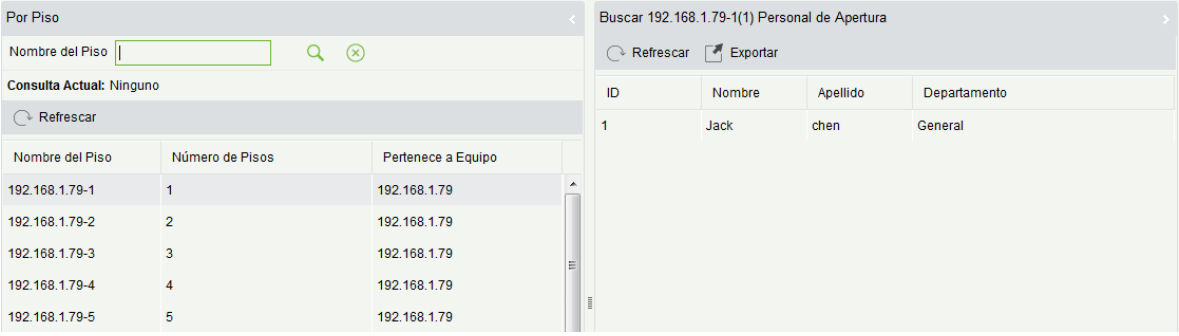


Limpiar Todos Los Eventos: De clic en [Limpiar Todos Los Eventos] para emerger una ventana y de clic en [OK] para limpiar los eventos de excepción.

5.3.3 Privilegios de Acceso

- Por Piso

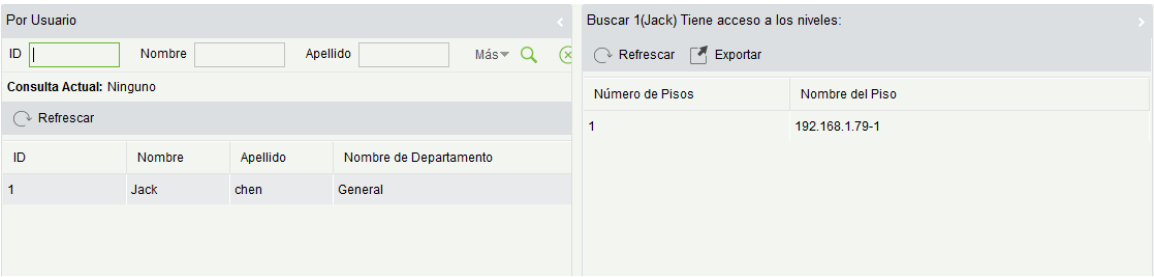
Ver los niveles de acceso por piso. De clic en [Reportes] > [Por Piso], la lista de datos en la izquierda muestra todas las puertas en el sistema, seleccione un piso y se mostrará el personal que tiene el nivel de acceso al piso en la lista de la derecha.



Por Usuario

Ver los niveles de acceso por personal.

De clic en [Reportes] > [Por Usuario], la lista de datos en la izquierda muestra todos los usuarios, seleccione un usuario y se mostrarán los pisos a los que el personal tiene acceso en la lista de la derecha.



6 Módulo de Hotel

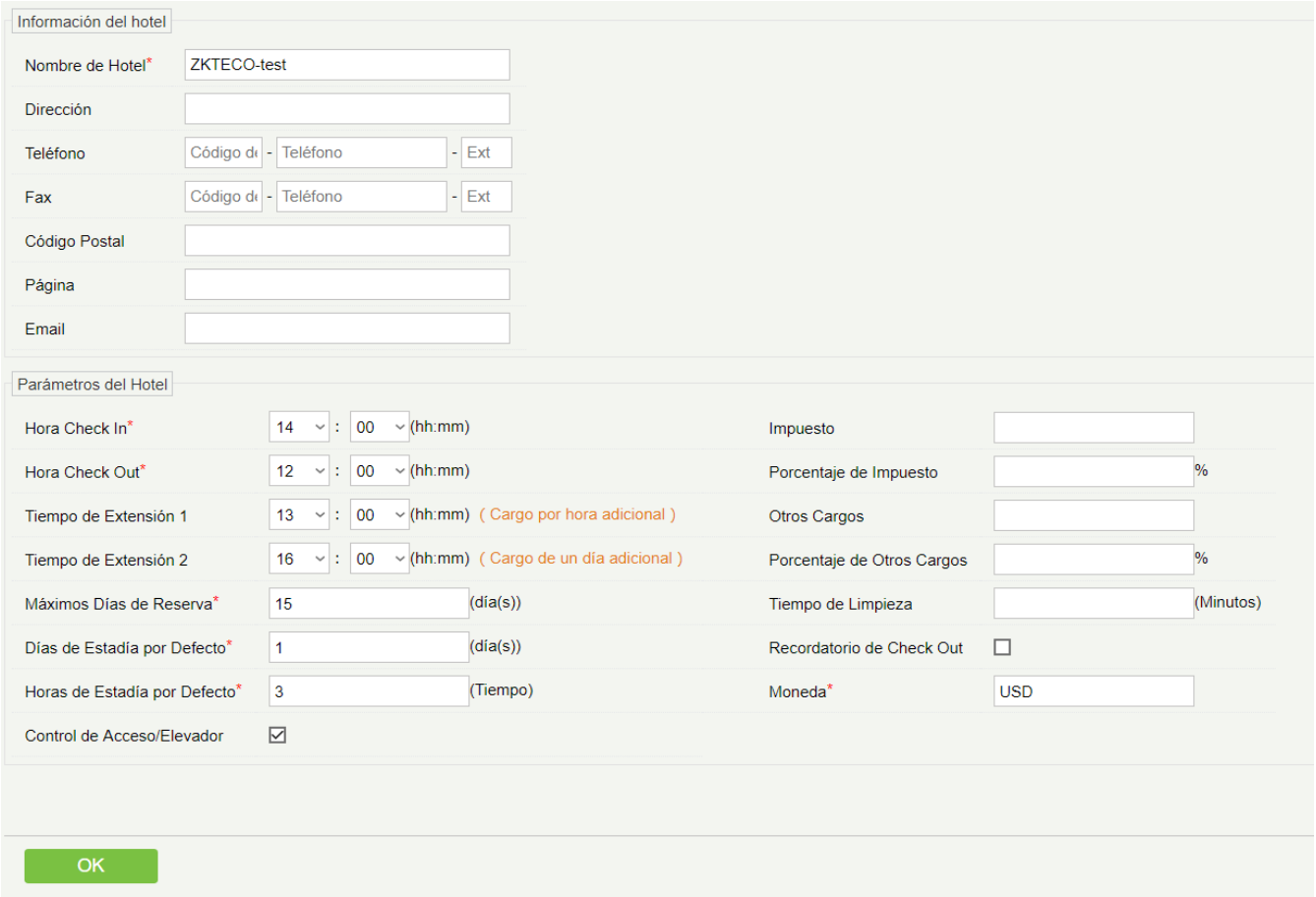
El módulo de hotel brinda funciones para configuración de cerraduras y gestión de huéspedes como check in, check out, extensión de estadía, tarifas, entre otras.

- Guía de Operación

Le ayuda para aprender rápidamente como navegar las funciones específicas, configurar y usar el módulo de hotel.

6.1 Información de Hotel

Puede establecer la información básica del hotel incluyendo el nombre, dirección, teléfono, fax, código postal, sitio web y correo electrónico. También permite establecer los parámetros relacionados con la hora de check in, check out, notificación de check out y los privilegios de acceso y elevador.
Seleccione **Habitaciones** > **Información de Hotel.** Se mostrará la siguiente página:



Los campos se describen a continuación:

Hora Check In: Establece la hora de entrada del huésped. Si el huésped realiza el check in antes de esa hora, el check out será el día actual si el huésped se hospeda por un día, de lo contrario el check out será el día siguiente.
Hora Check Out: Especifica la hora de finalización de la estadía de un día.
Tiempo de Extensión 1/2: Puede definir este tiempo. Si un huésped realiza el check out entre el tiempo de

extensión 1 y 2, el huésped deberá pagar un cargo por exceso de tiempo. Si un huésped realiza el check out después del tiempo de extensión 2, deberá pagar por un día extra.
Días de Estadía por Defecto: Especifica el número de días de estadía por defecto, usualmente 1 día.
Horas de Estadía por Defecto: Especifica el número mínimo de horas que puede permanecer un huésped. Si un huésped permanece por un tiempo menor a este, se le cobrará la tarifa correspondiente a este límite.
Tiempo de Limpieza: Especifica el tiempo disponible para asear una habitación después de que el huésped haya realizado el check out.
Recordatorio de Check Out: Especifica si desea mostrar un recordatorio una hora antes del check out. **Moneda**: Especifica el tipo de moneda.
Control de Acceso/Elevador: Después de marcar la casilla, puede seleccionar un nivel de acceso o elevador en la interfaz de gestión de tarjetas, de modo que una tarjeta emitida pueda utilizarse no solo como tarjeta de hotel sino también para acceder a los dispositivos correspondientes del nivel seleccionado. (Nota: Esta casilla solo estará disponible en la página de Información de Hotel después de usar el módulo de acceso y elevador y activar la licencia correspondiente).

Nota: El módulo de hotel puede ser utilizado para definir edificios, pisos y habitaciones además de gestionar las solicitudes de check in solo después de configurar estos parámetros.

6.2 Habitaciones

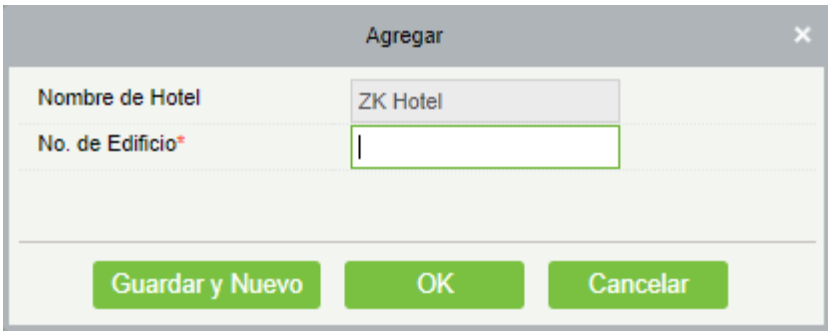
6.2.1 Tipos de Habitación

Puede introducir información sobre los diferentes tipos de habitación tal como el número de camas y número de huéspedes permitidos. Puede bloquear y desbloquear habitaciones vacías.
Seleccione **Habitaciones** > **Tipos de Habitación** > **Nuevo**. Se mostrará la siguiente interfaz:

Nota: Al agregar un tipo de habitación, el sistema verifica si existe la información de hotel configurada. Si no, será redirigido a la página de información de hotel. Los tipos de habitación no deben repetirse.

6.2.2 Edificios

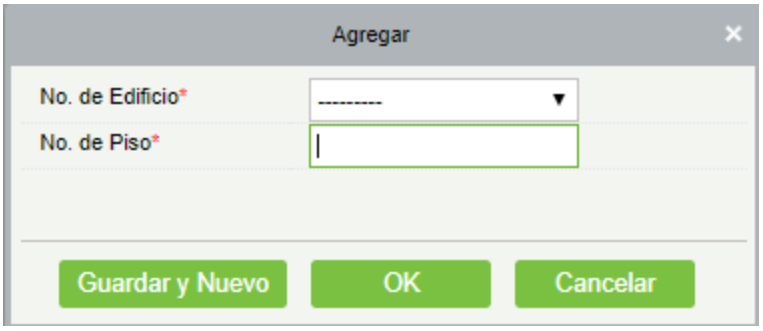
Puede definir los edificios del hotel. Cuando las habitaciones de un edificio no están reservadas o los huéspedes no se han registrado en las habitaciones puede bloquear o desbloquear el edificio.
Seleccione **Habitaciones** > **Edificios** > **Nuevo**. Se mostrará la siguiente interfaz:



Note: Al agregar un edificio, el sistema verifica si existe la información de hotel y tipos de habitación configurada en ese orden. Si no, será necesario realizar la configuración primero. Los edificios no deben repetirse.

6.2.3 Pisos

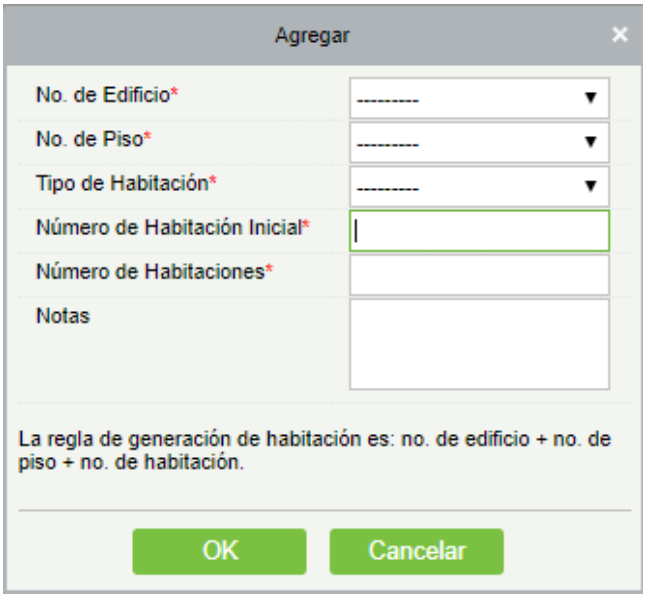
Puede definir los pisos del hotel. Cuando las habitaciones de un piso no están reservadas o los huéspedes no se han registrado en las habitaciones puede bloquear o desbloquear el piso.
Seleccione **Habitaciones** > **Pisos** > **Nuevo**. Se mostrará la siguiente interfaz:



6.2.4 Habitaciones

- **Agregar habitaciones de huésped**

Seleccione **Habitaciones** > **Habitaciones** > **Agregar**. Se mostrará la siguiente interfaz:



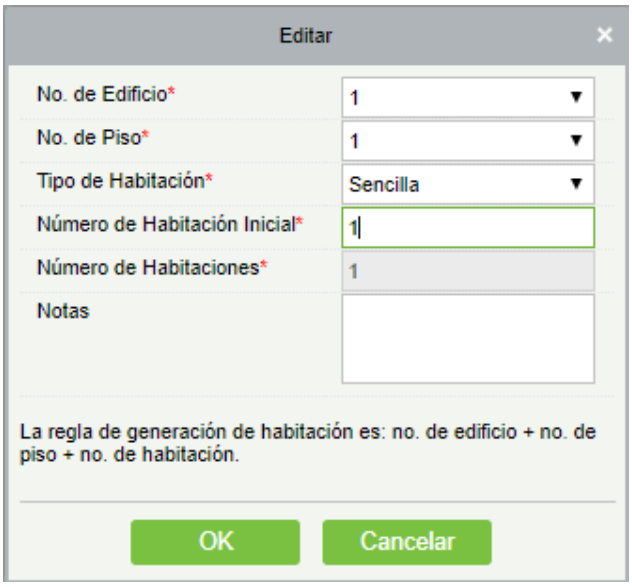
Número de Habitación Inicial: Especifica el número inicial de las habitaciones.
Número de Habitaciones: Especifica las habitaciones que se agregarán. El valor 1 indica que solo se agregará una habitación. Un valor mayor de 1 indica que se agregarán un lote de habitaciones.
Notas: Describe las habitaciones agregadas.

Nota: Las habitaciones no se pueden repetir.

- **Editar habitación**

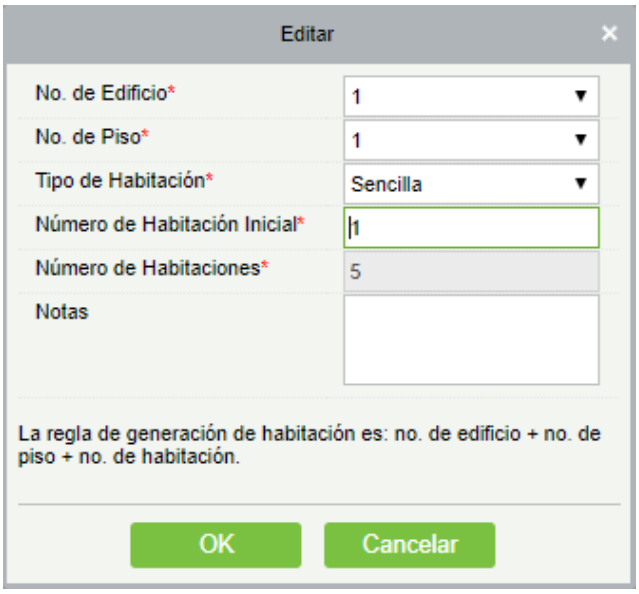
1) Editar una habitación

Seleccione una habitación y edite. No se permiten habitaciones duplicadas. Las habitaciones que han registrado algún huésped no podrán ser editadas. Vea la siguiente imagen:



2) Editar habitaciones por lote

Seleccione las casillas de las habitaciones y de clic en Editar para editar por lote. No se permiten habitaciones duplicadas. Solo las habitaciones que sean del mismo tipo y correspondan al mismo edificio podrán ser editadas por lote. Vea la siguiente imagen:



- **Borrar habitaciones**

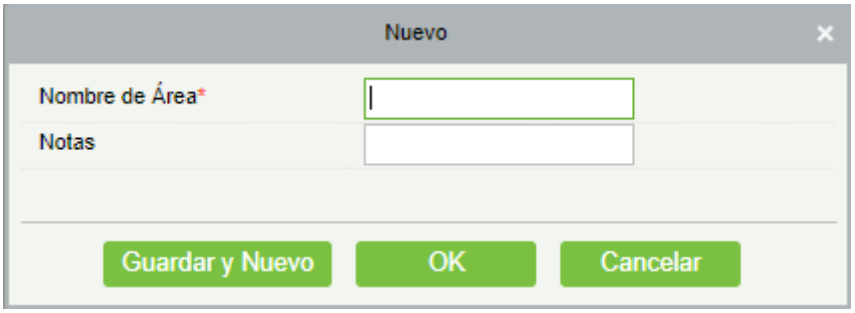
Seleccione una o más habitaciones y de clic en Borrar. Solo las habitaciones que no contengan huéspedes registrados podrán ser eliminadas.

- **Exportar la información de las habitaciones**

Consulte las operaciones comunes en Anexos.

6.2.5 Áreas

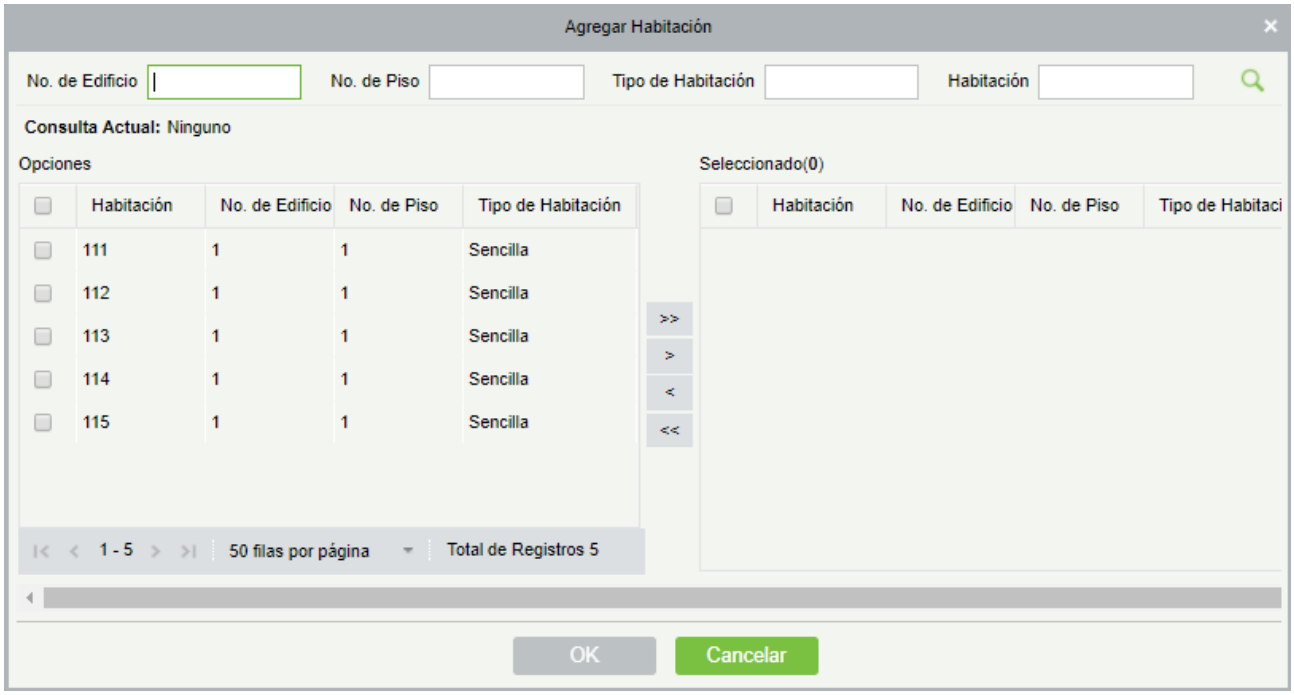
Es posible definir las áreas de las habitaciones, asignar una tarjeta para el área y asociar las cerraduras de las habitaciones del área, de modo que el administrador del hotel puede utilizar la tarjeta para gestionar todas las habitaciones del área.
Seleccione **Habitaciones** > **Áreas** > **Nuevo**. Se mostrará la siguiente interfaz:



Nota:

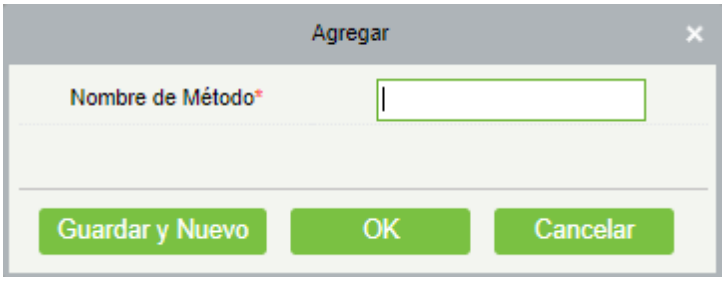
No se permiten nombres de área duplicados.

De clic en **Agregar Habitación** y agregue las habitaciones al área. Vea la siguiente imagen:



6.2.6 Métodos de Reserva

Puede definir los métodos de reservación de las habitaciones del hotel. Durante la instalación del Sistema, los métodos de reserva básicos son inicializados por defecto y no pueden ser editados o borrados.
Seleccione **Habitaciones** > **Métodos de Reserva** > **Nuevo.** Se mostrará la siguiente interfaz:

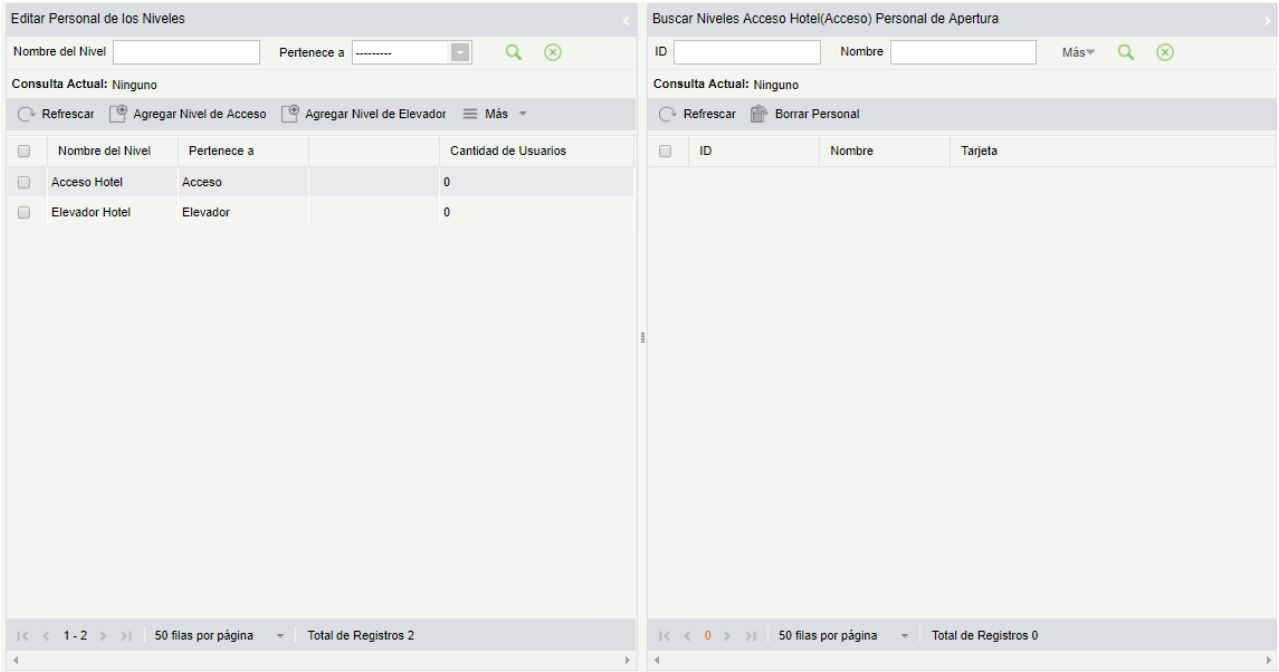


Nota: No se permiten nombres duplicados. Los métodos no usados pueden ser eliminados.

6.2.7 Control de Acceso/Elevador

Es posible asignar niveles de acceso y elevador a las tarjetas emitidas usando el módulo de hotel. Esto permite al usuario utilizar la misma tarjeta para el módulo de hotel y el módulo de acceso y elevador. Es decir, una tarjeta del módulo de hotel puede tener acceso a todos los dispositivos del nivel de acceso o elevador especificado.

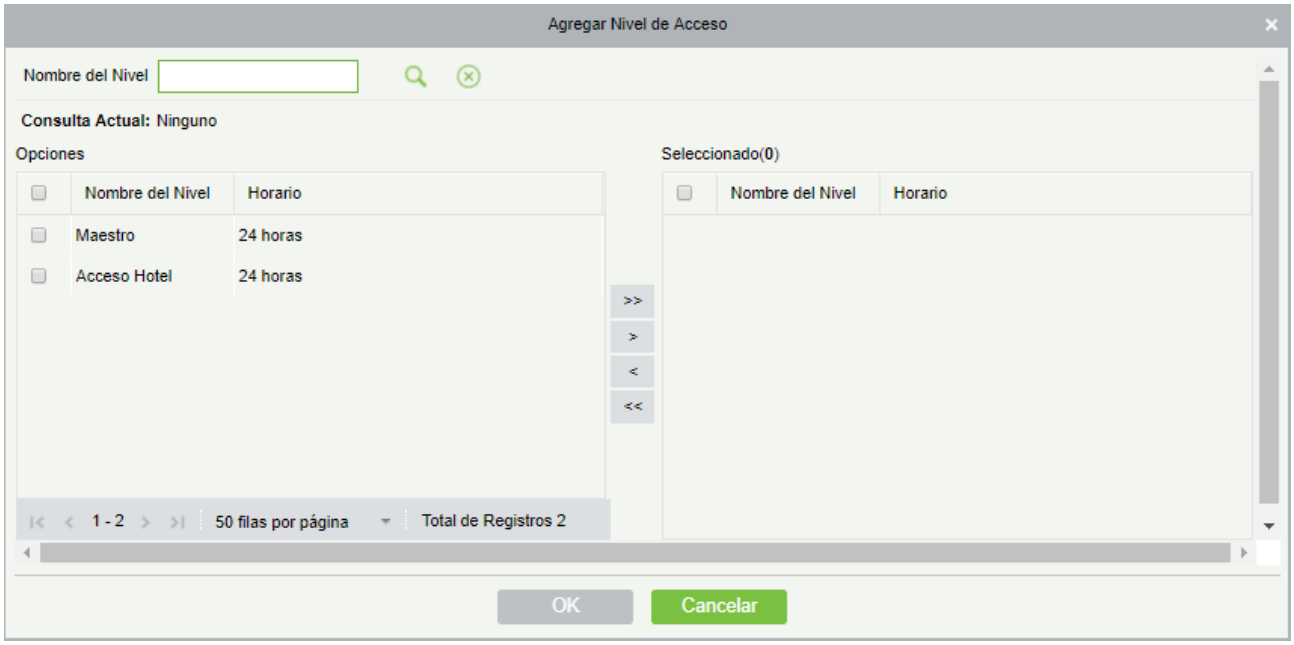
Nota: Esta función y la página de Editar Niveles de Personal solo estarán disponibles después de usar el módulo de acceso y elevador y activar las licencias correspondientes.
Seleccione **Habitaciones** > Control de **Acceso/Elevador**. Se mostrará la siguiente interfaz:



Puede agregar y borrar niveles de acceso y elevador, sincronizar los niveles, examinar y borrar los niveles del personal. Para borrar un usuario de un nivel, será necesario cancelar la tarjeta en vez de borrarlo directamente de ésta página, a menos de que pierda la tarjeta u ocurra una emergencia.

- **Agregar un nivel**

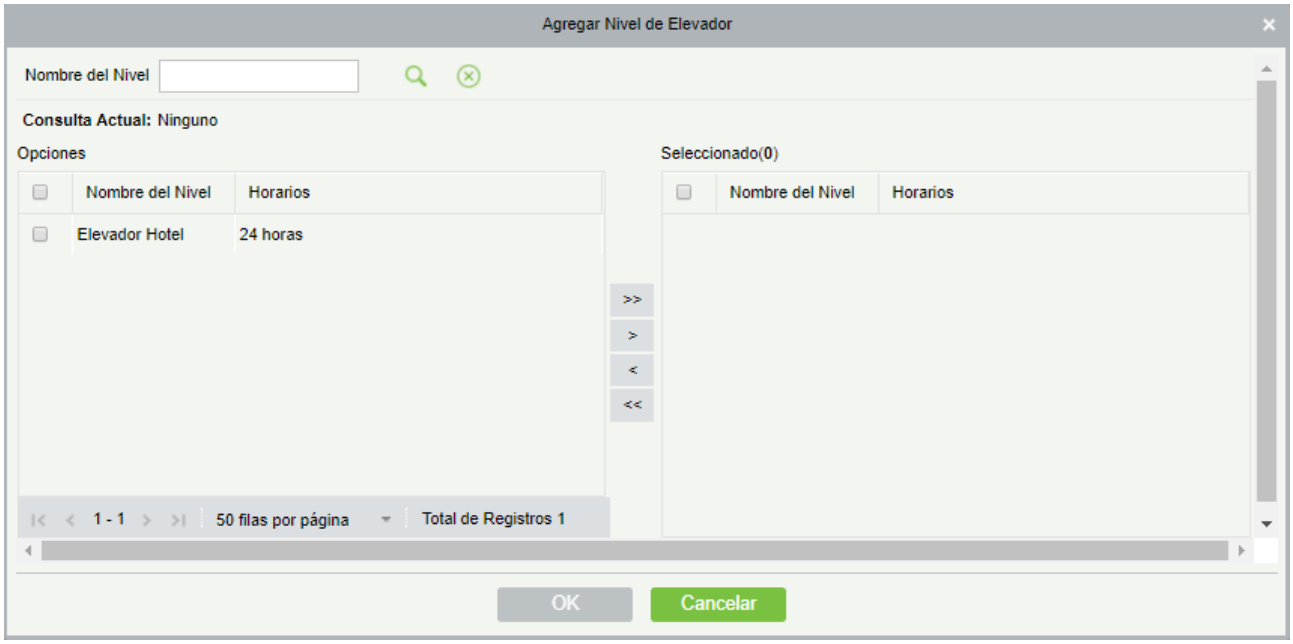
De clic en **Agregar Nivel de Acceso**. Se mostrará la siguiente interfaz:



Seleccione el nivel de acceso que será agregado y de clic en **OK**. Agregue el nivel de acceso del **Piso 1 del Edificio A** de la lista de niveles. Vea la imagen anterior. Si usted selecciona este nivel de acceso en el campo de **Control de Acceso/Elevador** al emitir una tarjeta, la tarjeta puede ser autenticada por todos los dispositivos de control de

acceso del piso 1 en el edificio A y abrir las habitaciones del hotel.

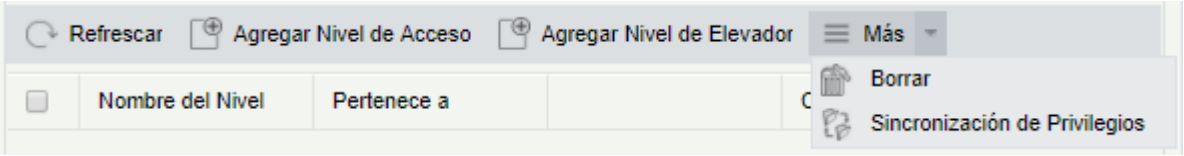
De clic en **Agregar Nivel de Elevador**. Se mostrará la siguiente interfaz:



Seleccione el nivel de elevador que será agregado y de clic en **OK**. Agregue el nivel de elevador del **Piso 6 del Elevador 1** de la lista de niveles. Vea la imagen anterior. Si usted selecciona este nivel de elevador en el campo de **Control de Acceso/Elevador** al emitir una tarjeta, la tarjeta puede llevarlo al piso 6 del elevador 1 y abrir las habitaciones del hotel.

- **Borrar/Sincronizar niveles**

En la página de **Control de Acceso/Elevador**, seleccione un nivel, de clic en **Más**, y seleccione Borrar o Sincronización de Privilegios para sincronizar el nivel seleccionado.



- **Examinar/Borrar personal de niveles**

Cuando selecciona un nivel en la página de **Control de Acceso/Elevador**, la información sobre el personal correspondiente al nivel será mostrada en el lado derecho. Puede seleccionar el personal que desea borrar y dar clic en **Más,** para eliminar el personal seleccionado. Después de ser borrado, el personal no tendrá acceso en los dispositivos incluidos en el nivel.

6.3 Gestión de Tarjetas

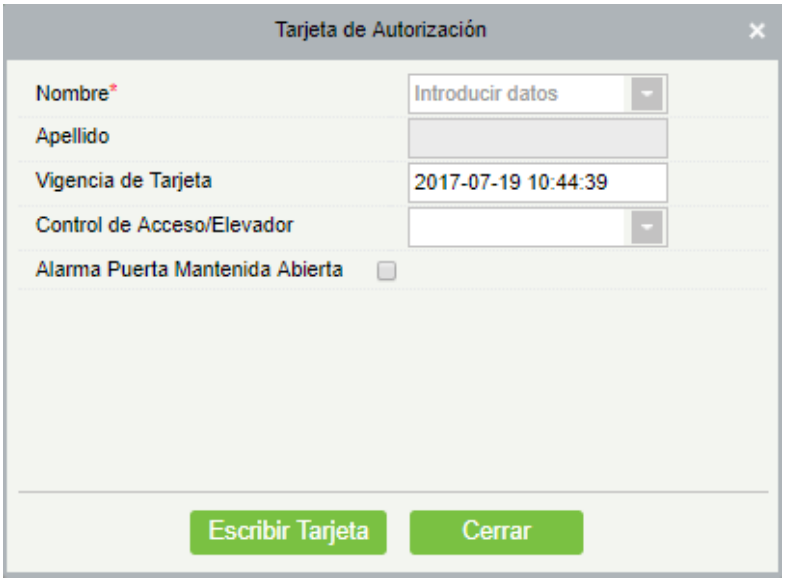
Puede crear diferentes tipos de tarjetas para realizar la configuración y administración de las cerraduras de las habitaciones en función de los requerimientos de gestión diaria del hotel. Los titulares de las tarjetas serán los empleados del hotel. Es necesario agregar los titulares usando el módulo de personal y especificar sus departamentos usando el módulo de hotel, de modo que pueda seleccionar los titulares al emitir las tarjetas de gestión.

6.3.1 Gestión de Tarjetas

Puede configurar la información básica, incluyendo la autorización de hotel, fecha y hora, número de habitación y área de las cerraduras, entre otras.

1. Tarjeta de Autorización

Puede crear tarjetas de autorización para las cerraduras y así vincularlas con la información del hotel para asegurar la seguridad de las tarjetas. Después de autorizar, las cerraduras solo podrán ser desbloqueadas por las tarjetas autorizadas y emitirán una alarma si se intenta usar otras tarjetas para desbloquearlas.



Descripción de los campos:

Nombre: Puede introducir uno o más caracteres contenidos en el apellido o ID del titular de una tarjeta para encontrarlo. El titular debe ser una persona que ha sido agregado usando el módulo de Personal.

Vigencia de Tarjeta: Especifica el tiempo de expiración de la tarjeta. Seleccione la vigencia como sea requerido. La vigencia por defecto es un día después del tiempo actual del sistema.

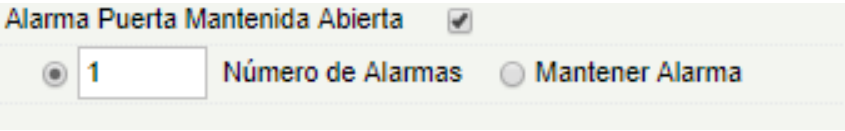
Control de Acceso/Elevador: De clic en la lista para seleccionar un nivel de acceso o elevador. Después de especificar el parámetro, la tarjeta no solo podrá abrir la cerradura de una habitación, sino también acceder a los dispositivos correspondientes al nivel de acceso o elevador.

Notas:

1. El campo de **Control de Acceso/Elevador** solo estará disponible si el campo es habilitado en la página de **Información de Hotel**. Será usado para asignar privilegios a la tarjeta a los dispositivos de acceso o elevador. Para detalles de la configuración consulte Información de Hotel.
2. Para los dispositivos de control de acceso y elevador que no soporten la función de múltiples tarjetas para el personal, solo asigne una tarjeta por usuario. Es decir, solo puede seleccionar una tarjeta por cada opción de **Control de Acceso/Elevador** al asignar tarjetas a los titulares. Como se muestra en la imagen anterior, si el **Control de Acceso/Elevador** está establecido al **Piso 1 del Edificio A** (todos los dispositivos de acceso del piso 1 - edificio A no permiten más de una tarjeta por usuario) cuando una tarjeta de autorización es emitida a un titular, solo la primera tarjeta puede ser asignada con el permiso de acceder al piso 1 del edificio A. No es posible establecer **Control de Acceso/Elevador** al **Piso 1 del Edificio A** al emitir cualquier otra tarjeta al titular.
3. Si un dispositivo permite un usuario con múltiples tarjetas, puede asignar un nivel de acceso o elevador a las múltiples tarjetas. Puede seleccionar el nivel nuevamente al asignar otros tipos de tarjetas o tarjetas continuas al usuario.
4. Los tres puntos anteriores relacionados con control de acceso/elevador son aplicables a todas las tarjetas del módulo de hotel descrito en este documento.
5. Los modelos y versión de firmware de los paneles de control de acceso que permiten la función de múltiples tarjetas al personal son:

   Serie InBioPro: AC Ver 5.7.7.3030 Mar 23 2017 y versiones superiores.

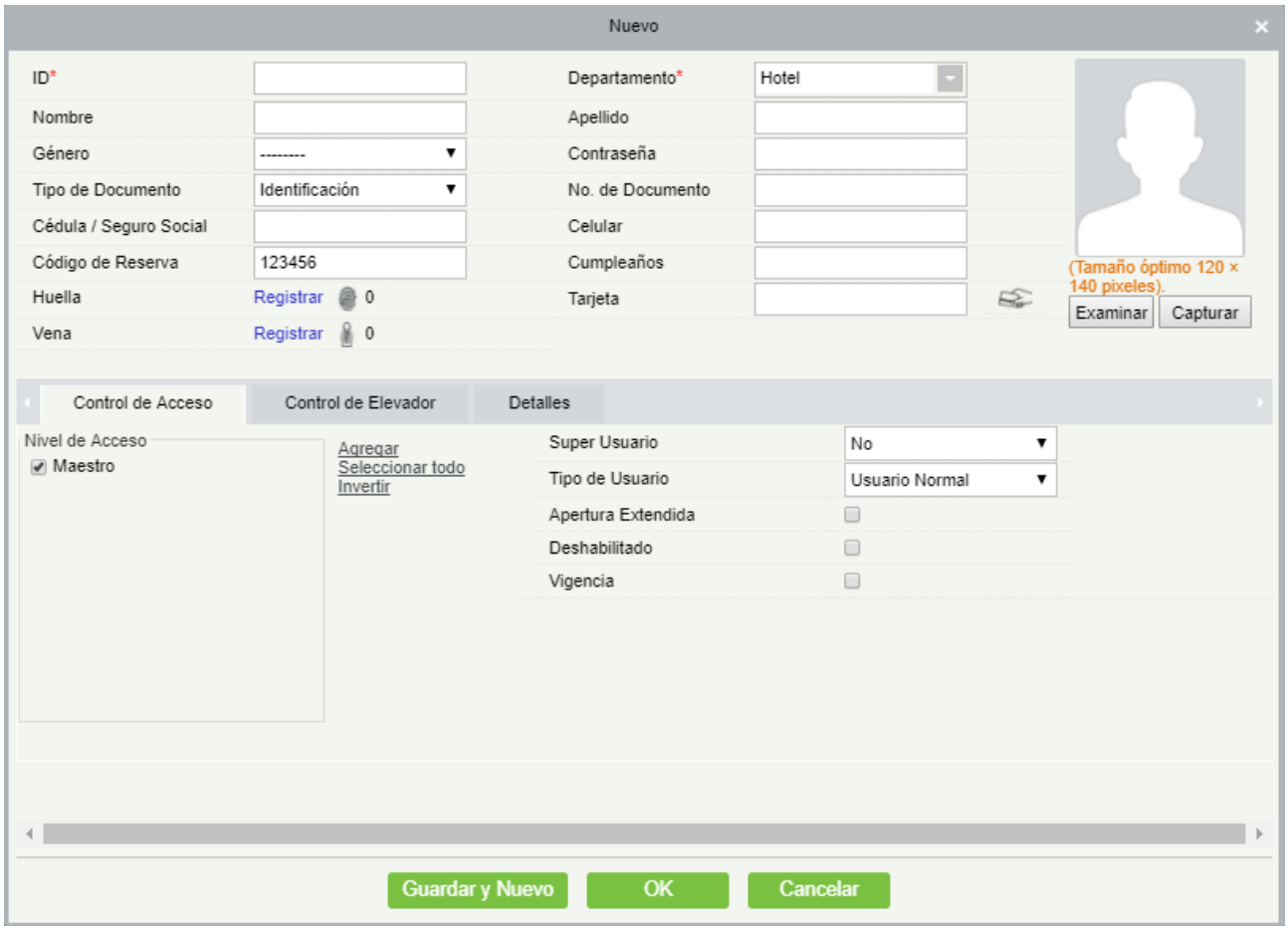
Alarma Puerta Mantenida Abierta: Después de marcar la casilla, puede especificar el número de alarmas para emitir o mantener alarma si la puerta se mantiene abierta.



Después de la configuración, presente una tarjeta en blanco en el codificador y de clic en **Escribir Tarjeta**.

- **Agregar personal de hotel**

Seleccione **Personal** > **Usuarios** > **Agregar**. Se mostrará la siguiente interfaz:



Introduzca la información del personal, seleccione un departamento de hotel y de clic en **OK**. Puede seleccionar los usuarios agregados en el módulo de emisión de tarjetas.

2. Tarjeta de hora

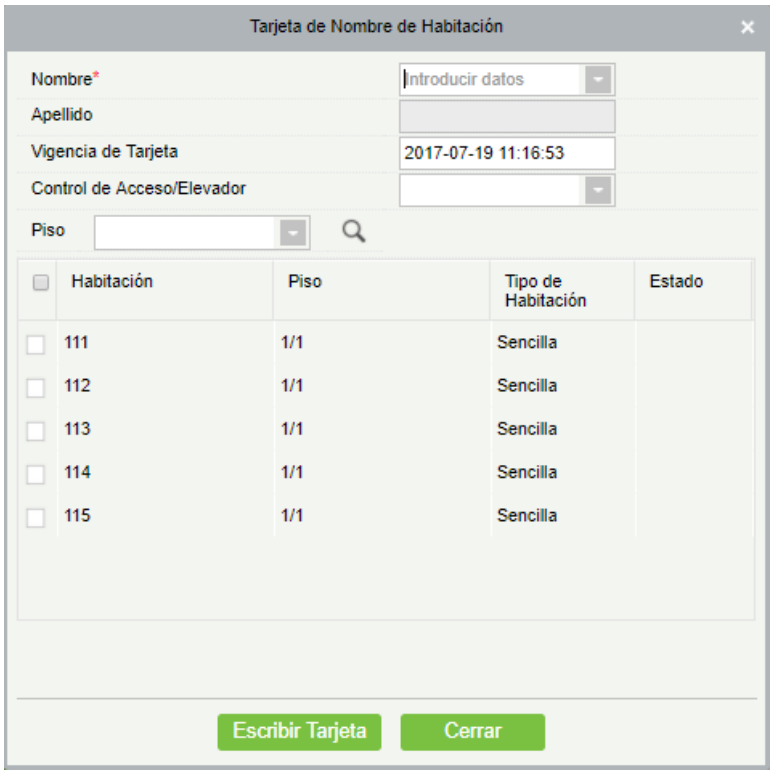
Una tarjeta de hora puede ser usada para desbloquear las habitaciones durante el tiempo de validez. Después de la configuración, sincronice la fecha y hora de las cerraduras de las habitaciones con la hora del sistema. De lo contrario, la cerradura emitirá una alarma de tarjeta expirada cuando la presente en la cerradura.

Control de Acceso/Elevador: De clic en la lista para seleccionar el nivel de acceso/elevador. Después de especificar el parámetro, la tarjeta no solo podrá desbloquear la habitación, sino también tener acceso a los dispositivos correspondientes al nivel de acceso o elevador.

Después de la configuración, presente una tarjeta en blanco en el codificador y de clic en **Escribir Tarjeta**.

3. Tarjeta de Nombre de Habitación

Una tarjeta de nombre de habitación es usada para desbloquear las cerraduras de las habitaciones con nombres específicos. Puede seleccionar múltiples habitaciones para emitir tarjetas de nombre de habitación en lotes.



Control de Acceso/Elevador: De clic en la lista para seleccionar el nivel de acceso/elevador. Después de especificar el parámetro, la tarjeta no solo podrá desbloquear la habitación, sino también tener acceso a los dispositivos correspondientes al nivel de acceso o elevador.

4. Tarjeta de área

Una tarjeta de área se usa para desbloquear habitaciones de un área específica. Si una habitación se encuentra en el área especificada, la tarjeta podrá abrir la habitación.

Control de Acceso/Elevador: De clic en la lista para seleccionar el nivel de acceso/elevador. Después de especificar el parámetro, la tarjeta no solo podrá desbloquear la habitación, sino también tener acceso a los dispositivos correspondientes al nivel de acceso o elevador.

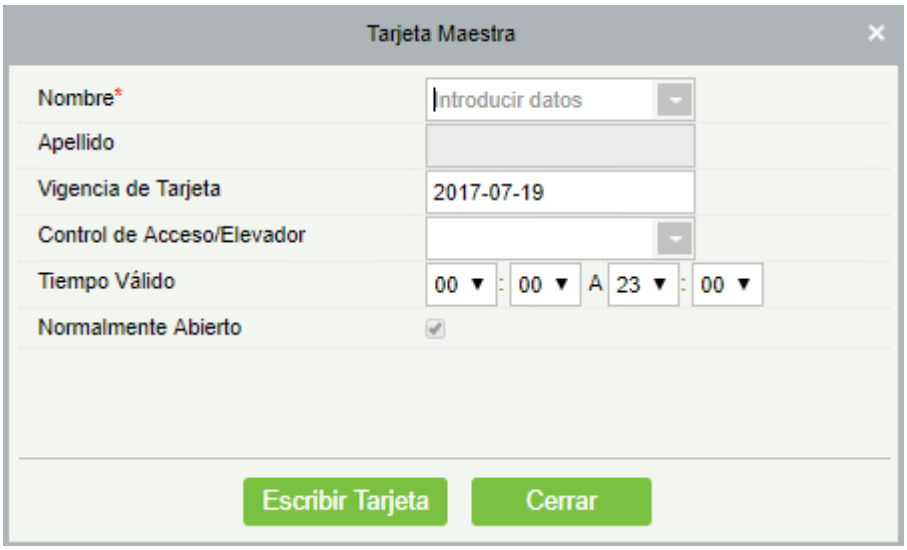
Nota: Un máximo de 6 áreas pueden ser seleccionadas para una tarjeta de área.

6.3.2 Tarjetas para Empleados

Puede crear varias tarjetas de acceso/elevador, tales como maestra y emergencia para que el personal gestione los servicios del hotel.

1. Tarjeta Maestra

Una tarjeta maestra se usa para abrir todas las habitaciones del hotel durante el tiempo de validez. Por defecto, abrirá las cerraduras en modo normalmente abierto.



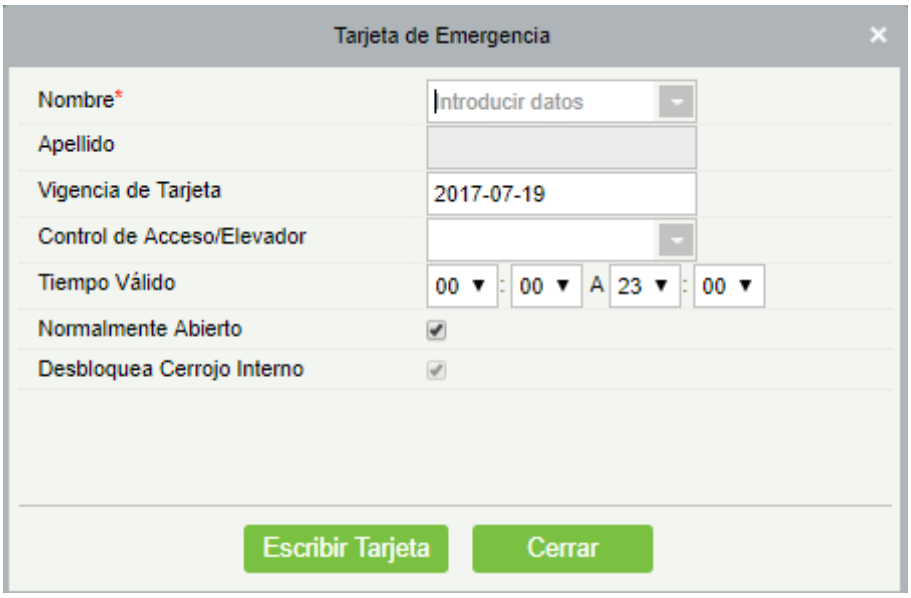
Control de Acceso/Elevador: De clic en la lista para seleccionar el nivel de acceso/elevador. Después de especificar el parámetro, la tarjeta no solo podrá desbloquear la habitación, sino también tener acceso a los dispositivos correspondientes al nivel de acceso o elevador.
Si selecciona el modo normalmente abierto, las habitaciones permanecerán desbloqueadas.

Establezca la **Vigencia de la Tarjeta** y **Tiempo Válido**. La tarjeta solo podrá abrir las habitaciones dentro del tiempo especificado.

Después de la configuración, presente una tarjeta en blanco en el codificador y de clic en **Escribir Tarjeta**.

2. Tarjeta de Emergencia

Una tarjeta maestra puede ser usada para abrir todas las habitaciones del hotel dentro del tiempo de validez. Por defecto, la función **Deshabilitar Cerrojo Interno** es activado. Puede seleccionar si desea habilitar el modo normalmente abierto.

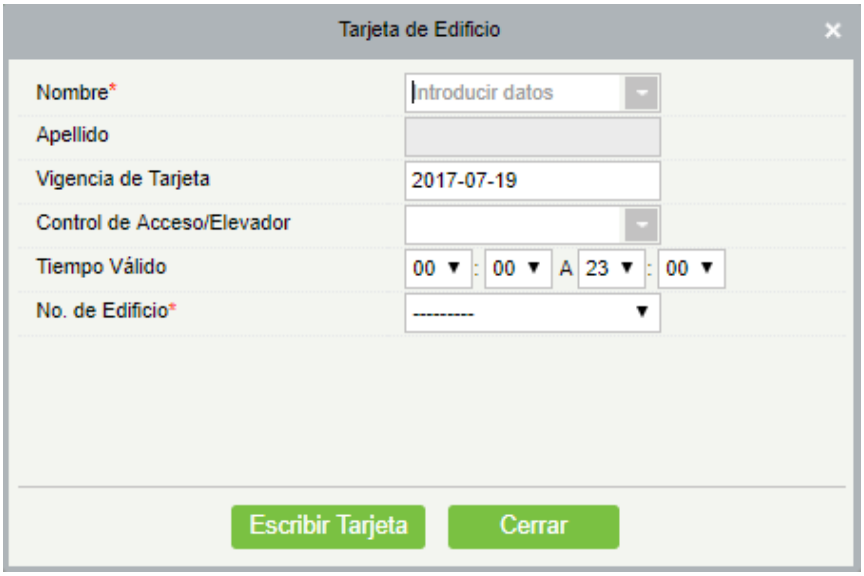


Control de Acceso/Elevador: De clic en la lista para seleccionar el nivel de acceso/elevador. Después de especificar el parámetro, la tarjeta no solo podrá desbloquear la habitación, sino también tener acceso a los dispositivos correspondientes al nivel de acceso o elevador.

Si selecciona el modo normalmente abierto, las habitaciones permanecerán desbloqueadas.
Para deshabilitar el **Modo Normalmente Abierto**, es necesario usar una tarjeta que pueda abrir todas las habitaciones, tal como una tarjeta de piso o edificio.
Si selecciona Desbloquea Cerrojo Interno, significa que la tarjeta puede abrir las habitaciones, aunque estén bloqueadas desde adentro con el cerrojo.

3. Tarjeta de Edificio

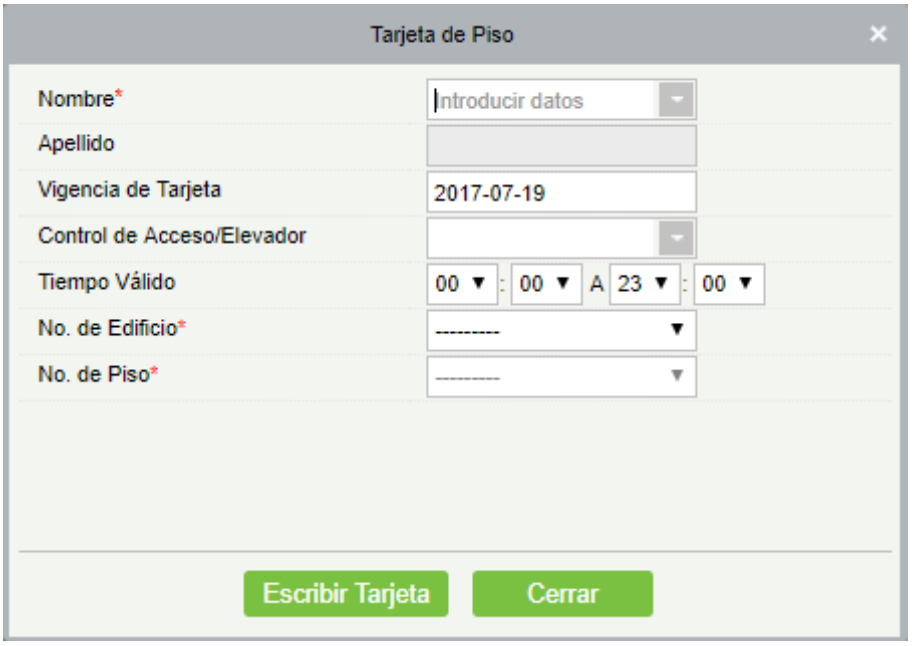
Una tarjeta de edificio se usa para abrir las habitaciones de un edificio específico durante el tiempo de validez.



Control de Acceso/Elevador: De clic en la lista para seleccionar el nivel de acceso/elevador. Después de especificar el parámetro, la tarjeta no solo podrá desbloquear la habitación, sino también tener acceso a los dispositivos correspondientes al nivel de acceso o elevador.

4. Tarjeta de Piso

Una tarjeta de piso se usa para abrir las habitaciones de un piso específico durante el tiempo de validez.



Control de Acceso/Elevador: De clic en la lista para seleccionar el nivel de acceso/elevador. Después de especificar el parámetro, la tarjeta no solo podrá desbloquear la habitación, sino también tener acceso a los dispositivos correspondientes al nivel de acceso o elevador.

5. Tarjeta de Área

La tarjeta de área se usa para abrir las habitaciones de un área específica durante el tiempo de validez.

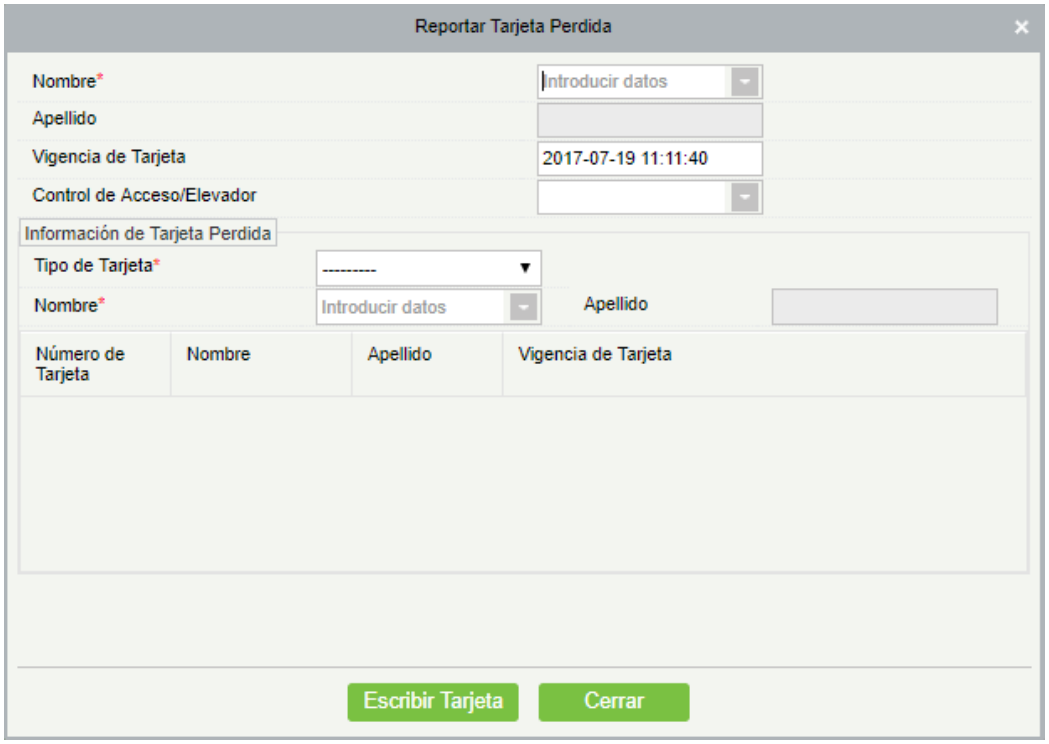
Control de Acceso/Elevador: De clic en la lista para seleccionar el nivel de acceso/elevador. Después de especificar el parámetro, la tarjeta no solo podrá desbloquear la habitación, sino también tener acceso a los dispositivos correspondientes al nivel de acceso o elevador.

6.3.3 Tarjetas de Mantenimiento

Una tarjeta de mantenimiento se usa para gestionar las cerraduras del hotel.

1. Reportar tarjeta perdida

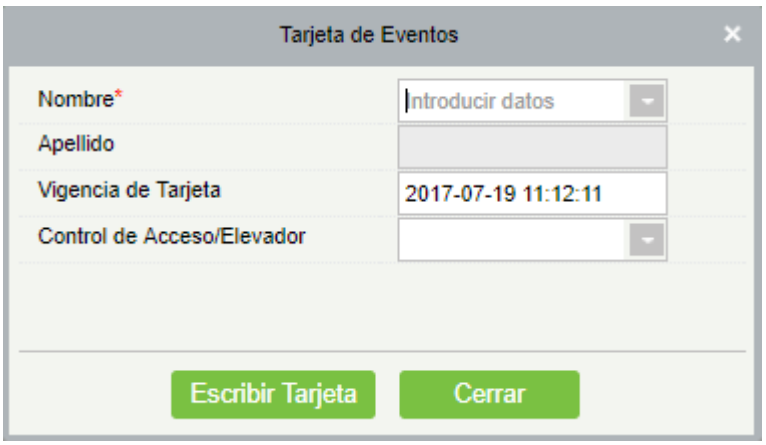
Una tarjeta reportada como perdida (o dañada) quedará invalidada y obsoleta en el tiempo de validez.



Control de Acceso/Elevador: De clic en la lista para seleccionar el nivel de acceso/elevador. Después de especificar el parámetro, la tarjeta no solo podrá desbloquear la habitación, sino también tener acceso a los dispositivos correspondientes al nivel de acceso o elevador.

2. Tarjeta de Eventos

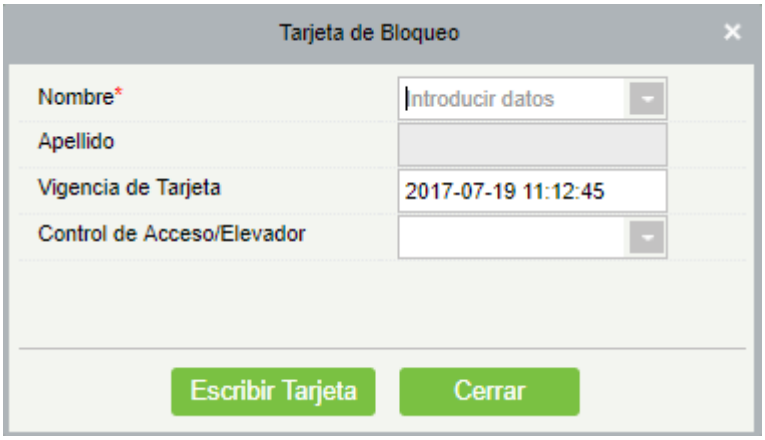
Una tarjeta de eventos se usa para obtener los registros de eventos de una cerradura durante el tiempo de validez especificado. Solo las tarjetas S70 pueden ser usadas como tarjeta de eventos.



Control de Acceso/Elevador: De clic en la lista para seleccionar el nivel de acceso/elevador. Después de especificar el parámetro, la tarjeta no solo podrá desbloquear la habitación, sino también tener acceso a los dispositivos correspondientes al nivel de acceso o elevador.

3. Tarjeta de bloqueo

Una tarjeta de bloqueo es una tarjeta especial usada para bloquear y proteger la escena de una habitación en caso de una emergencia. Una vez que se aplica el bloqueo, la habitación ya no podrá ser abierta por todas las tarjetas que originalmente podían desbloquear la cerradura antes de re-autorizar las tarjetas.



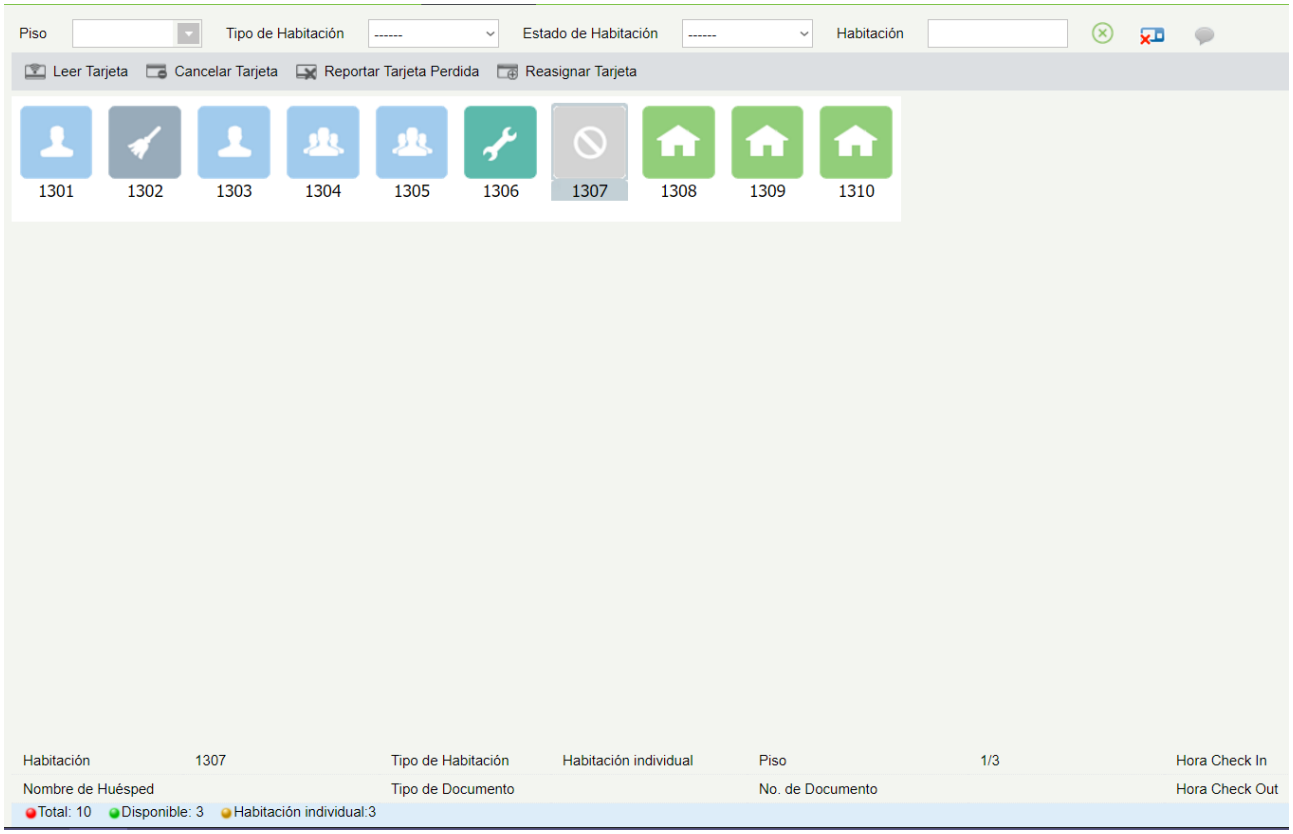
Control de Acceso/Elevador: De clic en la lista para seleccionar el nivel de acceso/elevador. Después de especificar el parámetro, la tarjeta no solo podrá desbloquear la habitación, sino también tener acceso a los dispositivos correspondientes al nivel de acceso o elevador.

6.4 Gestión de Hotel

6.4.1 Recepción

La función permite a los usuarios gestionar los servicios de las habitaciones y verificar la ocupación del hotel, tal como el total de habitaciones, habitaciones disponibles y tipos de habitación.

Vea la siguiente imagen:



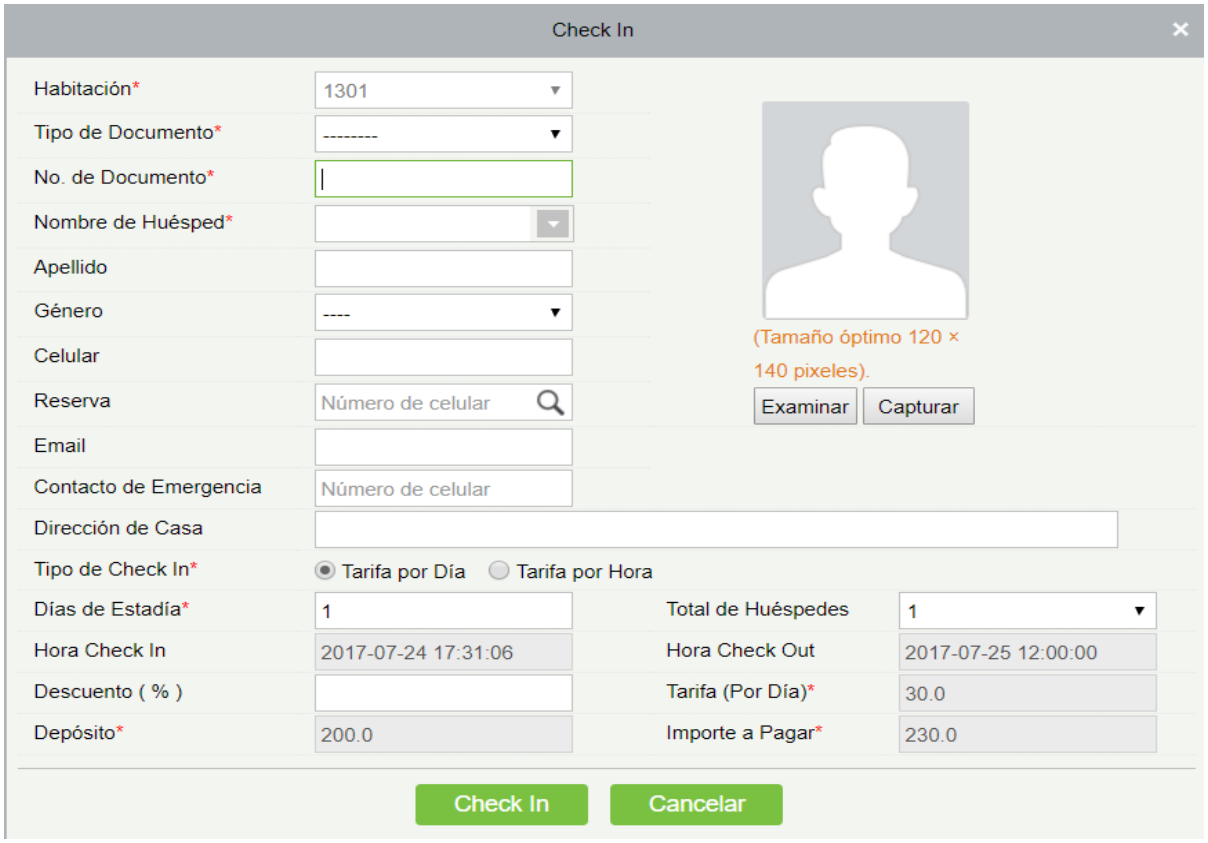
Descripción de los íconos

	Disponible		**Extendida**		**Check in Individual**		**Check in Grupal**
	No Disponible		**En Mantenimiento**		**Sucia**		

1. Gestión Individual

- **Check in individual**

1) De doble clic o clic derecho en una habitación disponible y seleccione **Individual** > **Check In**. Se mostrará la siguiente interfaz:



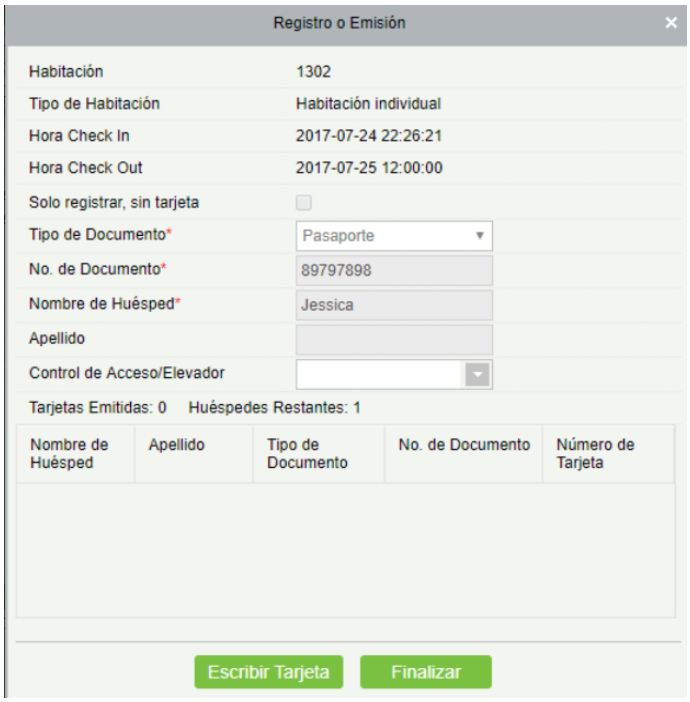
Reserva: Introduzca el número de celular usado para hacer la reservación.

Días de Estadía: Introduzca el número de días que el huésped desea hospedarse.

Descuento: Descuento en el costo de la habitación. Por ejemplo, si tiene el 10% de descuento, el costo de la habitación será 1*120*0.9 + 150=258.

Importe a pagar: Cantidad que será pagada en el check in, incluyendo la habitación y el depósito.

2) Después de llenar la información del **Check In Individual**, se mostrará la página de **Registro:**

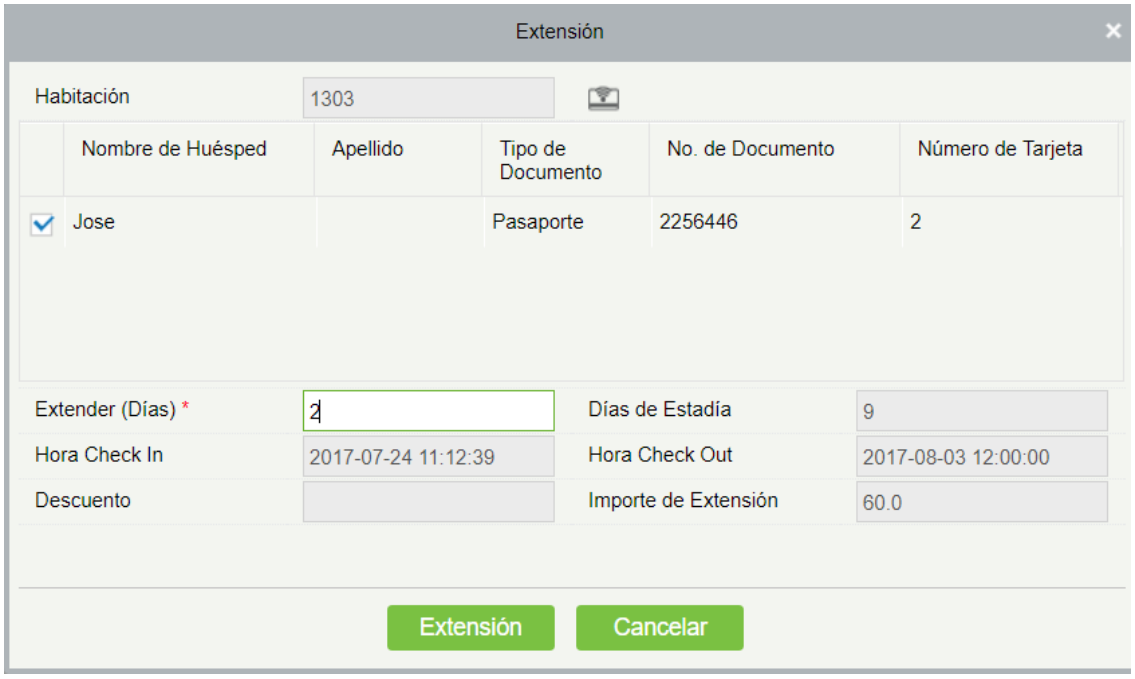


Control de Acceso/Elevador: De clic en la lista para seleccionar el nivel de acceso/elevador. Después de especificar el parámetro, la tarjeta no solo podrá desbloquear la habitación, sino también tener acceso a los dispositivos correspondientes al nivel de acceso o elevador.

Nota: Debe emitir a menos una tarjeta para cada habitación. La tarjeta debe ser emitida para el huésped registrado. Al emitir la tarjeta del primer huésped, la opción **Solo registrar, sin tarjeta** no estará disponible. Después de emitir la tarjeta del primer huésped puede seleccionar **Solo registrar, sin tarjeta** como sea requerido. La opción indica que el huésped solo será registrado, pero no tendrá una tarjeta de huésped.

- **Extensión individual**

1) De clic derecho en una habitación con check in y seleccione **Individual** > **Extensión**. Se mostrará la siguiente interfaz:



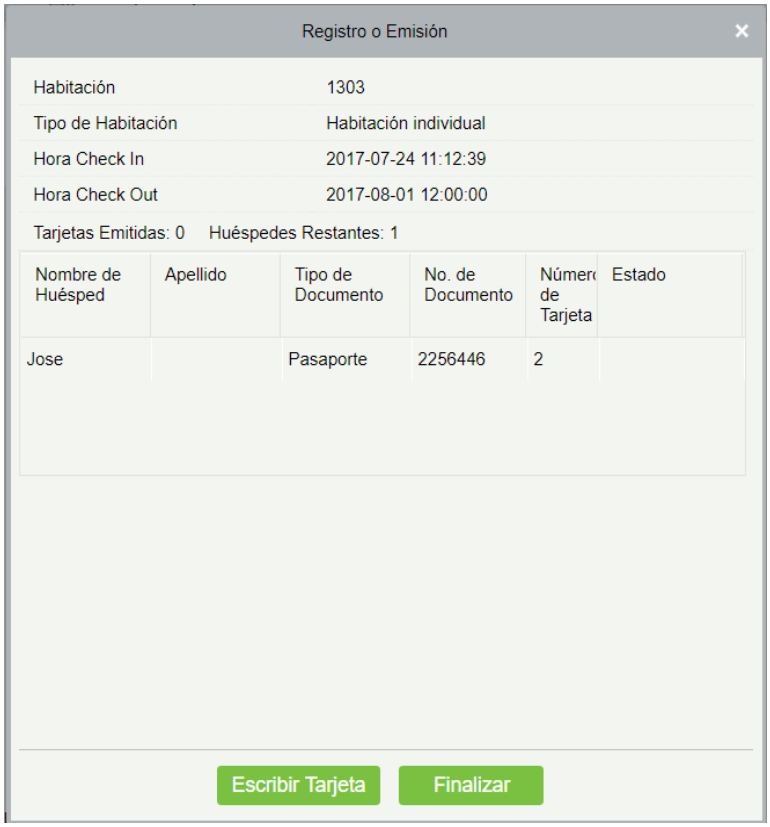
Notas: a. Si el número de días de extensión causa conflicto con la reservación, la extensión no será permitida.

b. Seleccione el huésped que requiere la extensión para procesar el servicio.

c. El descuento no puede ser modificado para la extensión.

d. **Importe de Extensión** muestra la cantidad a pagar por la extensión.

2) Después de llenar la información del **Extensión Individual**, se mostrará la página de **Registro:**

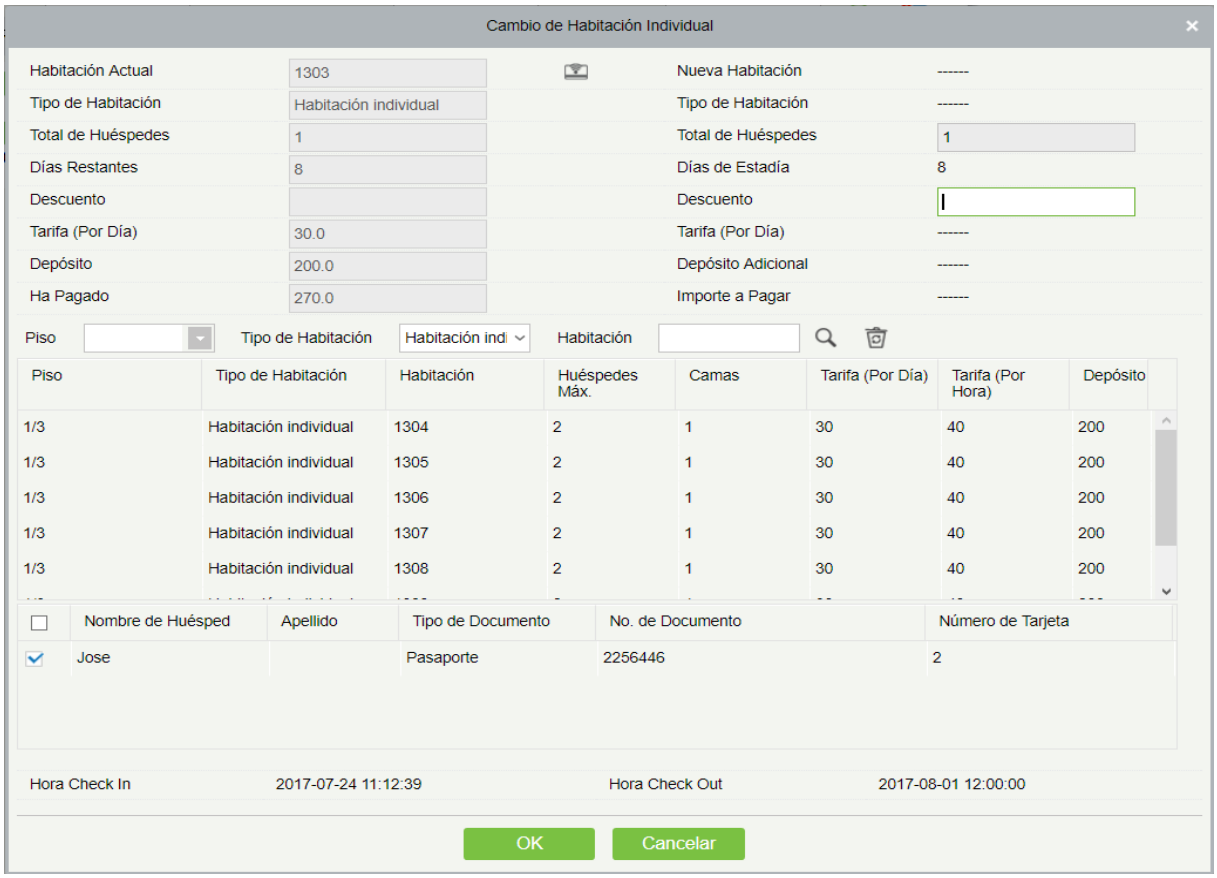


Notas: a. Al volver a emitir la tarjeta para la extensión, la tarjeta debe ser la misma que se usó para realizar el check in, de lo contrario la emisión para la extensión fallará.

b. Puede dar clic en Escribir Tarjeta para escribir automáticamente todas las tarjetas para la extensión de la estadía en un intervalo de 3 segundos.

- **Cambio de Habitación**

1) De clic derecho en una habitación con check in y seleccione **Individual** > **Cambio de Habitación**. Se mostrará la siguiente interfaz:



Total de Huéspedes: Número de huéspedes que requieren cambio de habitación.

Notas: a. Puede verificar la información de la habitación leyendo la tarjeta.

b. El máximo de huéspedes de las habitaciones seleccionadas no debe ser menor que el máximo número de huéspedes de la habitación original.

c. Los huéspedes sin tarjetas no pueden ser cambiados de habitación solos.

d. Si la habitación original se deja con un huésped sin tarjeta durante el cambio de habitación, el sistema pregunta si desea cambiar la habitación para ese huésped también. Si selecciona No, el cambio de habitación no se podrá realizar.

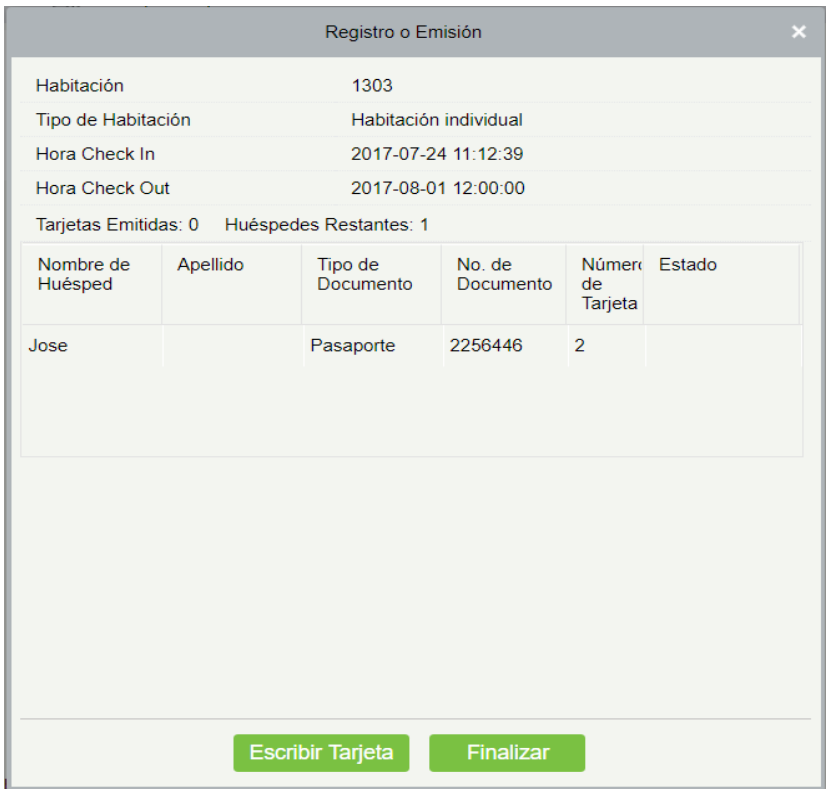
e. Si la nueva habitación está reservada, se mostrará la información del conflicto. Puede seleccionar si desea proceder con el servicio.

f. El descuento puede ser establecido para la nueva habitación.

g. Si el depósito requerido la nueva habitación es mayor que la habitación original, el huésped tendrá que hacer el depósito. Si el depósito requerido para la nueva habitación es menor que la habitación original, el total del depósito se devolverá al momento del check out.

h. Si la tarifa de la nueva habitación es mayor que la habitación original, el huésped tendrá que pagar la diferencia. Si la tarifa es menor que la habitación original, la cantidad adicional será devuelta al momento del check out.

2) Después de llenar la información del cambio de habitación, se mostrará la página de **Registro**.

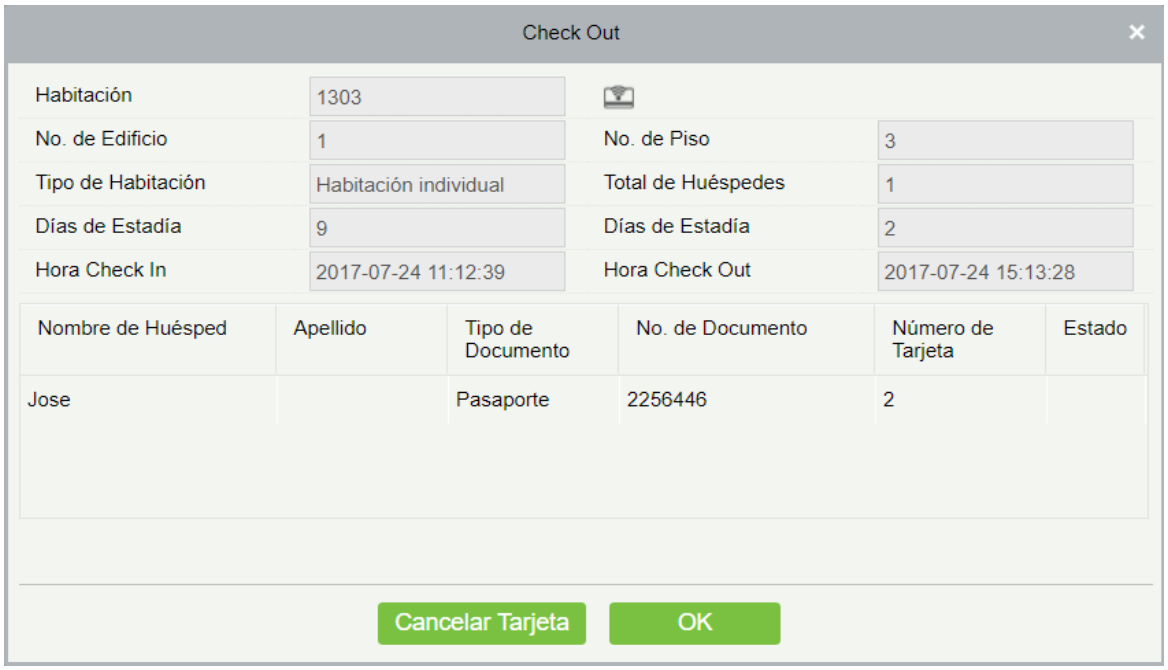


Control de Acceso/Elevador: De clic en la lista para seleccionar el nivel de acceso/elevador. Después de especificar el parámetro, la tarjeta no solo podrá desbloquear la habitación, sino también tener acceso a los dispositivos correspondientes al nivel de acceso o elevador.

Nota: Puede dar clic en **Escribir Tarjeta** para automáticamente escribir las tarjetas para todos los cambios de habitación en circulación hasta que todas las tarjetas hayan sido escritas.

- **Check out Individual**

De clic en una habitación con registro de check in y seleccione **Individual** > **Check Out**. Se mostrará la siguiente interfaz:

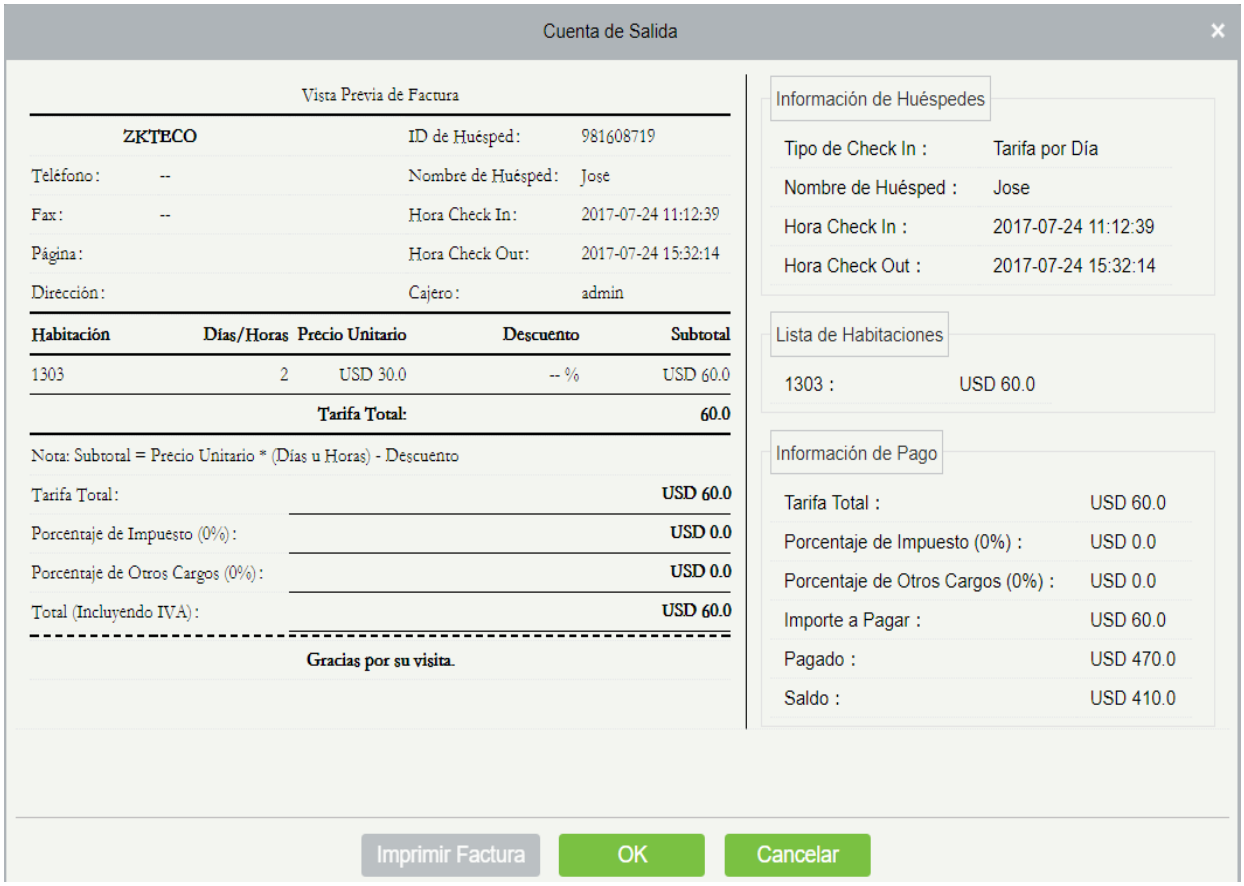


Cancelar Tarjeta: Verifique si la tarjeta que será cancelada coincide con la habitación actual del huésped. Si coincide, se cancelará la tarjeta, de lo contrario se mostrará la notificación.

Nota: Cuando las tarjetas son canceladas una por una, el número de huéspedes registrados será reducido.

Cuando no hay titular de la tarjeta, el botón de **Cancelar Tarjeta** estará deshabilitado.

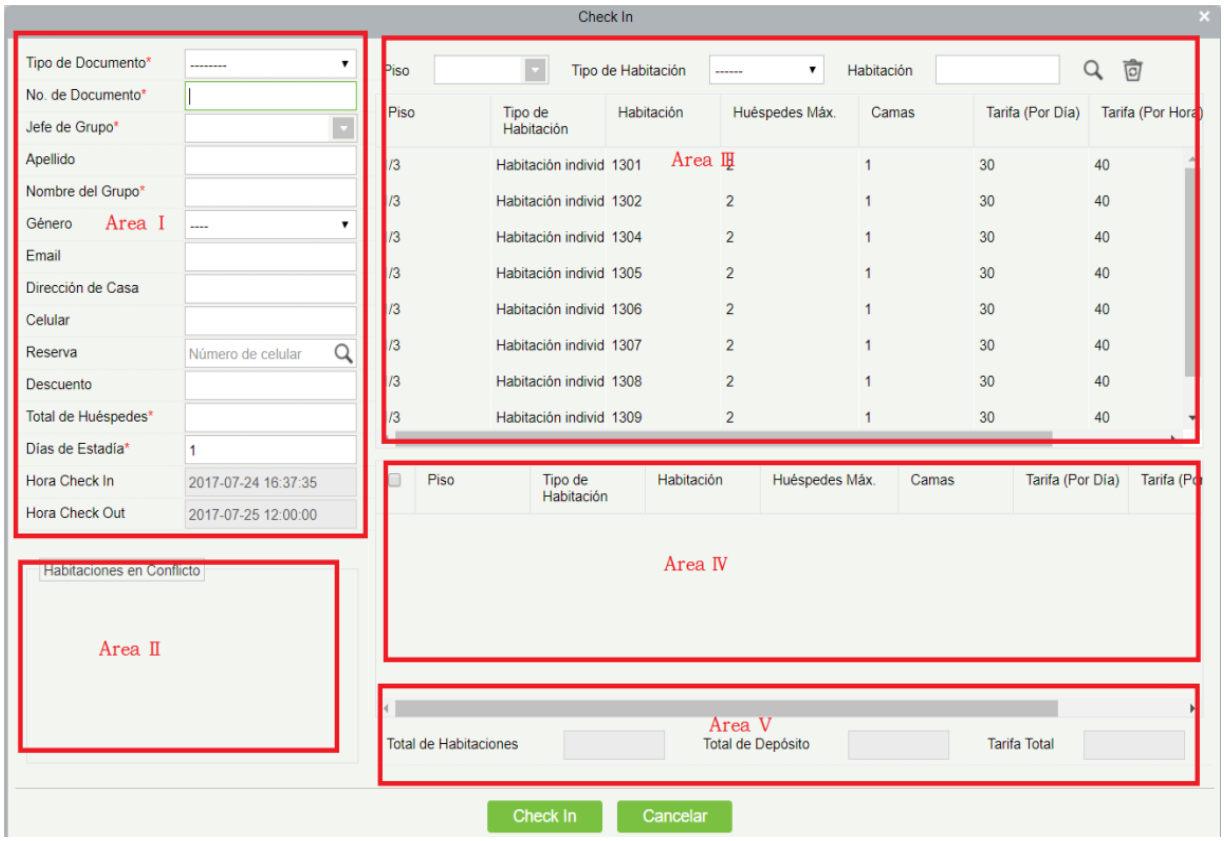
De clic en **OK**, y la factura se mostrará como se ve en la siguiente imagen:



2. Gestión de Grupos

- **Check in de Grupo**

1) De clic derecho en una habitación disponible y seleccione **Grupo** > **Check In**. Se mostrará la siguiente interfaz:



Reserva: Introduzca el número de celular usado para hacer la reservación y de clic en el ícono para buscar.

Descripción de la interfaz:

Área I: Para introducir la información del check in del grupo.

Área II: Muestra la información de la reserve en la habitación actual. Si la habitación ha sido reservada, la información de la reserva se muestra en la lista del Área II. Si la reserva está en conflicto con el tiempo de check in, la operación no podrá ser procesada.

Área III: Muestra la lista de las habitaciones disponibles (puede dar doble clic en una habitación para agregarla al Área IV).

Área IV: Muestra la reserva y las habitaciones seleccionadas en el Área III.

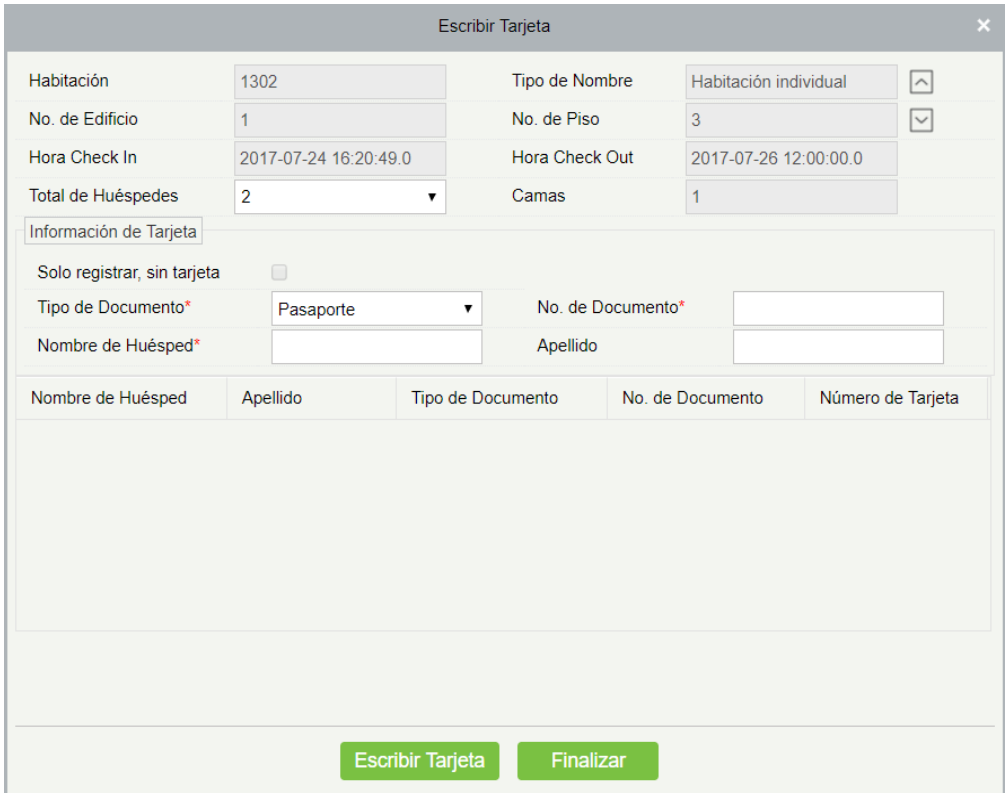
Área V: Muestra el importe del depósito y el costo del check in del grupo.

Notas:

a. Si los días de estadía traslapan con el periodo de la reserva, el botón de **Check In** se mostrará inhabilitado y el check in no será permitido.

b. Si el número de huéspedes de check in es mayor que el máximo número de todas las habitaciones en total, el botón de **Check In** se mostrará inhabilitado y el check in no será permitido.

2) De clic en **Check In** y la página de **Escribir Tarjeta** para check in de grupo aparecerá como se muestra en la siguiente imagen:



Total de Huéspedes: Número de huéspedes que registrarán check in en la habitación. El número no debe exceder el número máximo permitido en la habitación.

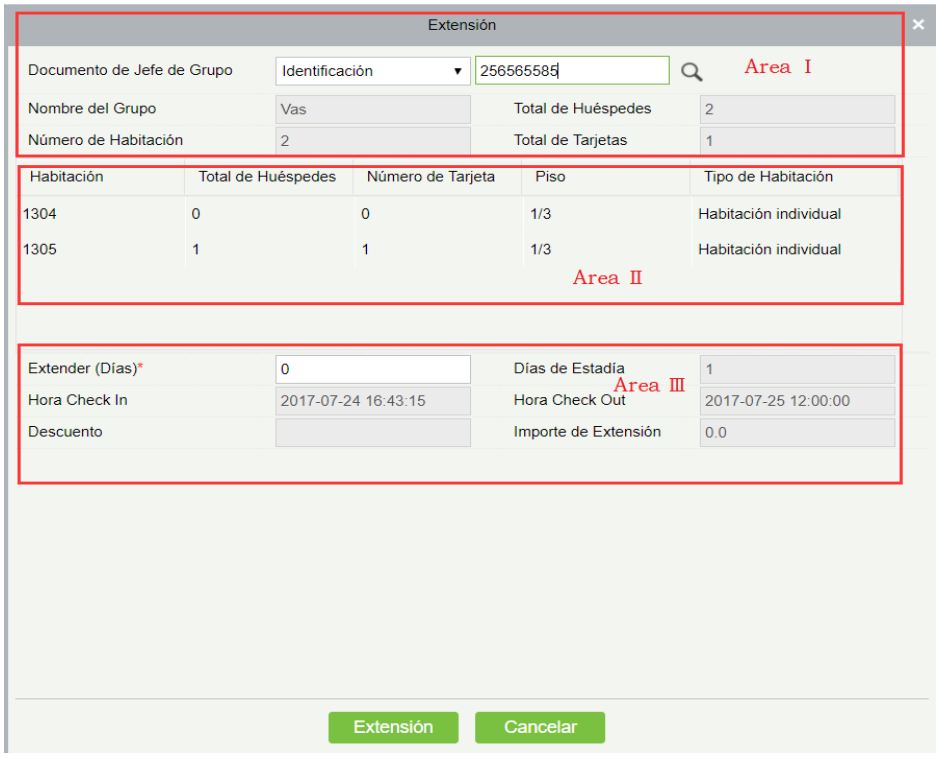
Solo Registrar, sin tarjeta: Si se selecciona esta opción, solo se registrará la información de los huéspedes, pero no se emitirán tarjetas.

Control de Acceso/Elevador: Si existen dispositivos de acceso o elevador y la opción de **Control de Acceso/Elevador** se encuentra activada en la **Información de Hotel**, la opción estará disponible y puede asignar los niveles de acceso o elevador a una tarjeta. Para los detalles sobre la información de hotel consulte Información de Hotel.

Nota: Puede dar clic en o para ir a la habitación siguiente o previa.

- **Extensión de Grupo**

1) De clic derecho en una habitación con registro de check in y seleccione **Grupo** > **Extensión de Grupo**. Se mostrará la siguiente interfaz:



Descripción de la página:

Área I: La información acerca de las habitaciones con check in por el grupo y la información de los huéspedes.

Área II: Lista de las habitaciones reservadas.

Área III: La información de Check in del grupo.

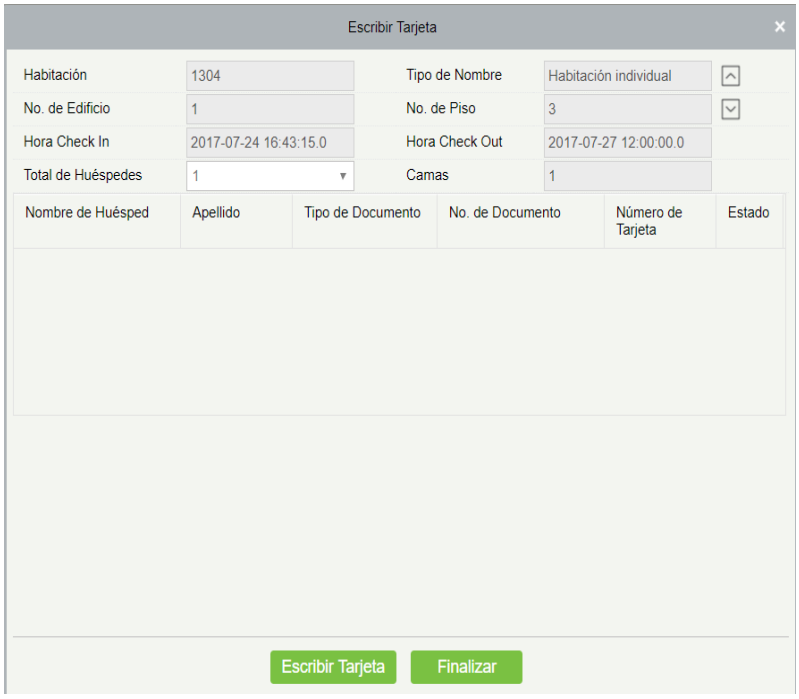
Notas:

a. El tiempo de extensión no puede traslapar con el periodo de reservación, de lo contrario, el botón de **Extensión** se mostrará inhabilitado.

b. Por defecto, los días de estadía serán extendidos para todo el grupo.

c. El periodo de extensión es mínimo un día. Para una condición especial, el número de extensión de días puede ser **0**.

2) De clic en **Extensión** y la página para **Escribir Tarjeta** para la extensión de grupo se mostrará como en la siguiente imagen:



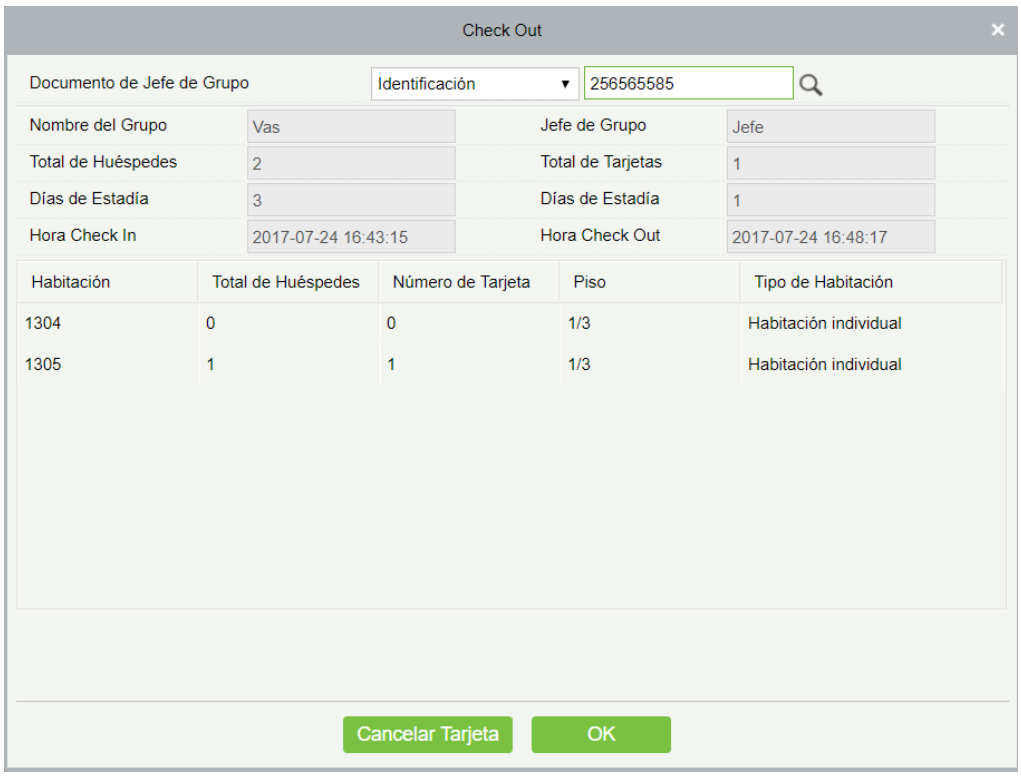
Notas:

Re-escriba todas las tarjetas emitidas
para los miembros del grupo para la extensión.
Cuando de clic a **Escribir Tarjeta**, todas las tarjetas son escritas para las habitaciones una por una en un ciclo con intervalo de 3 segundos.
La tarjeta emitida durante el check in del huésped es requerida para re-escribir. En caso de que la tarjeta haya sido dañada o perdida, es necesario reportar la tarjeta como perdida y escribir una tarjeta nueva antes de volver a emitirla.

Puede dar clic en o para ir a la habitación siguiente o previa.

- **Check Out de Grupo**

De clic derecho en una habitación con registro de check in y seleccione **Grupo** > **Check Out**. Se mostrará la siguiente interfaz:



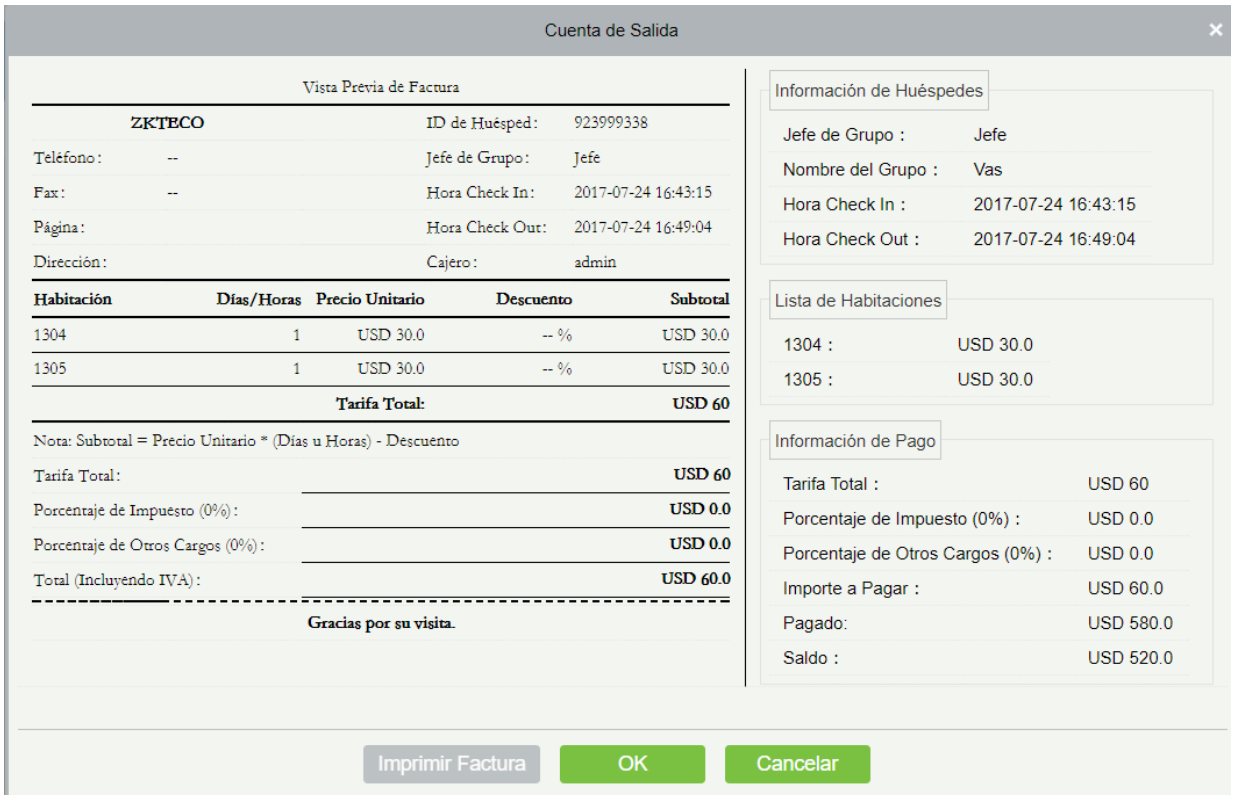
Notas:

a) Puede seleccionar hacer el check out solo en algunas de las habitaciones del grupo. Por defecto, se hace el check out en todas las habitaciones de un grupo.

b) Las tarjetas de las habitaciones seleccionadas son canceladas.

c) Puede hacer check out de una habitación antes de cancelar las tarjetas (y cancelar las tarjetas cuando hayan sido recolectadas).

De clic en **Check Out,** se mostrará la página de factura como se muestra a continuación:



3. Leer Tarjeta

Puede ver la información de emisión de todas las tarjetas del módulo de hotel, excepto las tarjetas de eventos. El contenido se muestra basado en tipo de tarjeta (por ejemplo, tarjeta de huésped y tarjeta de autorización). Cuando se lee una tarjeta de eventos solo se mostrará el tipo de tarjeta.

4. Cancelar Tarjeta

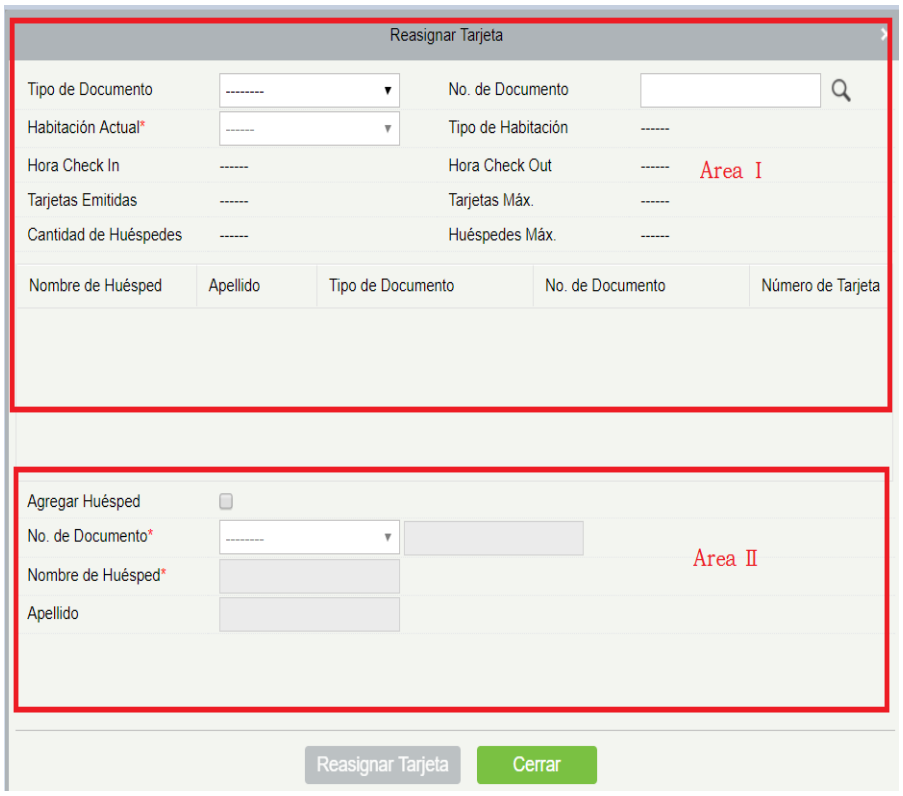
Puede borrar toda la información de la tarjeta (IC). Para una tarjeta de huésped, el Sistema verifica si la tarjeta es la última tarjeta de la habitación registrada por el huésped. Si lo es, la tarjeta no podrá ser cancelada (ya que el sistema no soporta check in sin tarjeta). Para otros tipos de tarjetas, no se realiza ninguna verificación.

5. Reportar Tarjeta Perdida

Puede establecer una tarjeta dañada o perdida en un estado de invalidez. Para los detalles, consulte Reporte de Tarjeta Perdida en la sección Tarjetas de Mantenimiento.

6. Reasignar Tarjeta

Puede reasignar una tarjeta para un huésped registrado, un huésped que reporta la tarjeta como perdida o una tarjeta adicional para una habitación con registro de check in. Si el número de huéspedes de una habitación ha alcanzado el máximo, no se permitirá asignar tarjetas adicionales.
Seleccione **Gestión de Hotel** > **Recepción** > **Reasignar Tarjeta**. Seleccione una habitación para reasignar la tarjeta o encuentre la habitación buscando el número de documento del huésped (y haciendo clic el) en la página de **Resignar Tarjeta**, como se muestra a continuación:

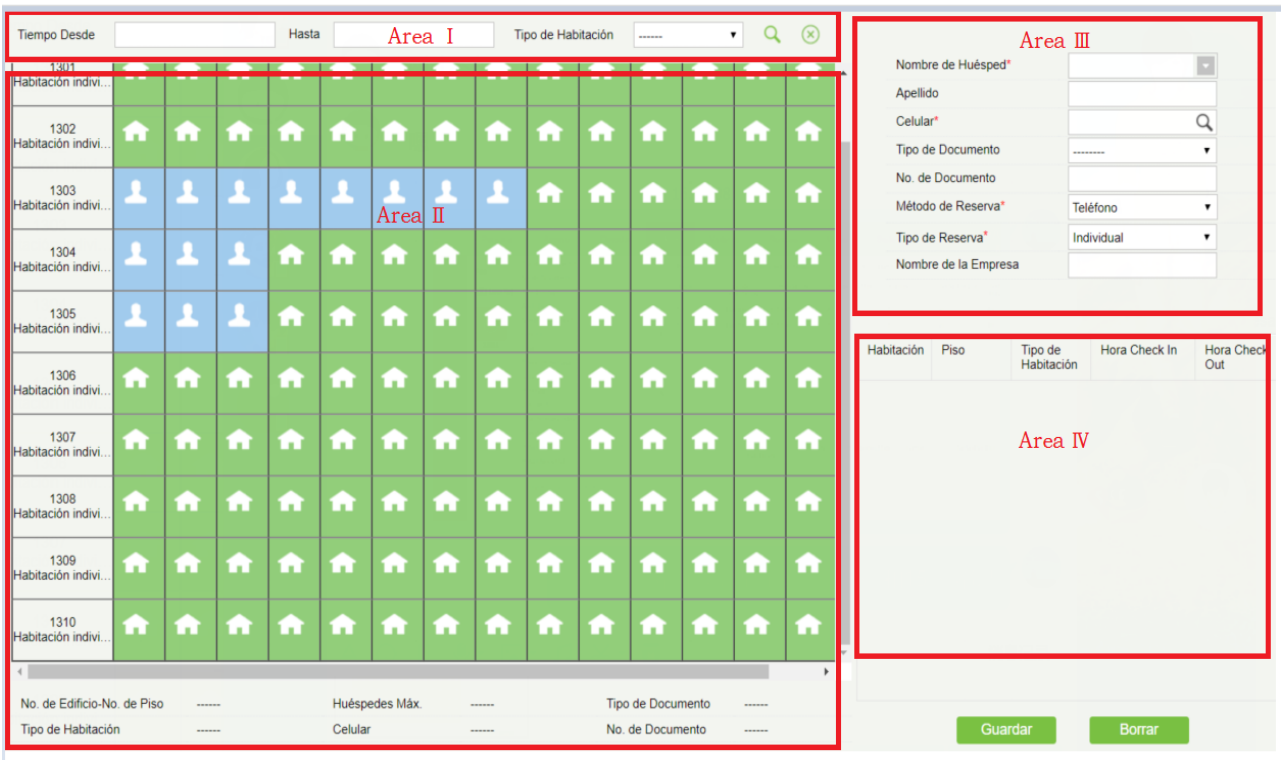


Descripción de la Página:

Área I: Muestra la información del huésped y la información de check in de la habitación.
Área II: Permite introducir la información del huésped de la tarjeta que será emitida.

6.2.4 Reservas

Puede verificar el estado de check in y reserva de todas las habitaciones dentro de un periodo específico y procesar la reserva de una habitación.
Seleccione **Gestión de Hotel** > **Reservas**. Se mostrará la siguiente interfaz:



Descripción de la página:

Área I (fechas disponibles): Por defecto, se muestra un periodo de 15 días (empezando por el día actual del sistema). Puede cambiar el periodo mostrado en el parámetro **Máximos Días de Reserva** en la página de **Información de Hotel**. Para los detalles, consulte la sección Información de Hotel.

El rango de hora de la reserva varía desde las 12:00 en la fecha inicial hasta las 12:00 en la fecha final. Puede cambiar el punto del tiempo en el parámetro **Hora Check Out** en la página de Información de Hotel. Para los detalles consulte la sección Información de Hotel.

Área II (habitaciones disponibles): Se muestran todas las habitaciones del hotel. Puede especificar la fecha inicial y final y el tipo de habitación para realizar la búsqueda de la habitación requerida.

Estado de habitación indica que puede reservarse para el periodo de tiempo.

Estado de habitación indica que está ocupada para el periodo de tiempo y no puede reservarse.

Estado de habitación indica que ha sido reservada para el periodo de tiempo.

Nota: Si una habitación está ocupada y se realizará el check out durante el periodo de reserva, la habitación se mostrará disponible pero no podrá ser reservada hasta el check out.

Área III: Información del huésped de la reserva.

Área IV: Información de las habitaciones seleccionadas para la reserva.

- **Proceso de Reserva**

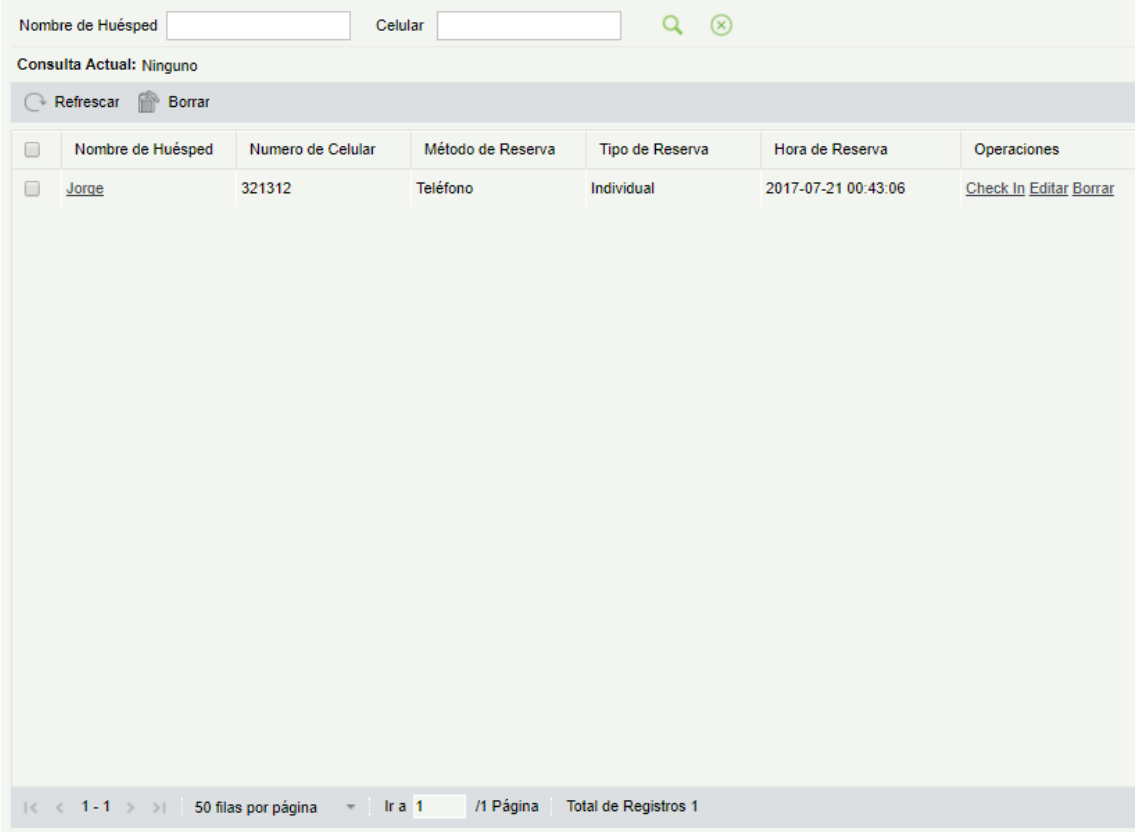
Paso 1: De clic en la habitación y fecha de la reserva. Las fechas seleccionadas para una habitación cambiarán a rojo . Puede dar clic en la habitación y en las fechas nuevamente para cancelar la selección. Puede seleccionar múltiples habitaciones en la misma fecha, múltiples fechas (solo continuas) de una habitación o múltiples fechas (solo continuas) de múltiples habitaciones.
Después de la selección, la información acerca de las habitaciones seleccionadas se muestra en la lista del Área IV, en la parte derecha de la página de **Reservas**.
Paso 2: Llene la información del huésped, incluyendo el nombre, celular, documento y método de reserva (teléfono o en sitio).
Paso 3: De clic en **Guardar**.

6.4.3 Gestión de Reservas

Puede buscar, editar, borrar y gestionar el check in de una reserva.

- **Buscar una reserva**

Seleccione **Gestión de Hotel** > **Gestión de Reservas**. Se muestra la siguiente interfaz.
Puede introducir el nombre del huésped o celular para buscar la reserva.



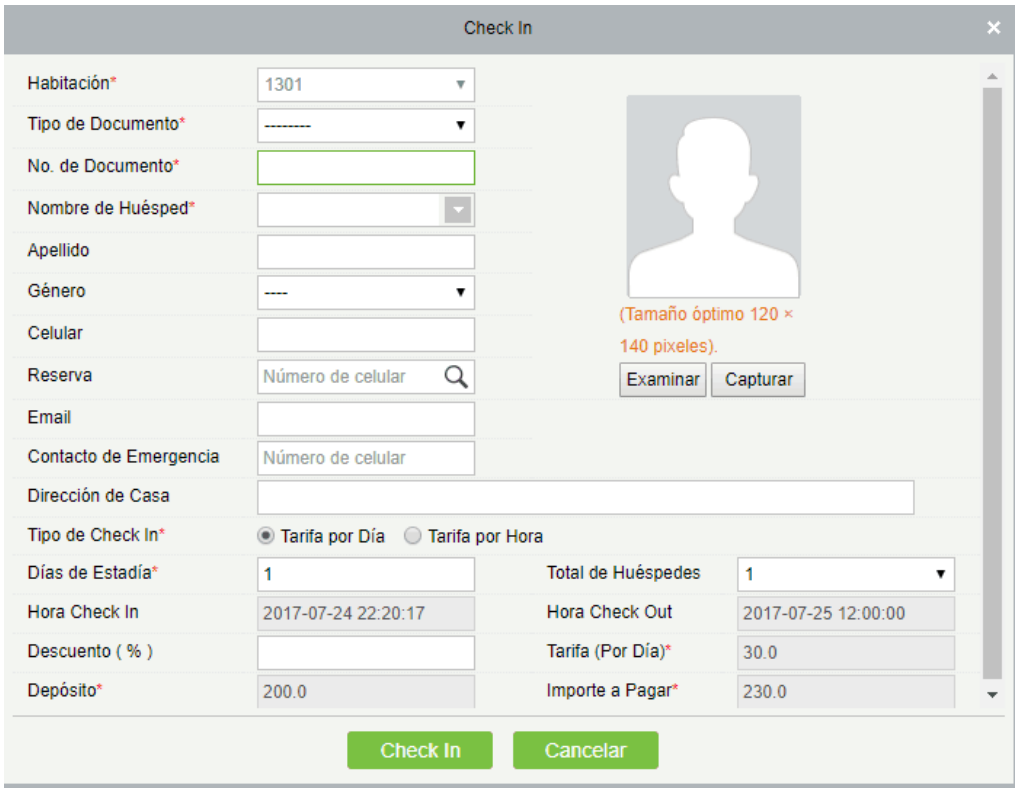
- **Editar / borrar una reserva**

Seleccione el nombre del huésped de la reserva y de clic en **Editar** debajo de **Operaciones**. En la página de Reservas mostrada, puede cambiar la habitación o modificar la información del huésped para la reserva.

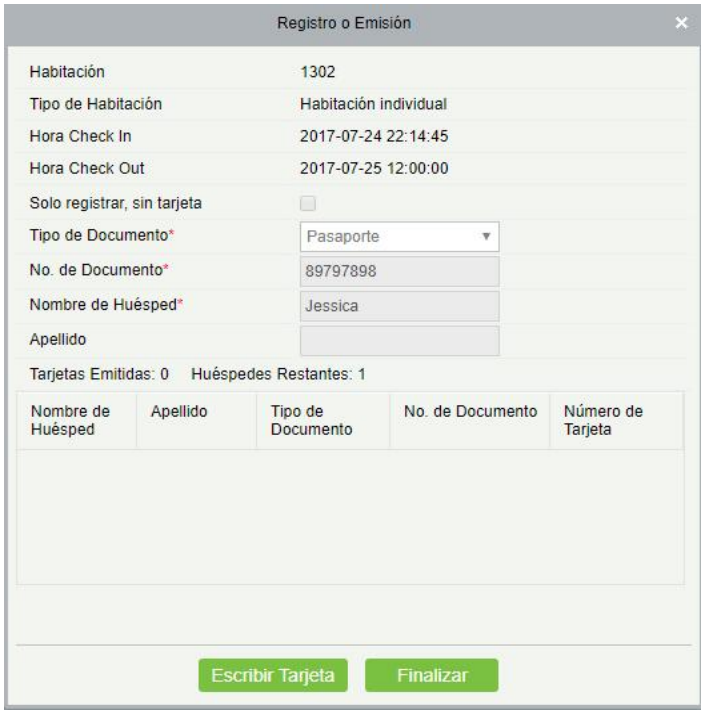
Seleccione el nombre del huésped de la reserva y de clic en **Borrar** debajo de **Operaciones** o el botón **Borrar** en la parte superior de la lista para eliminar la reserva.

- **Gestión de check in**

Seleccione el nombre del huésped de la reserva y de clic en **Check In** debajo de **Operaciones**. La página de **Check In Individual** se mostrará:



El sistema cargará la reserva de la habitación automáticamente. Modifique y complete la información del huésped y de clic en **Check In**. La página de **Registro o Emisión** se mostrará a continuación:



Coloque la tarjeta en el codificador y de clic en **Escribir Tarjeta** y **Finalizar** para completar el check in. **Notas:**

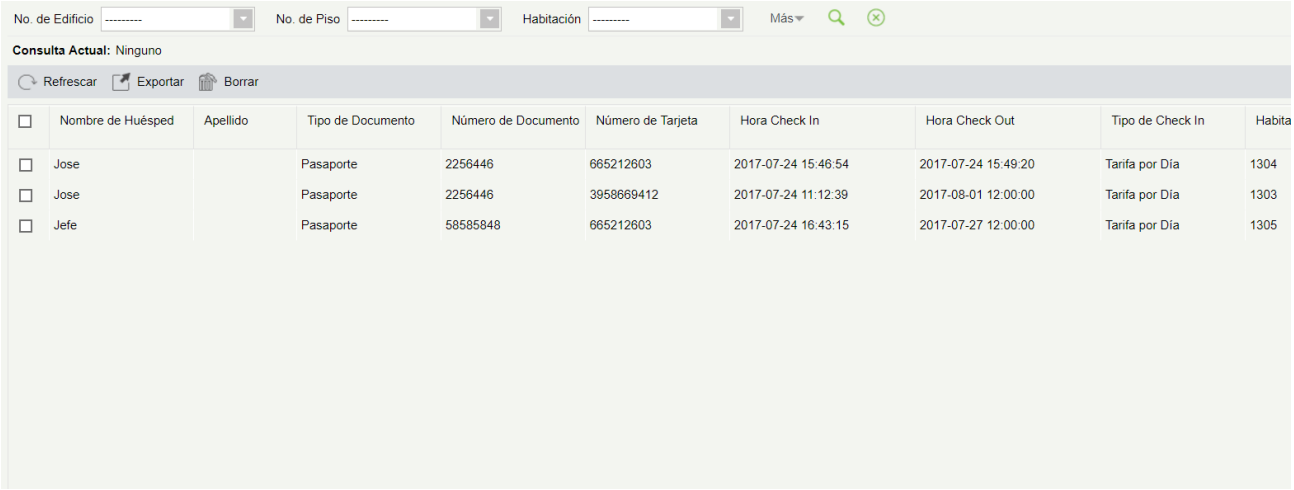
(1) No puede procesar el check in de una reserva expirada. El check in solo puede ser procesado en Sitio (Lobby). Para los detalles consulte Check In Individual en Recepción.

(2) El huésped puede realizar el check in antes del tiempo de la reserva.

6.5 Reportes

6.5.1 Reporte de Check In de Huésped

Para ver el reporte de los check in de los huéspedes introduzca las condiciones de la búsqueda y visualice los eventos. Puede exportar los registros en un archivo de Excel, PDF o CSV. Vea la siguiente imagen:



Nombre de Huésped	Apellido	Tipo de Documento	Número de Documento	Número de Tarjeta	Hora Check In	Hora Check Out	Tipo de Check In	Habita
Jose		Pasaporte	2256446	665212603	2017-07-24 15:46:54	2017-07-24 15:49:20	Tarifa por Día	1304
Jose		Pasaporte	2256446	3958669412	2017-07-24 11:12:39	2017-08-01 12:00:00	Tarifa por Día	1303
Jefe		Pasaporte	58585848	665212603	2017-07-24 16:43:15	2017-07-27 12:00:00	Tarifa por Día	1305

6.5.2 Reporte de Check In de Habitación

Para verificar la información de la ocupación de las habitaciones (incluyendo el nombre de la habitación, tipo, tipo de check, hora de check in y check out), introduzca las condiciones de la búsqueda y visualice los eventos. Puede exportar los registros en un archivo de Excel, PDF o CSV. Vea la siguiente imagen:

No. de Edificio --------- No. de Piso --------- Habitación --------- Más

Consulta Actual: Ninguno

Refrescar Exportar

Habitación	Tipo de Habitación	Tipo de Check In	Hora Check In	Hora Check Out
1303	Habitación individual	Tarifa por Día	2017-07-24 11:12:39	2017-08-01 12:00:00
1304	Habitación individual	Tarifa por Día	2017-07-24 15:46:54	2017-07-24 15:49:20
1305	Habitación individual	Tarifa por Día	2017-07-24 16:43:15	2017-07-27 12:00:00

6.5.3 Reporte de Pagos

Para verificar el registro de pagos de las habitaciones introduzca las condiciones de la búsqueda (incluyendo la hora, nombre de huésped y habitación) y visualice los eventos. Vea la siguiente imagen:

Tiempo Desde 2017-04-24 00:00:00 Hasta 2017-07-24 23:59:59 Nombre de Huésped Más

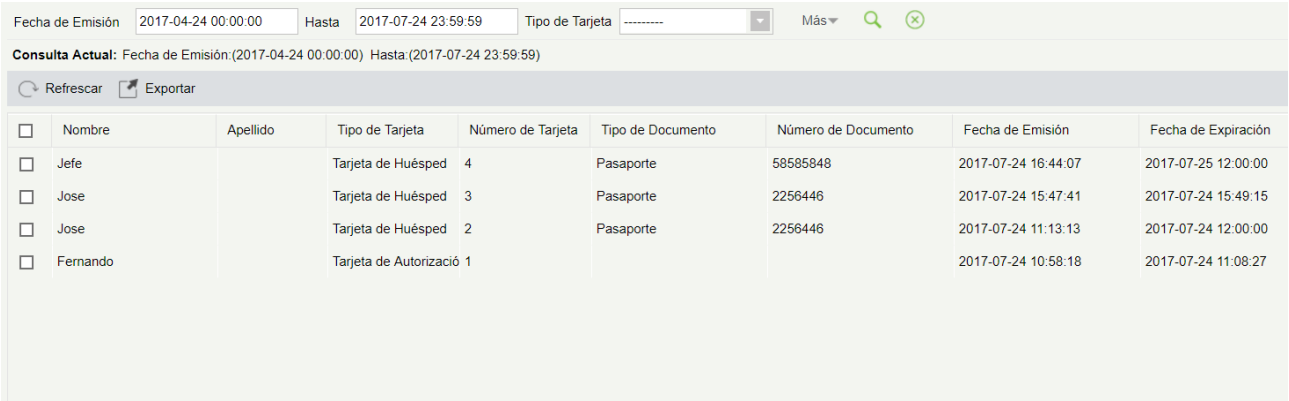
Consulta Actual: Tiempo Desde:(2017-04-24 00:00:00) Hasta:(2017-07-24 23:59:59)

Refrescar

Habitación	Tipos de Habitación	Nombre de Huésped	Apellido	Hora Check In	Hora Check Out	Tipo de Check In	Tiempo de Estadía	Tarifa de Habitación	Tarifa Extra	Porce Impue
1302	Habitación individua	Prueba		2017-07-24 11:09:10	2017-07-24 15:31:42	Tarifa por Día	1	30.0	90.0	0.0
1303	Habitación individua	Jose		2017-07-24 11:12:39	2017-07-24 15:32:14	Tarifa por Día	2	30.0	0.0	0.0
1304	Habitación individua	Jose		2017-07-24 15:46:54	2017-07-24 15:49:17	Tarifa por Día	1	30.0	0.0	0.0
1309	Habitación individua	Hill		2017-07-24 15:50:58	2017-07-24 16:19:58	Tarifa por Día	1	30.0	0.0	0.0
1307	Habitación individua	Hill		2017-07-24 15:50:58	2017-07-24 16:19:58	Tarifa por Día	1	30.0	0.0	0.0
1310	Habitación individua	Hill		2017-07-24 15:50:58	2017-07-24 16:19:58	Tarifa por Día	1	30.0	0.0	0.0
1308	Habitación individua	Hill		2017-07-24 15:50:58	2017-07-24 16:19:58	Tarifa por Día	1	30.0	0.0	0.0
1305	Habitación individua	Hill		2017-07-24 15:50:58	2017-07-24 16:19:58	Tarifa por Día	1	30.0	0.0	0.0
1302	Habitación individua	Prueba		2017-07-24 11:09:10	2017-07-24 16:20:31	Tarifa por Día	2	30.0	0.0	0.0
1301	Habitación individua	Jose		2017-07-24 10:58:28	2017-07-24 16:20:37	Tarifa por Día	2	30.0	0.0	0.0
1306	Habitación individua	Jefe		2017-07-24 16:20:49	2017-07-24 16:37:29	Tarifa por Día	1	30.0	0.0	0.0
1302	Habitación individua	Jefe		2017-07-24 16:20:49	2017-07-24 16:37:29	Tarifa por Día	1	30.0	0.0	0.0

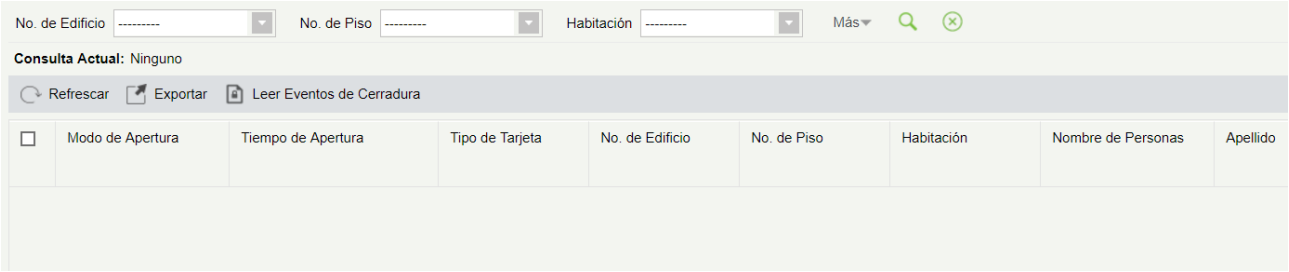
6.5.4 Reporte de Emisión de Tarjetas

Puede ver todos los registros de emisión de tarjetas o buscarlos mediante múltiples condiciones de búsqueda. Introduzca las condiciones de la búsqueda (incluyendo la hora, tipo y número de tarjeta, fecha de emisión y expiración) y visualice los registros de emisión asociados.



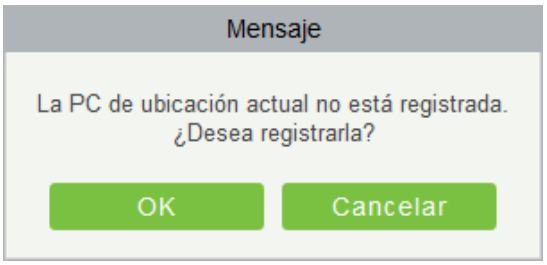
6.5.5 Reporte de Eventos de Cerradura

Puede leer una tarjeta de eventos para verificar los registros de una cerradura. Coloque la tarjeta en el codificador y de clic en **Leer Eventos de Cerradura** para obtener todos los eventos de la cerradura de con la tarjeta de eventos. Introduzca las condiciones de la búsqueda (incluyendo el edificio, piso, nombre de habitación, fecha inicial y final) y visualice los registros asociados. Puede exportar los registros en un archivo de Excel, PDF o CSV.



7 Módulo de Visitantes

Después de dar clic en [Visitante], emergerá la siguiente ventana. De clic en [OK] para registrar las PC cliente que accederán al servidor en la lista de Lugar de Entrada. Para más información acerca del registro de Lugar de Entrada, consulte Lugar de Entrada .



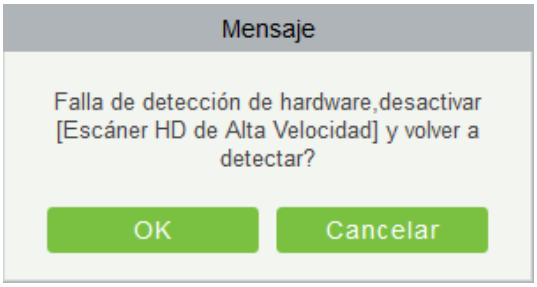
7.1 Registro de Visitas

7.1.1 Registro de Entrada

- Registro de Entrada

1. De clic en [Registro de Visitas] > [Registro de Entrada], el sistema detectará el hardware del entorno basado en los parámetros de [Parámetros] en [Gestión Básica] antes de entrar a la página de registro:

Si la detección es completada, de clic en [Cerrar] para continuar el registro como se muestra en la figura de abajo en la izquierda. Si la detección es fallida, el sistema mostrará un mensaje, de clic el [OK] para cerrar la ventana de registro, como se muestra en la figura de abajo en la derecha.

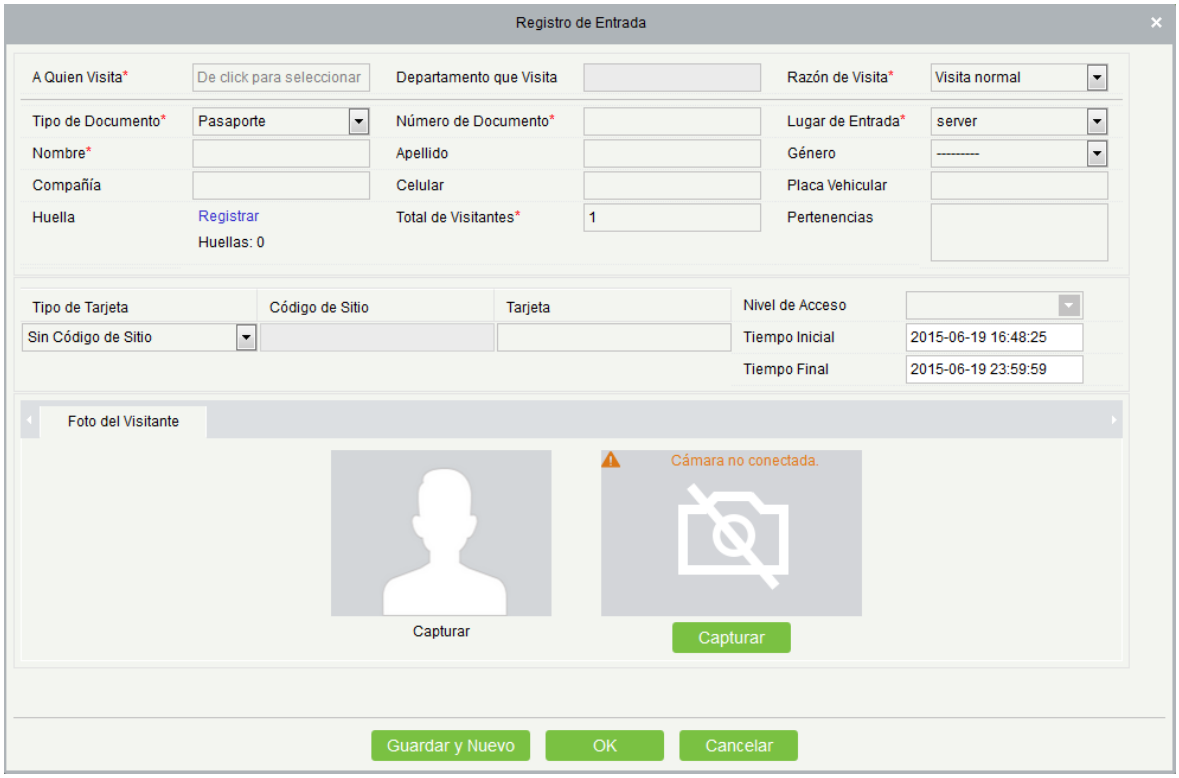


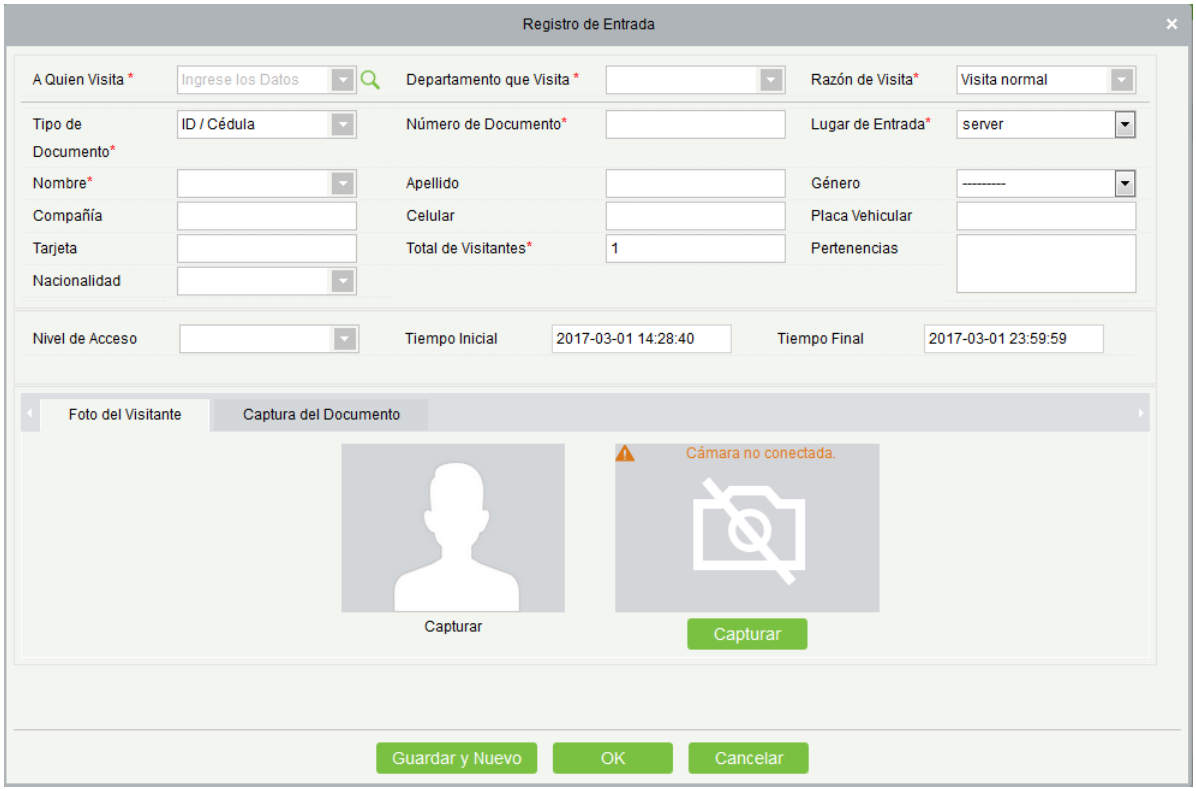
✍Nota:

1) En [Parámetros] de [Gestión Básica], si está marcado "Después de Registrar Imprimir Comprobante", "Requiere Huella Digital" y "Usar Escáner HD de Alta Velocidad", los controladores o drivers correspondientes serán detectados. Para más detalles acerca de [Parámetros], consulte Parámetros.

2) Si se detecta que un driver no está instalado o se encuentra instalada una versión obsoleta, el sistema pedirá que descargue los drivers más recientes.

2. La página de registro se muestra a continuación:





Descripción de los campos:

A Quién Visita: Seleccione el personal al que visita (anfitrión).

A Quién Visita: Seleccione el departamento del anfitrión.

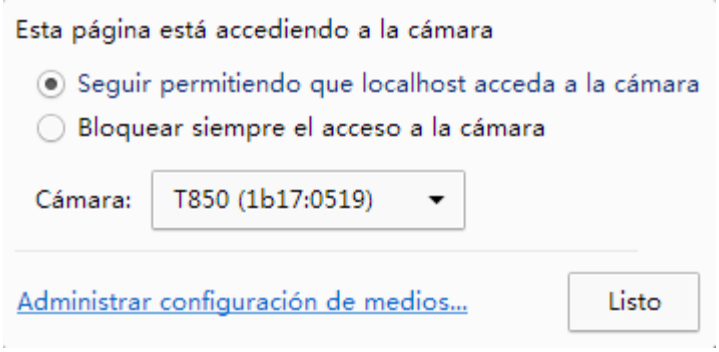
Razón de Visita: Seleccione la razón de la visita. Puede agregar nuevas razones de visita y se mostrará en la lista de Razón de Visita en [Gestión Básica] > [Razón de Visita].

Tipo de Documento: Puede seleccionar Pasaporte, Licencia de Conducir, ID Personal y Otros.

Lugar de Entrada: Seleccione el lugar por donde está accediendo el visitante. Puede agregar lugares de entrada en [Gestión Básica] > [Lugar de Entrada].

Número de Documento: Números y letras del documento de identificación del visitante. Máx. 20.

Foto del Visitante: Si existe una cámara conectada en la PC servidor, puede dar clic en [Capturar] para tomar la foto del visitante. El navegador pudiera bloquear el acceso a la cámara, por lo que debe dar clic en el ícono en la barra de dirección para seleccionar la cámara y permitir el acceso a esta página.



✍Notas:

1) Cada navegador mostrará diferente contenido y mensajes, la pantalla del navegador prevalece, solo elija la cámara compartida y permita el acceso a la cámara.

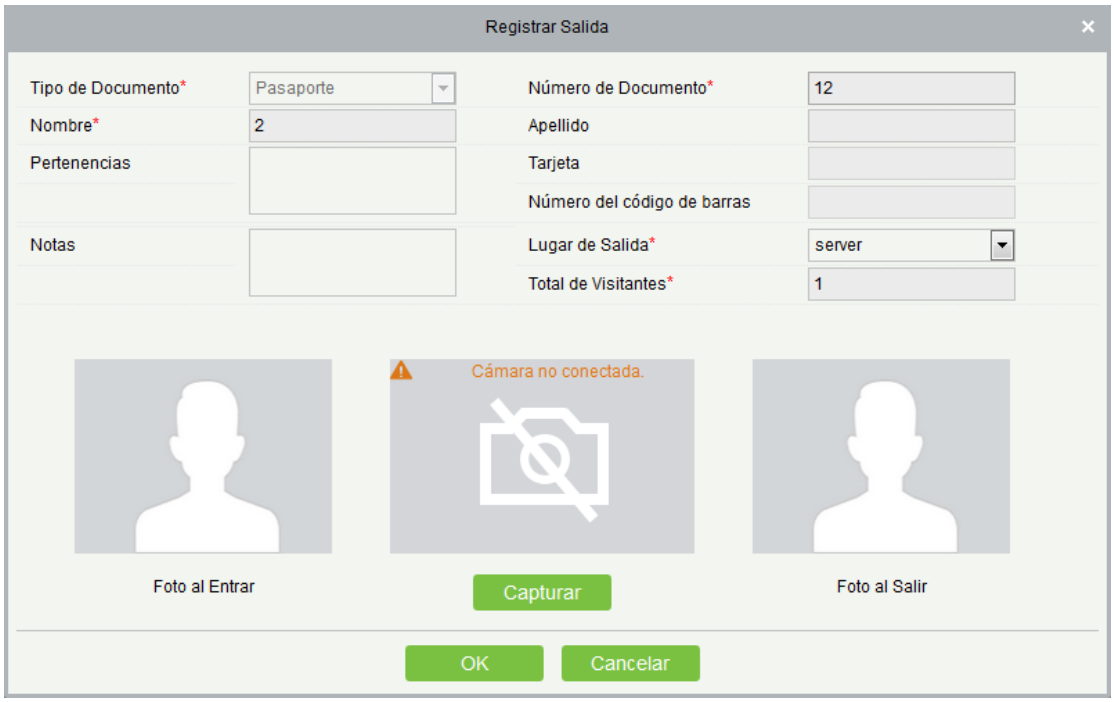
2) Si el Lugar de Entrada soporta cámara IP, scanner y cámara de alta velocidad, no mostrará este aviso.

3) Puede seleccionar ya sea el número de tarjeta o huella para el registro (configure en los parámetros).

- Registrar Salida

Existen 2 maneras:

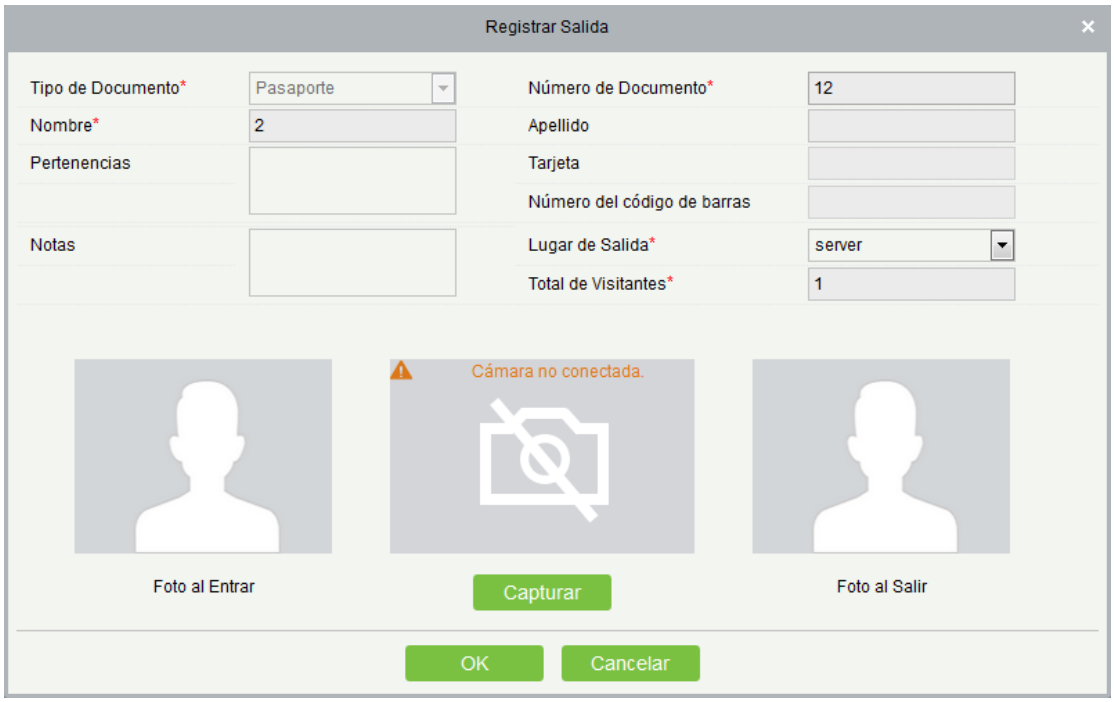
1. De clic en [Registrar Salida] debajo de Operaciones cuando un visitante está listo para salir.



Seleccione el Lugar de Salida y de clic en [OK].

2. Puede dar clic en [Registrar Salida] en la barra del menú cuando exista mucha información en la lista:

:



Introduzca el Número de Documento para obtener la demás información del visitante rápidamente. Seleccione el Lugar de Salida y de clic en [OK].

7.1.2 Información de Visitantes

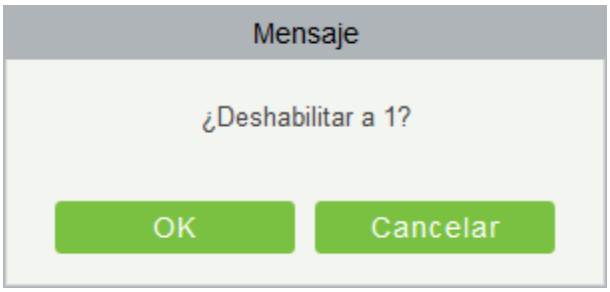
Puede borrar, deshabilitar o habilitar un visitante.

- Borrar un Visitante

De clic en [Registro de Visitas] > [Información de Visitantes], seleccione y de clic en [Borrar].

- Deshabilitar Visitante

De clic en [Registro de Visitas] > [Información de Visitantes], seleccione y de clic en [Deshabilitar].



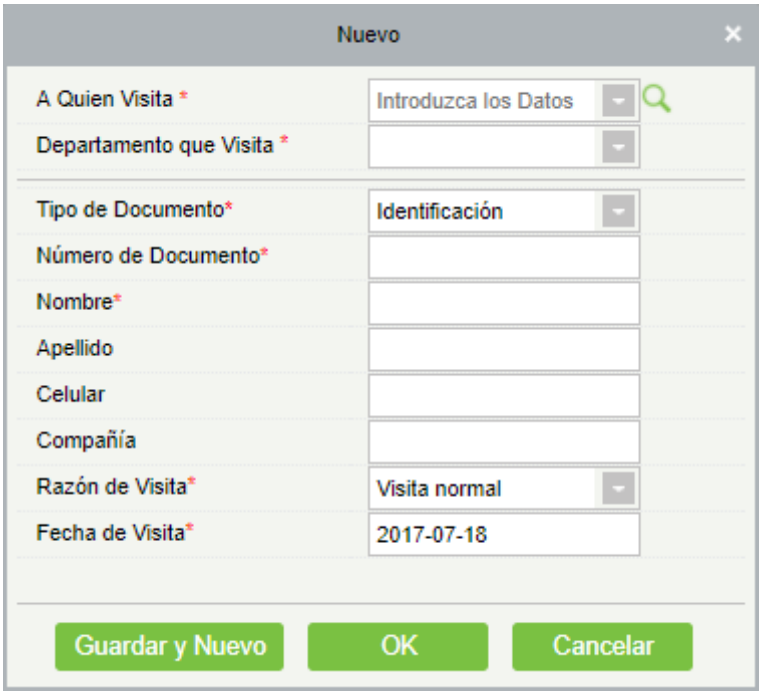
De clic en [OK] para deshabilitar al visitante. Se mostrará la marca debajo de Deshabilitado.

- Habilitar Visitante

De clic en [Registro de Visitas] > [Información de Visitantes], seleccione y de clic en [Habilitar].

7.2 Reservación

1. De clic en [Reservación] > [Reservación] > [Nuevo]:



A Quién Visita: Seleccione al anfitrión. De clic en el campo para filtrar la consulta de acuerdo a los caracteres introducidos, o de clic en el botón de búsqueda para emerger la lista de los usuarios para seleccionar el anfitrión.

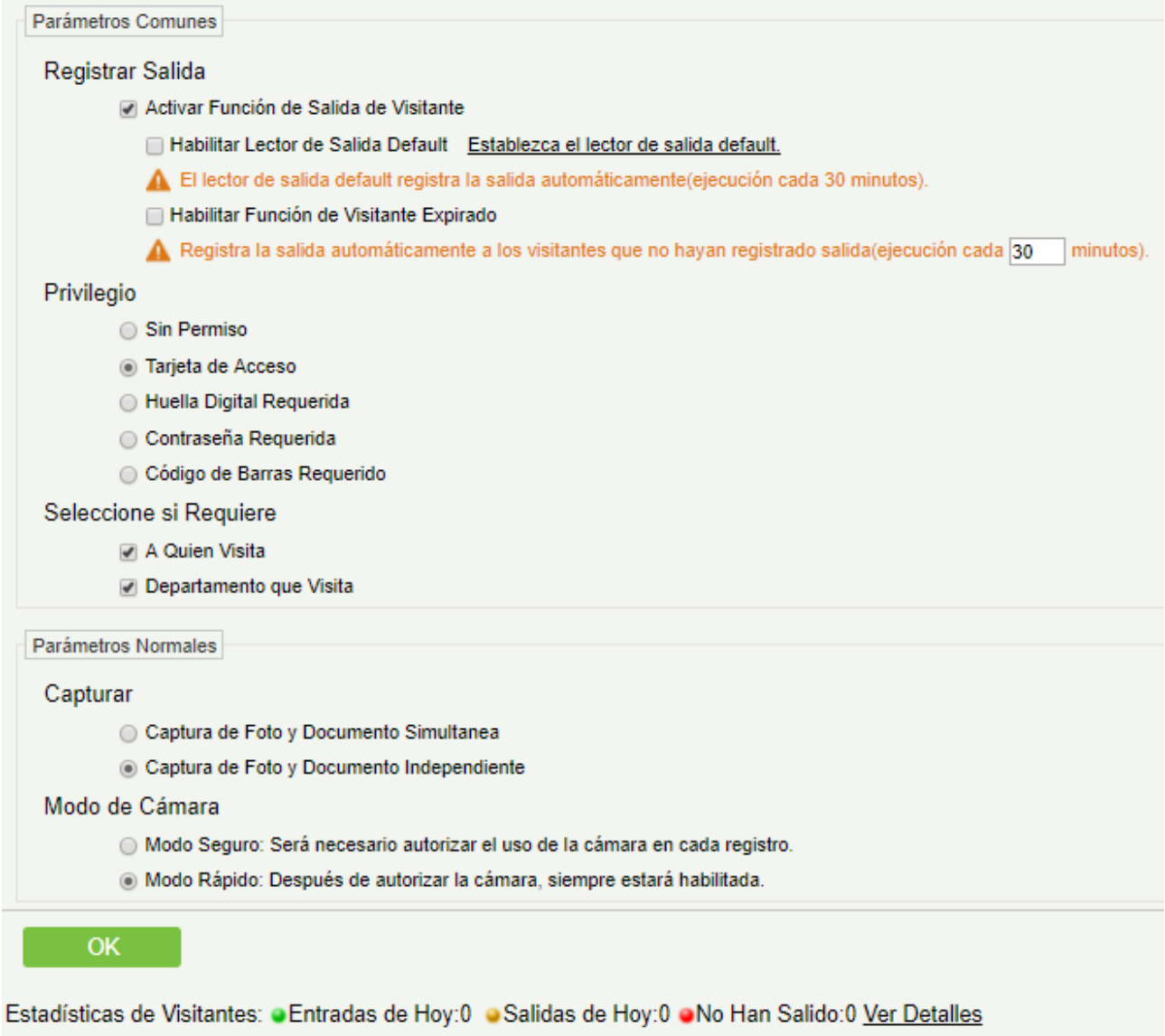
2. Introduzca los datos de la reservación y de clic en [OK].

Los usuarios del sistema pueden realizar las reservaciones por sí mismos en "Gestión de Visitas". El método es el mismo con las descripciones anteriores. Acerca de cómo acceder a la interfaz de Gestión de Visitas consulte Gestión de Visitas.

7.3 Gestión Básica

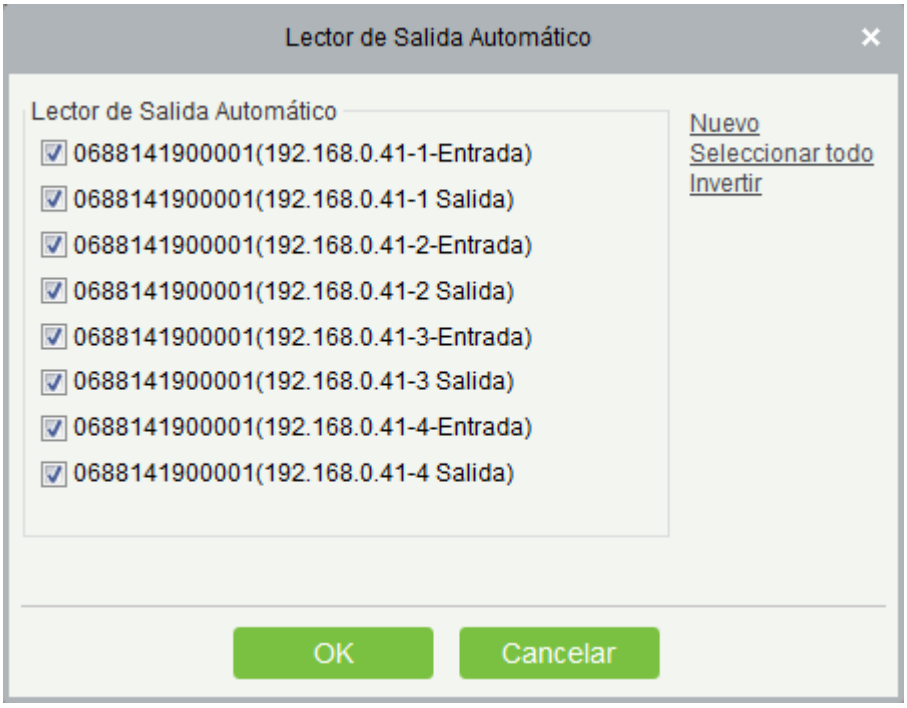
7.3.1 Parámetros

De clic en [Gestión Básica] > [Parámetros]:



- Parámetros Comunes

Registrar Salida: Habilite o deshabilite la función de lector de salida defecto. Auto Salida significa que cuando un visitante sale presentando una tarjeta o usando su huella en un lector pre definido, sin realizar la operación de Registrar Salida en el software. La configuración de lector de salida defecto requiere especificar los lectores para realizar la salida automática. De clic en [Establezca el lector de salida defecto]:



De clic en [OK] para terminar.

Función de Visitante Expirado: A los visitantes expirados que no hayan registrado salida manualmente, se les realizará el registro de salida automático después de un intervalo específico.

Mostrar Pop-Up con Información de Visitantes: Establece la hora para recordar los visitantes que no han salido, cada día.

- Privilegio

Tarjeta de Acceso: Seleccione si desea usar tarjeta de acceso para los visitantes.

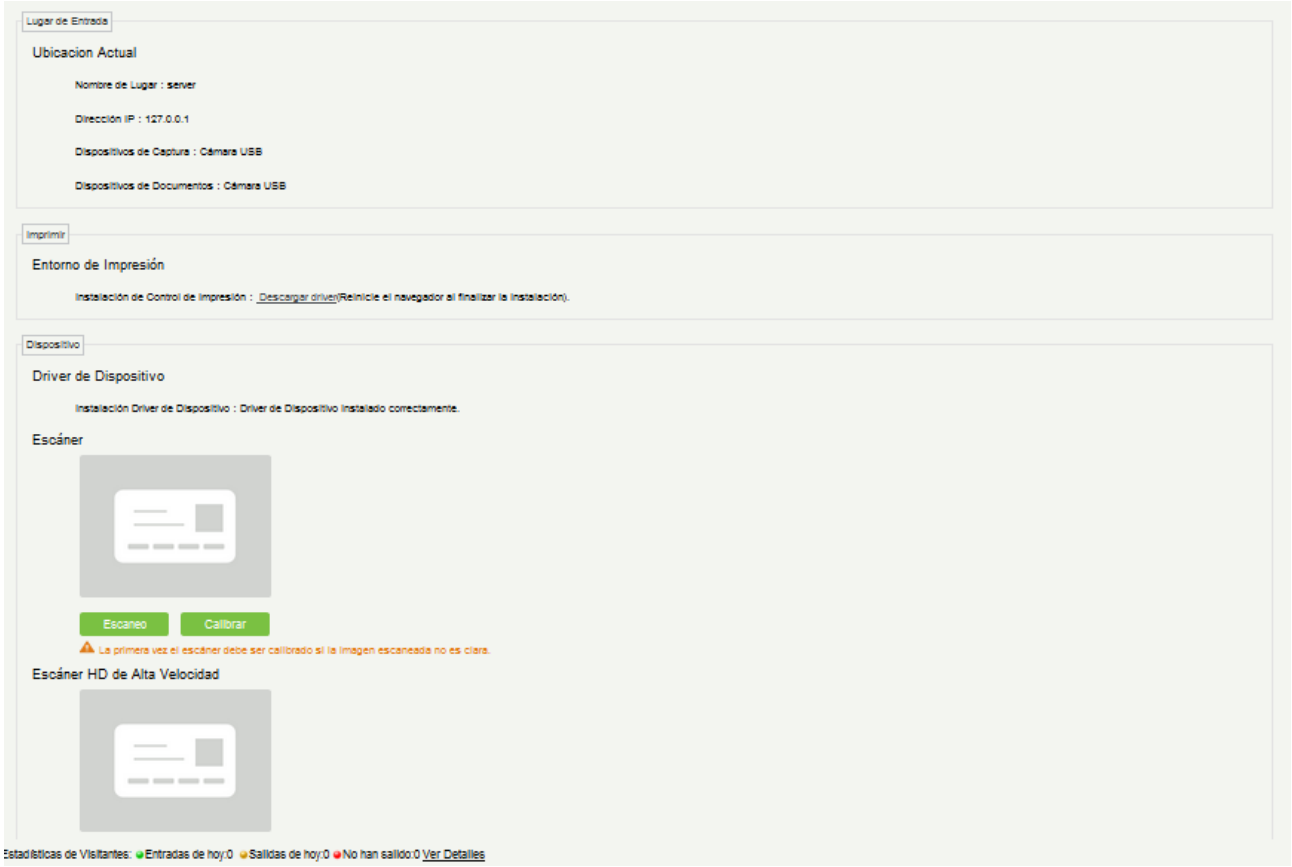
Huella Digital Requerida: Seleccione para registrar las huellas digitales de los visitantes.

- Modo de Cámara: Configure la cámara USB para habilitarla permanentemente o en cada registro.
- Seleccione si Requiere: Puede definir si desea solicitar la información del anfitrión y departamento que visita en la pantalla de registro o la ventana de reservación.
- Parámetros Normales

Dispositivos: Seleccione si desea usar dispositivos para escanear documentos.

- Destinatario de Correo de Lista de Visitantes: Introduzca la dirección de email del destinatario y la hora en la que el sistema enviará la lista de visitantes del día.

7.3.2 Depuración de Equipo

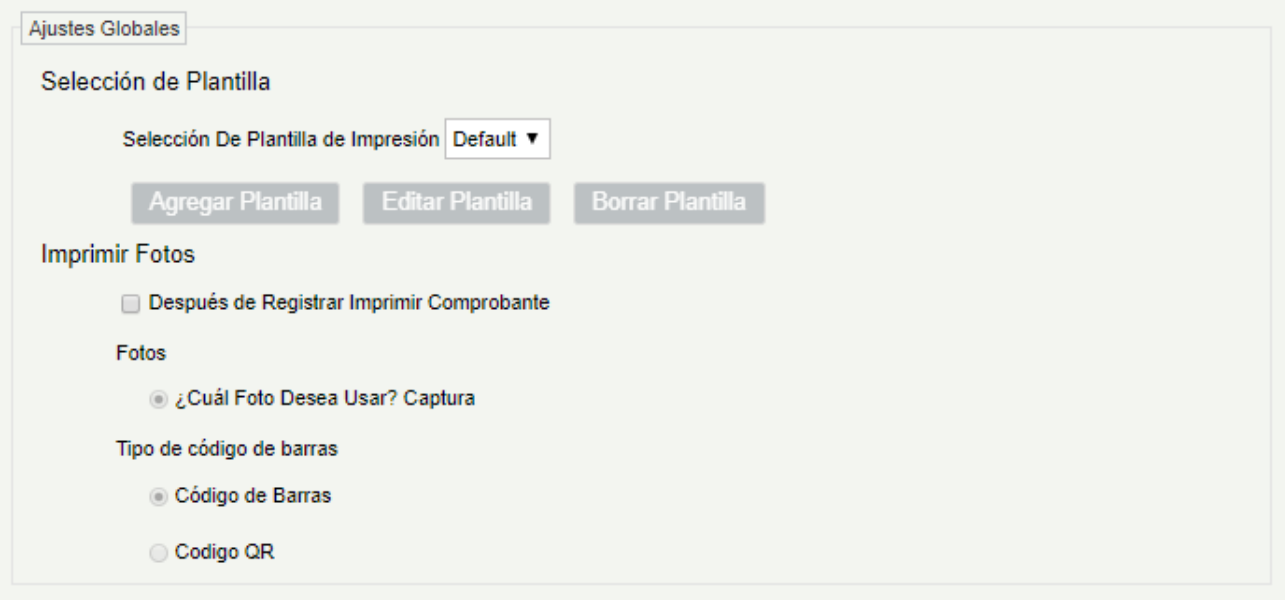


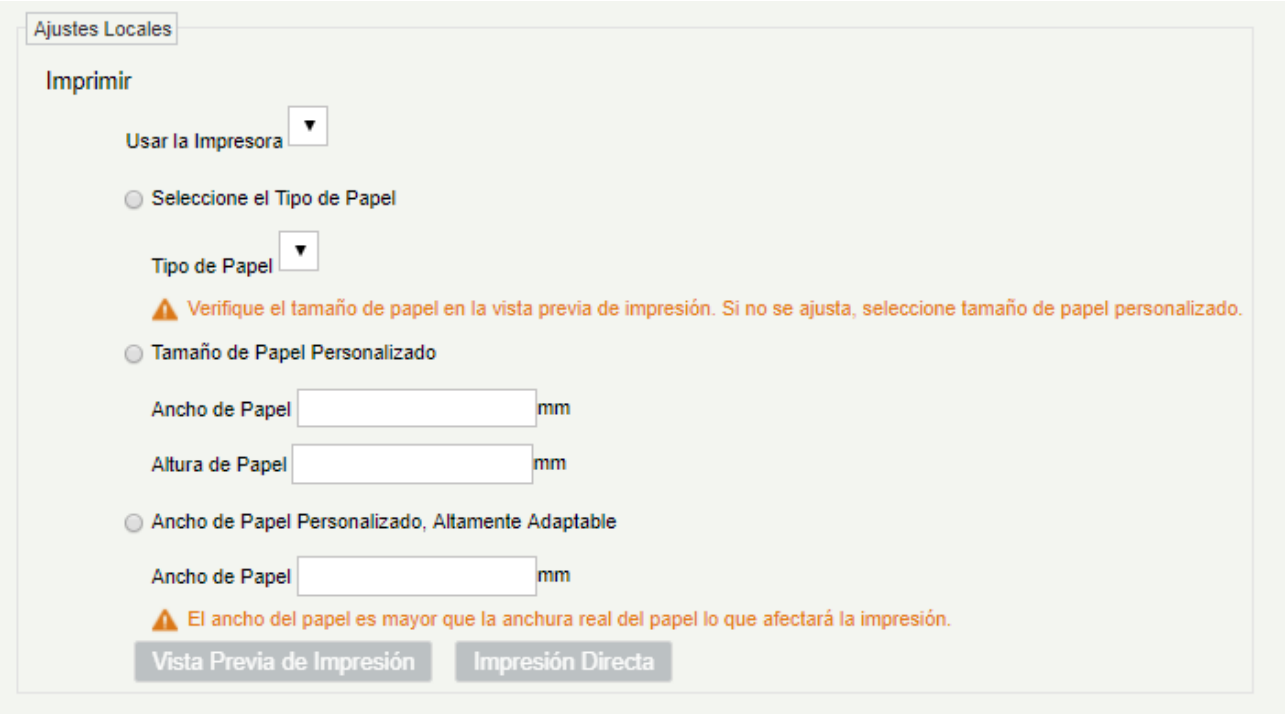
Nombre de Lugar: Muestra la información del lugar de entrada, tales como el nombre del lugar, dirección IP, equipo en uso, etc.

Imprimir: Entorno de impresión.

Dispositivo: Muestra la instalación del driver del dispositivo y depuración del escáner, cámara de alta definición y cámara USB cuando haya instalado los drivers correctamente (el navegador IE no muestra la depuración de equipos).

7.3.3 Ajustes de Impresión





- Ajustes Globales (Aplican en todos los Lugares de Entrada)

Selección de Plantilla: Seleccione una plantilla para imprimir el comprobante. Si la plantilla no tiene el contenido deseado, puede editar la plantilla o agregar una nueva (la plantilla defecto no puede ser editada ni eliminada).

Imprimir Fotos: Seleccione si desea imprimir un comprobante después de registrar un visitante si el servidor está conectado con una impresora y si desea incluir la imagen (foto o captura del visitante).

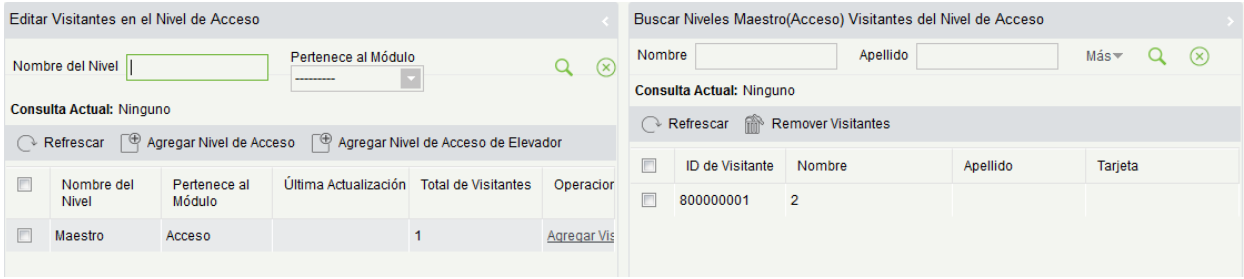
- Ajustes Locales (Aplican solo en el Lugar de Entrada actual)

Imprimir: Puede realizar los ajustes de la impresora, el tipo del papel, personalizar el tamaño de papel y ver el resultado dando clic en Vista Previa de Impresión o Impresión Directa. Finalmente puede guardar los ajustes de impresión del punto de entrada actual.

7.3.4 Niveles de Acceso de Visitantes

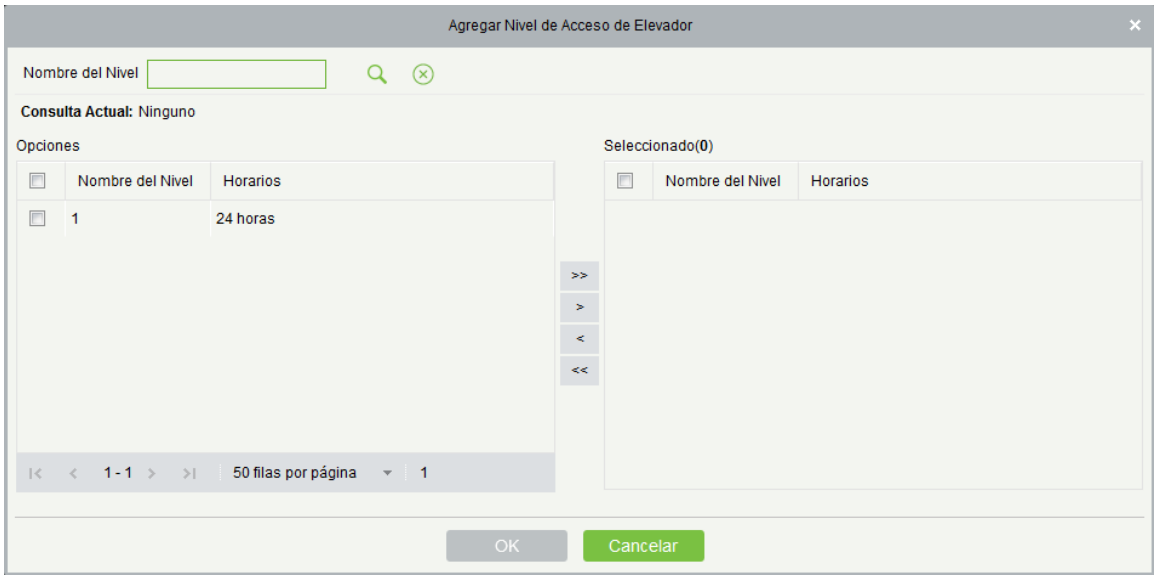
Es posible asignar niveles de acceso o de elevador una vez que se hayan configurado los niveles.

De clic en [Gestión Básica] > [Niveles de Visitante]:



- Agregar Niveles de Acceso

De clic en [Gestión Básica] > [Niveles de Visitante] > [Agregar Nivel de Acceso]:



Introduzca el nombre del nivel, seleccione uno o varios niveles de acceso, de clic en > o >> para mover al menú de Seleccionado y de clic en [OK].

Asignar los niveles de acceso para el visitante al momento del registro.

- Agregar Niveles de Acceso de Elevador

La operación se realiza igual que Agregar Nivel de Acceso.

- Borrar Niveles

Seleccione el nivel del visitante, de clic en [Borrar] en la lista de [Mas].

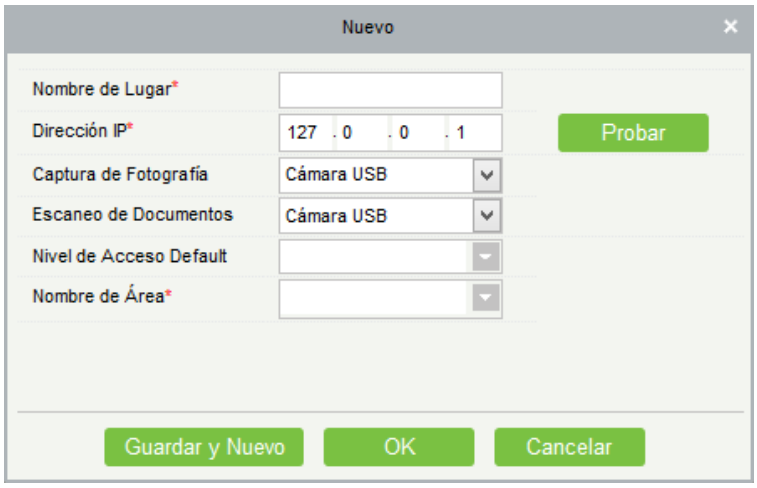
- Refrescar Niveles de Acceso

Cuando los niveles de acceso o elevador son modificados, de clic en [Refrescar Niveles de Acceso] en la lista de [Más] para actualizar los datos modificados.

7.3.5 Lugar de Entrada

- Agregar un Lugar de Entrada

De clic en [Gestión Básica] > [Lugar de Entrada] > [Nuevo]:



Descripción de los campos:

Nombre del Lugar: No se debe repetir. Puede introducir hasta 50 caracteres.

Dirección IP: La dirección IP de la PC servidor.

Captura de Fotografía: Puede seleccionar Cámara USB o IP. La cámara IP debe agregarse previamente en dispositivos de video.

Escaneo de Documentos: Seleccione el dispositivo para escaneo de documentos, puede ser cámara USB, escáner de alta velocidad, escáner.

Nivel de Acceso Defecto: Establece el nivel de acceso defecto para este lugar de entrada.

Nombre de Área: El nombre de área al que pertenece el lugar de entrada. El registro de entrada del visitante podrá ser filtrado de acuerdo al área del lugar de entrada.

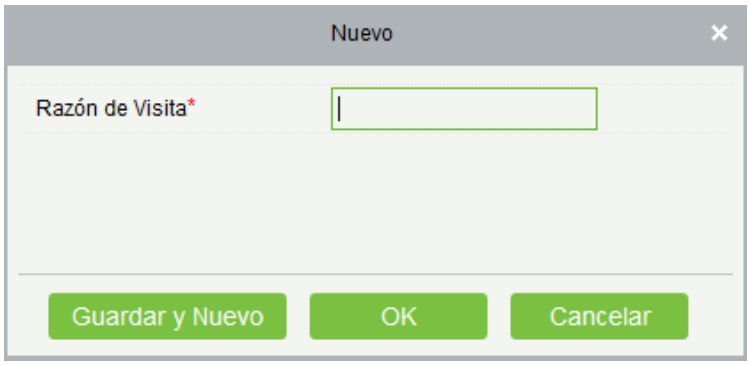
2. De clic en [Editar] o [Borrar] como sea necesario.

- Lugar de Salida Automático

Consulte Parámetros.

7.3.6 Razón de Visita

1. De clic en [Gestión Básica] > [Razón de Visita] > [Nuevo]:



2. Introduzca la razón y de clic en [OK] para terminar. De clic en [Editar] o [Borrar] como sea necesario.

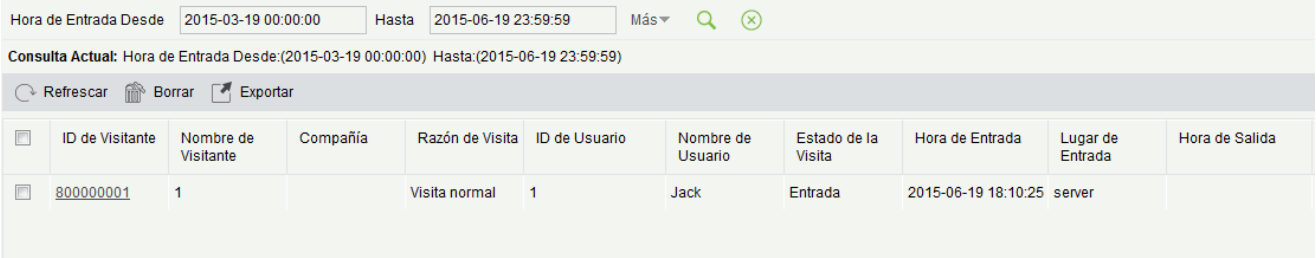
7.4 Reportes de Visitantes

7.4.1 Último Acceso Registrado

De clic en [Reportes] > [Último Acceso Registrado] para ver el reporte. Los reportes pueden ser filtrados por diferentes condiciones de búsqueda.

7.4.2 Historial de Visitas

De clic en [Reportes] > [Historial de Visitas] para ver los reportes. Los reportes pueden ser filtrados por diferentes condiciones de búsqueda.



7.4.3 Gráficas

De clic en [Visitantes] > [Reportes] > [Gráficas]. Se muestran las gráficas de los registros de visitantes.

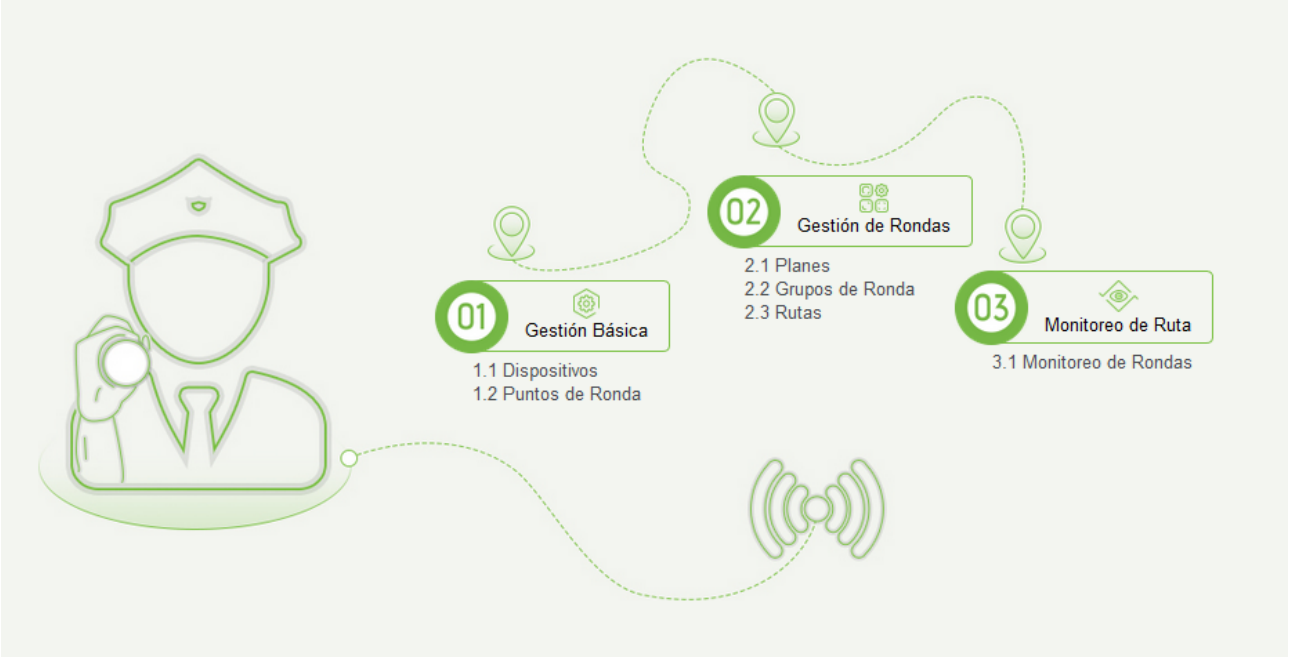
8 Sistema de Rondas

El módulo de rondas brinda a directivos y administradores de corporativos la capacidad de supervisar de forma efectiva al personal de vigilancia incluyendo los planes, rutas y tiempos de vigilancia. Además, permite realizar estadísticas periódicas y análisis basados en los resultados de las rondas.

✍Nota: Antes de realizar cualquier operación en el módulo de rondas, es necesario agregar dispositivos de ronda en el módulo de [Acceso] y agregar personal de ronda en el módulo de [Personal].

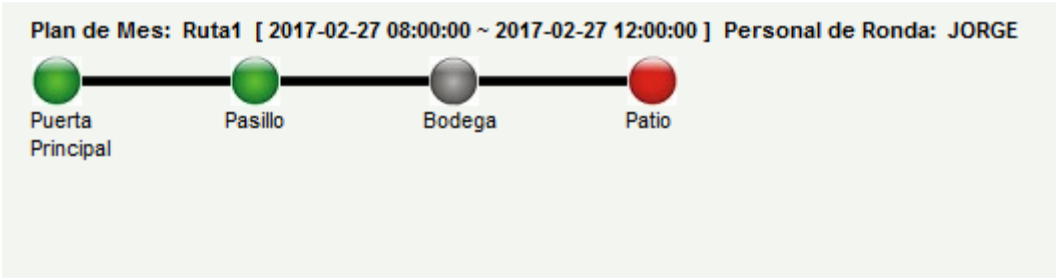
8.1 Asistente de Configuración

Después de iniciar sesión en el sistema, de clic en [Rondas] para ir al [Asistente de Configuración]. De clic en la página como sea necesario para acceder a las diferentes funciones del módulo y realizar las operaciones. La página se muestra a continuación:



8.2 Monitoreo de Rondas

Esta función muestra todas las rutas programadas del día en el plan de ronda. Cuando el personal de ronda realiza la ronda conforme al plan, los puntos de la ronda cambiarán a color verde. Si el personal no realiza la ronda conforme al plan, los puntos de ronda cambiarán a color rojo. La página se muestra a continuación:



Estados de los Puntos:

Ronda Normal: El personal completó la ronda en el tiempo y secuencia establecido.

Error de Ruta: El personal completó la ronda en el tiempo establecido, pero no siguió la ruta correctamente.

Ruta Anormal: El personal no completó la ronda en el tiempo establecido, esto significa que uno o más puntos de ronda no fueron vigilados.

Sin Ronda: El personal no realizó la ronda en el tiempo establecido, esto significa que la ronda no fue realizada en su totalidad.

8.3 Gestión Básica

8.3.1 Dispositivos

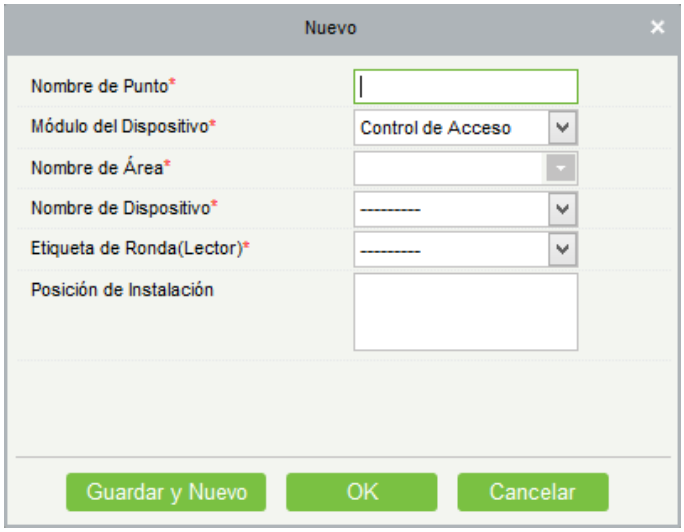
- Agregar

Seleccione el equipo que será usado como dispositivo de ronda entre los dispositivos de control de acceso. De clic en [Gestión Básica] > [Dispositivos] > [Nuevo]. En la tabla de [Opciones] seleccione los dispositivos disponibles y de clic en [OK] para guardar los cambios. La página se muestra a continuación:

8.3.2 Puntos de Ronda

- Agregar

(1) De clic en [Gestión Básica] > [Puntos de Ronda] > [Nuevo]. La página se muestra a continuación:

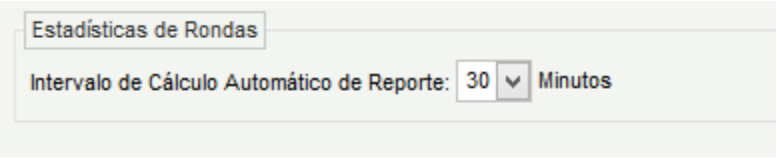


Nombre del Punto: Actualmente solo son soportados lectores de equipos de control de acceso.

(2) Después de llenar los campos (parámetros con * son obligatorios), de clic en [OK] para guardar los cambios. Puede dar clic en [Guardar y Nuevo] para guardar la configuración actual y agregar otro punto de ronda. De clic en [Cancelar] para cancelar la operación y regresar al menú anterior.

✍Nota: Los puntos de ronda que han sido agregados anteriormente no pueden usarse de nuevo para agregar otro punto de ronda.

8.3.3 Parámetros



1) De clic en [Rondas] > [Gestión Básica] > [Parámetros].
2) Establezca el intervalo para recopilar las estadísticas de la ronda.
3) De clic en [OK] para guardar los cambios.

8.4 Gestión de Rondas

8.4.1 Plan

- Agregar

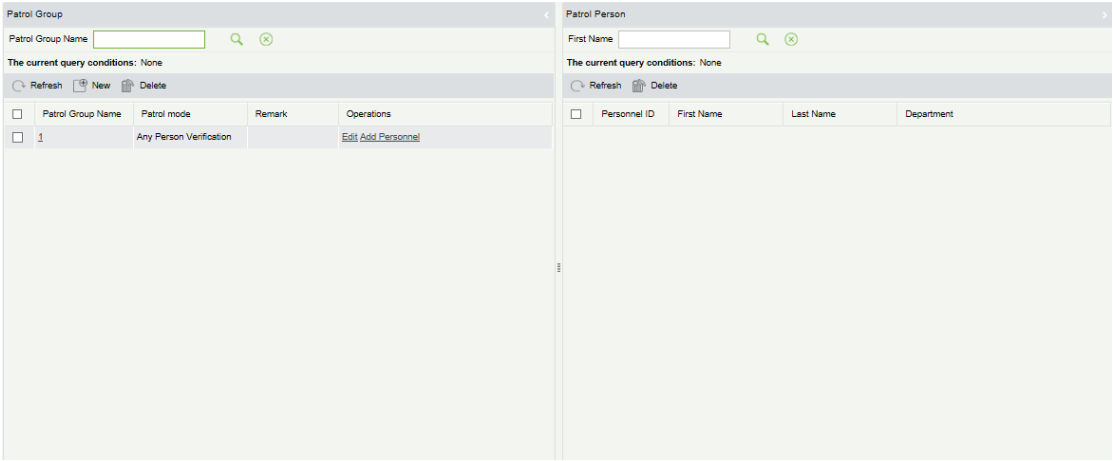
De clic en [Gestión de Rondas] > [Planes] > [Nuevo]. Se puede ajustar el plan por fecha, semana y mes como se muestra a continuación:

Segmento de Tiempo: Establezca el tiempo inicial y final de la ronda. El segmento puede cubrir los días siguientes.
Por Fecha: El plan de ronda se programa por fechas. Seleccione [Por Fecha] y configure la fecha inicial y final del plan de ronda.
Por Semana: El plan de ronda se programa por semana.

Por Mes: El plan de ronda se programa por mes.
Un plan de ronda por mes puede ser ejecutado diariamente o periódicamente. Si selecciona ejecutar la ronda diariamente, la ronda debe realizarse cada día en el mes específico. Si selecciona periódicamente, la ronda debe realizarse en las fechas específicas del mes.
✍Nota: Se pueden agregar un máximo de tres turnos en un plan de ronda.

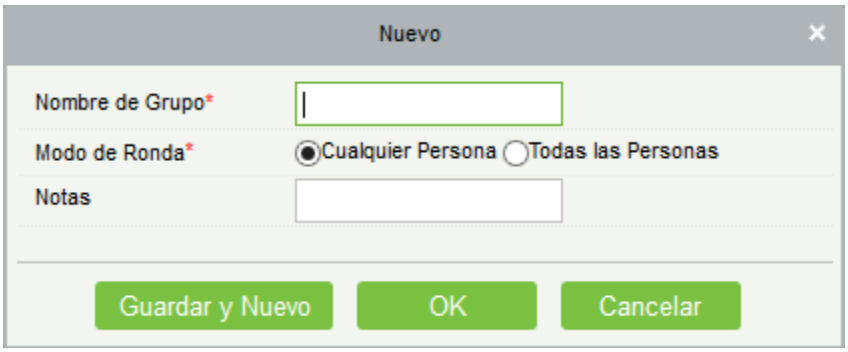
8.4.2 Grupos de Ronda

Un grupo de ronda consiste en múltiple personal para realizar las rondas. El personal en el grupo de ronda trabaja en conjunto para terminar la ronda correspondiente. De clic en [Gestión de Rondas] > [Grupos de Ronda].



- Agregar

1. De clic en [Gestión de Rondas] > [Grupos de Ronda] > [Nuevo] para ir a la ventana de agregar grupo como se muestra a continuación:



2. Configure los siguientes parámetros: Introduzca un nombre para el grupo de ronda (no repetible), el Modo de Ronda y las notas correspondientes.
3. De clic en [Guardar y Nuevo] para agregar otro grupo de ronda de clic en [OK] para terminar.
4. Agregue/Elimine personal para el grupo de ronda. (Esta operación no se puede realizar si el grupo de ronda está siendo usado en una ruta de ronda).
(1) De clic en [Gestión de Rondas] > [Grupos de Ronda]. De clic en un grupo de ronda de la lista de la izquierda. El personal del grupo de ronda será mostrado en la lista de la derecha.
(2) De clic en [Agregar Personal] debajo de Operaciones Relacionadas de la lista de la izquierda para mostrar la lista de agregar personal (o agregar por departamento). Agregue el personal de la lista hacia la derecha y de clic en [OK]

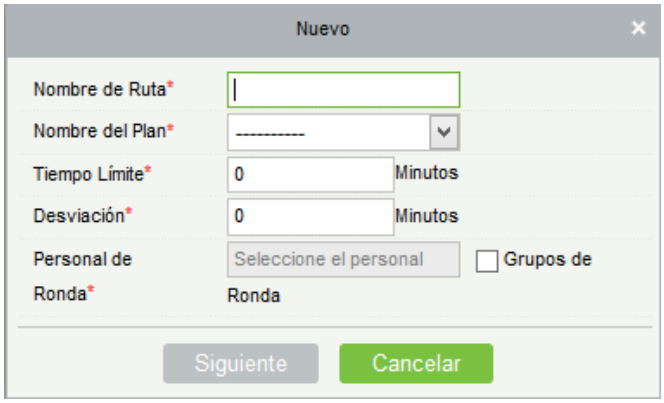
para guardar los cambios.
(3) Seleccione el personal de la lista de la derecha y de clic en [Eliminar] arriba de la lista para eliminar el personal del grupo de ronda.
✍Nota: En [Modo de Ronda], Cualquier Persona significa que la ronda se considerará terminada si al menos una persona del grupo realiza la ronda según el plan mientras que Todas las Personas significa que el plan la ronda deberá ser realizada por todas las personas del grupo para considerarse terminada. Un grupo de ronda no puede ser editada o eliminado si está siendo usado en una ruta de ronda.

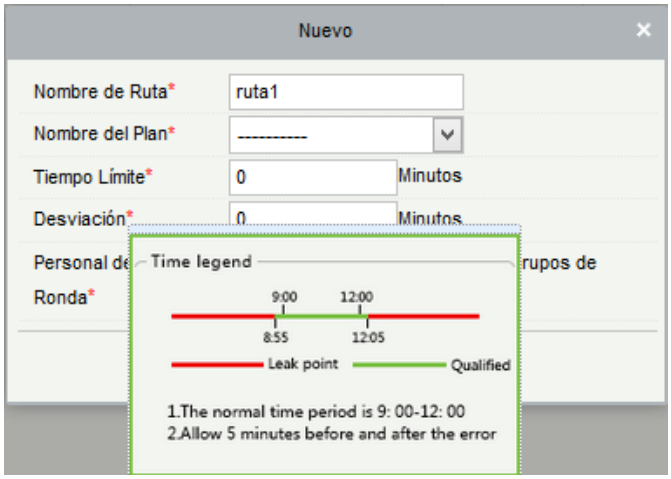
8.4.3 Rutas

Una ruta consiste en una serie de puntos de vigilancia (puntos de ronda) en una secuencia específica.

- Agregar

De clic en [Gestión de Rondas] > [Rutas] > [Nuevo]. Se muestra la página a continuación:
1. Introduzca la información básica de la ruta en los campos de la ventana. El Tiempo Límite se refiere al tiempo total para terminar toda la ruta.

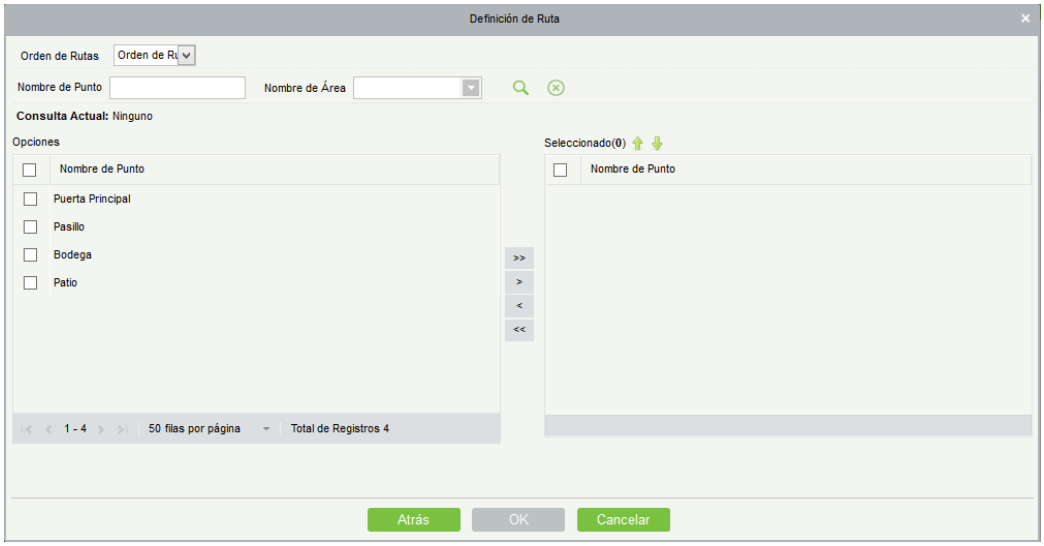




Descripción de la leyenda de segmento de tiempo: Se establece según el margen error permitido durante la ronda. Suponga que el plan de ruta está programado de 09:00 a 12:00 (que puede ser establecido en el plan de ronda) y el margen de error permitido es de 5 minutos; esto significa que si se registró la ronda entre las 08:55 y 12:05 será válido y los registros fuera de este tiempo serán inválidos.
2. Después de configurar, de clic en [Siguiente] para ir a la ventana de [Definición de Ruta]. Las rutas se clasifican en "En Orden" y "Sin Orden" (dos categorías y cinco situaciones están disponibles). Los botones ⬆ y ⬇ se usan

para mover los puntos de ronda hacia arriba y abajo.

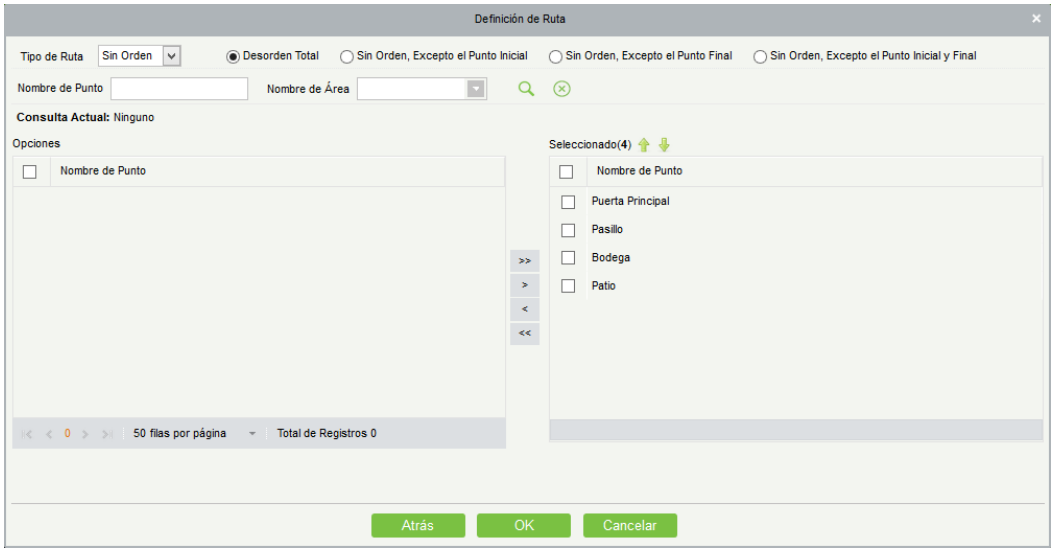
En Orden: Durante la ejecución del plan, no hay límite entre los puntos de ronda. El personal debe realizar la ronda en la secuencia específica conforme a sus hábitos dentro del tiempo límite.



Sin Orden: Las rutas Sin Orden están divididas en las siguientes situaciones:
Desorden Total: Todos los puntos de la ronda están en desorden. El personal puede realizar la ronda conforme a sus hábitos dentro del tiempo límite.
Sin Orden, Excepto el Punto Inicial: En la ruta, todos los puntos de ronda pueden realizarse sin orden, excepto el punto inicial.

Sin Orden, Excepto el Punto Final: En la ruta, todos los puntos de ronda pueden realizarse sin orden, excepto el punto final.

Sin Orden, Excepto el Punto Inicial y Final: En la ruta, todos los puntos de ronda pueden realizarse sin orden, excepto el punto inicial y el final.



3. De clic en [OK] para guardar la configuración.
✍Nota:

Antes de realizar operaciones de rondas, es necesario agregar dispositivos del módulo de [Acceso] y agregar personal del módulo de [Personal]. Tenga en cuenta que el personal que deba realizar la ronda con un número de tarjeta no tiene privilegio para abrir la puerta, ni puede seleccionar ningún privilegio de acceso al agregar el personal o agregar privilegios de puerta en ningún segmento de tiempo, y luego seleccionar los privilegios de control de acceso al agregar el personal.

8.5 Reportes

Hay cuatro opciones: Todos los Eventos, Eventos de Rondas de Hoy, Estadísticas de Rutas y Estadísticas de Personal. Puede analizar y recopilar estadísticas de los datos de las rondas para obtener el control total del proceso de las rondas de vigilancia.

8.5.1 Todos los Eventos

De clic en [Reportes] > [Todos los Eventos] para ver todos los eventos, esto es, todos los registros generados por los dispositivos de ronda.

8.5.2 Eventos de Rondas de Hoy

De clic en [Reportes] > [Eventos de Rondas de Hoy] para ver los eventos del día generados por los dispositivos de ronda.

8.5.3 Estadísticas de Rutas

De clic en [Reportes] > [Estadísticas de Rutas] para ver todas las situaciones normales y anormales recopiladas durante las rondas.

8.5.4 Estadísticas del Personal

De clic en [Reportes] > [Estadísticas del Personal] para ver las estadísticas del personal de rondas.

Rondas Programadas: Número de rondas programadas que el personal debe realizar.

Rondas Reales: Número de rondas que el personal realmente realizó.

Rondas Omitidas: Número de veces que el personal no realizó la ronda de uno o más puntos en la ruta de ronda durante el tiempo programado.

Rondas Incorrectas: Número de rondas que el personal realizó incorrectamente conforme la ruta de ronda.

Ausencias: Número de veces que el personal no realizó rondas.

9 Video

El sistema soporta la integración o vinculación de video con control de acceso y control de elevadores. Es posible realizar la gestión de DVRs, NVRs y Cámaras IP, ver el video en tiempo real, consultar grabaciones y emerger vínculos de eventos automáticamente.

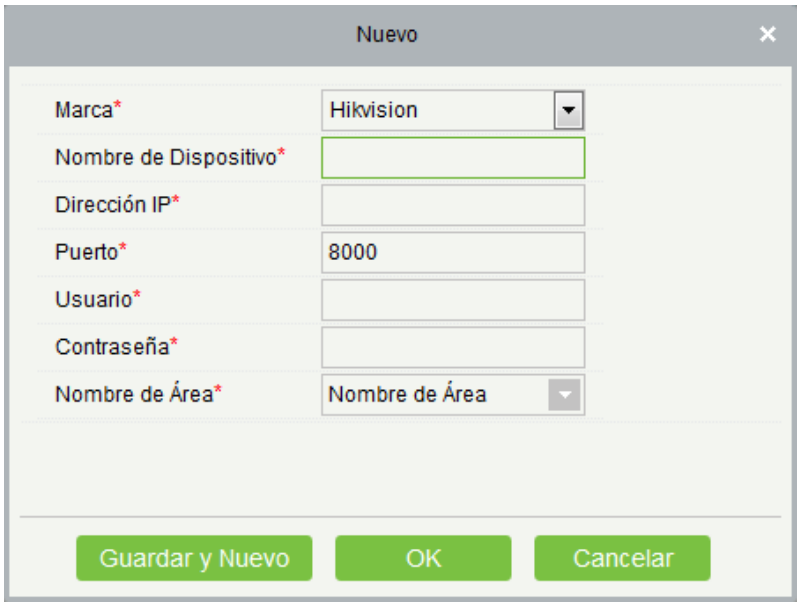
Debe agregar un dispositivo de video y configurar la función de vínculo en Vínculos y Vínculos Globales en avanzado.

✍Nota: Para más detalles sobre los modelos compatibles, contacte al personal de soporte técnico.

9.1 Dispositivo de Video

- Agregar un Dispositivo de Video

De clic en [Video] > [Dispositivos de Video] > [Dispositivos de Video] > [Nuevo]:



Descripción de los Campos:

Marca del Dispositivo: Seleccione la marca.

Nombre de Dispositivo: Cualquier caracter con un máximo de 30.

IP: Introduzca la Dirección IP del dispositivo.

Puerto: El puerto defecto es 8000.

Usuario: Usuario admin del dispositivo de video. Máximo 15 caracteres (sin espacios).

Contraseña: Contraseña del usuario admin. Máximo 32 caracteres (sin espacios).

Área: Área del dispositivo.

- Habilitar/Deshabilitar un Dispositivo de Video

Seleccione un dispositivo de la lista y de clic en [Habilitar] o [Deshabilitar].

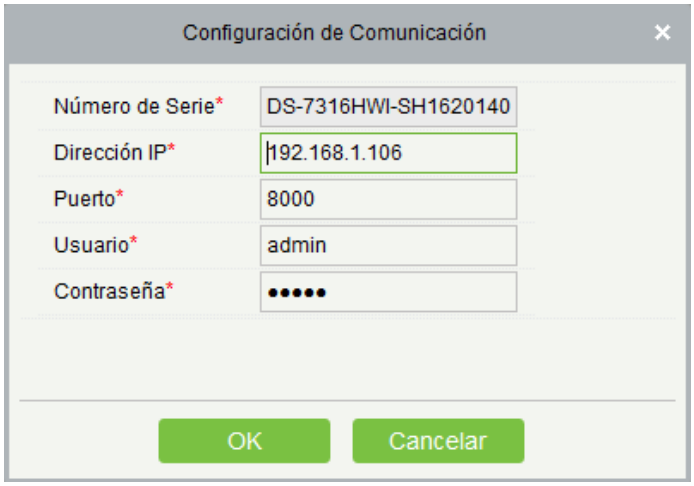
- Editar/Borrar un Dispositivo de Video

Seleccione un dispositivo de la lista y de clic en [Editar] o [Borrar].

- Configuración de Comunicación

Cuando los parámetros de comunicación son modificados en el dispositivo, la modificación se debe sincronizar al software para preservar la consistencia, de lo contrario los canales de video y la integración al sistema no funcionarán normalmente.

Seleccione un dispositivo y de clic en [Configuración de Comunicación]:



9.2 Canales de Video

Al agregar un dispositivo de video, el sistema automáticamente detectará el número de cámaras del dispositivo, es decir, el número de canales, y generará la lista correspondiente. Por ejemplo, al agregar un dispositivo de 16 cámaras, el sistema generará la lista de 16 canales de video y los nombrará usando el formato "Nombre de Dispositivo – Número de Canal".

- Habilitar/Deshabilitar Dispositivo de Video

De clic en [Video] > [Dispositivos de Video] > [Canales]:

De clic en [Editar] debajo de Operaciones en la lista:

Descripción de los campos:

Nombre del Canal: Cualquier carácter. Máximo 30.

El Nombre del Dispositivo, Número de Canales y Estado de Canal no son editables en esta interfaz. Pueden modificarse en 7.1 Dispositivos de Video. El número de canal es el correspondiente al dispositivo.

9.3 Video en Tiempo Real

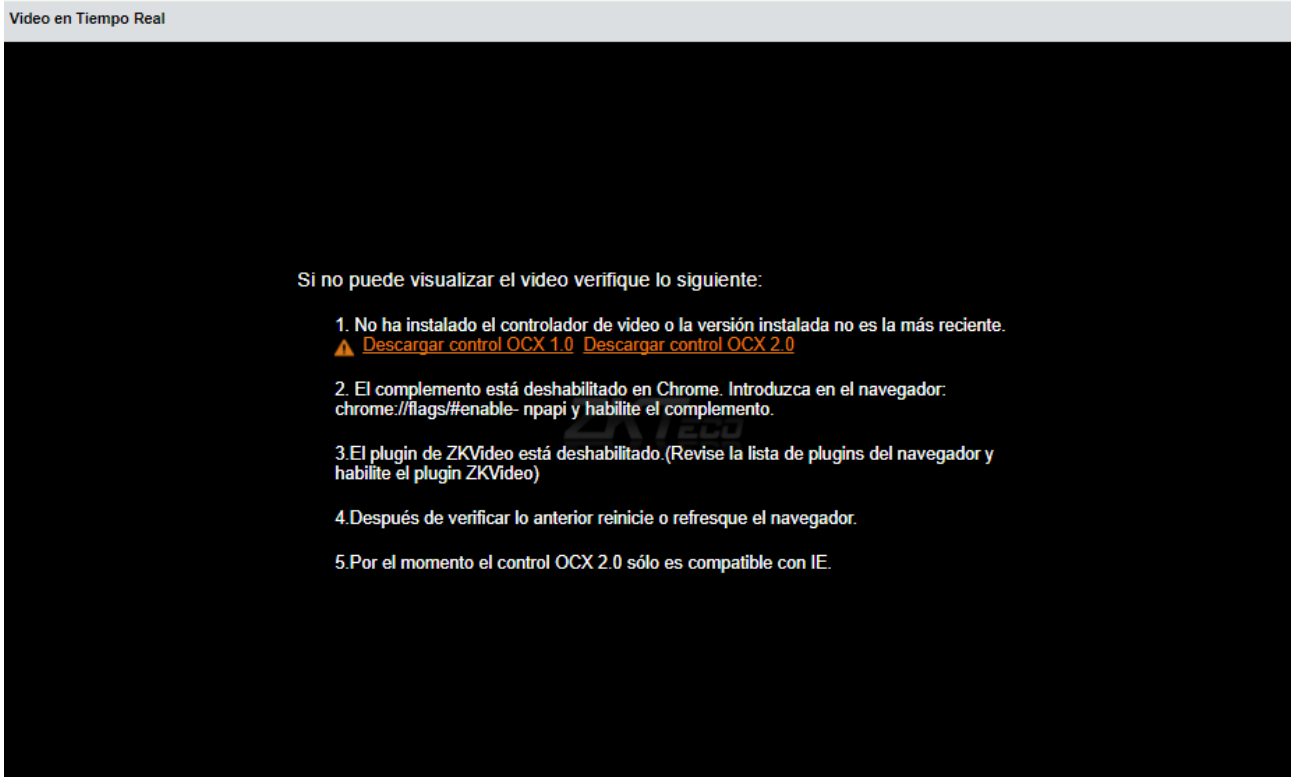
De clic en [Video] > [Dispositivos de Video] > [Video en Tiempo Real], en el lado izquierdo se encuentra la lista de dispositivos y canales. De clic en un canal para ver el video en la pantalla.

Vuelva a dar clic en el canal para detener el video.

✍Notas:

1) Un dispositivo de video puede permitir a cinco usuarios ver el video simultáneamente. Cuando se excede el número de usuarios simultáneos no se mostrará el video y la imagen será gris.

2) Si no existen controladores de video en el sistema, se mostrará el siguiente mensaje:



De clic en "Descargar el control OCX" y se descargarán los controladores. Instale los controladores y refresque la página para ver la pantalla de monitoreo normalmente. Para prevenir la visualización de video de manera anormal, instale los controladores que ofrece ZKBioSecurity.

9.4 Eventos de Video

Muestra los eventos de video o captura de imagen.

De clic en [Video] > [Dispositivos de Video] > [Eventos de Video]:

Tiempo Inicial	Tiempo Final	Nombre de Área	Dispositivo	Nombre del Canal	Archivo de Media	Estado
2015-06-12 11:22:33	2015-06-12 11:22:33	Nombre de Área	192.168.1.1066	192.168.1.106-6		Captura exitosa.
2015-06-12 11:22:33	2015-06-12 11:22:33	Nombre de Área	192.168.1.1066	192.168.1.106-2		Captura exitosa.
2015-06-12 11:22:32	2015-06-12 11:23:02	Nombre de Área	192.168.1.1066	192.168.1.106-6		Video exitoso.
2015-06-12 11:22:32	2015-06-12 11:23:02	Nombre de Área	192.168.1.1066	192.168.1.106-2		Video exitoso.
2015-06-12 11:19:08	2015-06-12 11:19:08	Nombre de Área	192.168.1.1066	192.168.1.106-6		Captura exitosa.
2015-06-12 11:19:08	2015-06-12 11:19:08	Nombre de Área	192.168.1.1066	192.168.1.106-2		Captura exitosa.
2015-06-12 11:19:07	2015-06-12 11:19:37	Nombre de Área	192.168.1.1066	192.168.1.106-6		Video exitoso.
2015-06-12 11:19:07	2015-06-12 11:19:37	Nombre de Área	192.168.1.1066	192.168.1.106-2		Video exitoso.

Los archivos se muestran de la siguiente manera:

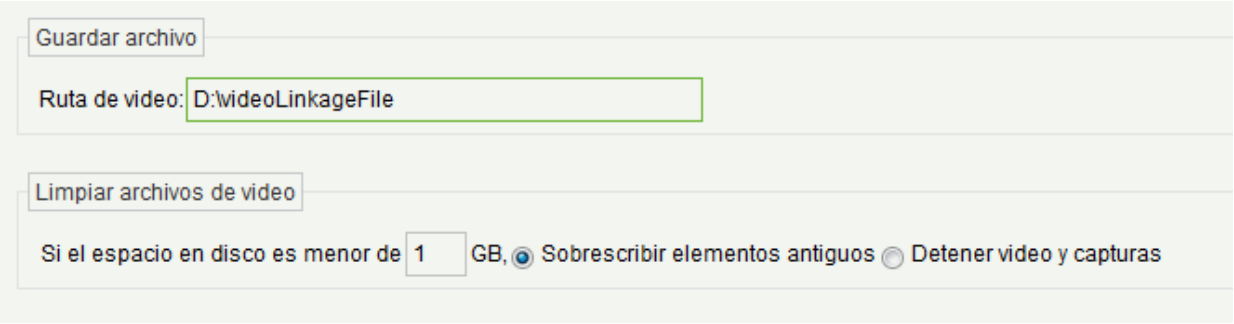
: Indica que el tipo de archivo es video. De clic para descargarlo. Utilice un reproductor de video de terceros para reproducir el video.

: Indica que el tipo de archivo es captura. Puede dar clic para ver el archivo.

Nota: Si se seleccionan "Video" y "Captura" como vínculos de un evento, existirán 2 registros. Para más detalles acerca de cómo establecer el vínculo, consulte 4.3.2 Vínculos.

9.5 Parámetros

De clic en [Video] > [Dispositivos de Video] > [Parámetros]:



Ruta de Video: Ruta para almacenar los archivos cuando el servidor grabe videos o capture imágenes.

Limpiar Archivos de Video: Cuando el espacio en el disco para almacenar archivos de video es menor que el valor definido, puede seleccionar sobrescribir los videos antiguos o detener la grabación y captura de imágenes. Si selecciona sobrescribir, el software sobrescribirá los videos más antiguos y continuará grabando video. Si selecciona detener, el software dejará de grabar video y capturar imágenes.

9.6 Solución de Excepciones

1. El navegador cliente no puede reproducir video, pre-visualizar, o el monitoreo en tiempo real no muestra pop-up de video:

Asegure de usar el navegador IE11 o superior, que la PC cliente y el dispositivo de video estén en el mismo segmento de red y que se haya instalado el driver o ActiveX correctamente. Si la instalación del ActiveX falla, desinstale el ActiveX de video que fue instalado originalmente, ejecute el comando "regsvr32-u NetVideoActiveX23.ocx", y después, en el navegador, configure las opciones en Herramientas > Opciones de Internet > Seguridad > Nivel Personalizado y en los controladores seleccione "Habilitado o Preguntar", abra el navegador, inicie sesión y abra la página de video en tiempo real y seleccione "agregar todos los objetos del sitio".

2. La red o la fuente de alimentación es apagada mientras se realiza el monitoreo en tiempo real.

Revise que la red o la alimentación estén conectados correctamente. Refresque o vuelva a abrir la página de monitoreo de video en tiempo real después de asegurar que la conexión es normal.

3. En el mapa virtual, no se muestra el pop-up de video después de dar clic en el ícono de la cámara:

Asegure de usar el navegador IE11 o superior, que la PC cliente y el dispositivo de video estén en el mismo

segmento de red y que se haya instalado el driver o ActiveX correctamente. También revise que el navegador u otro software estén previniendo las ventanas emergentes pop-up. Si es así permita las ventanas pop-up para el sitio.

4. Al ocurrir un vínculo de video, no hay archivo de video o el archivo de video descargado es de 0kb:

Primero, asegure que el software tenga configurada la función Time Server (mantenga la función activada en Windows y que la función NTP esté activada en el dispositivo de video), es recomendado configurar el intervalo de video menor para asegurar la sincronización precisa entre el software, el dispositivo de video y el servidor de tiempo, además mantenga el tiempo consistente entre el software y los controladores. Es recomendado configurar la grabación del vínculo de más de 5 segundos, para evitar el retardo en ejecutar el comando del vínculo, que puede originar que el archivo descargado sea de 0kb.

5. El módulo de video no opera normalmente en Windows Server 2008:

Es necesario instalar Desktop Experience en Windows Server 2008 antes de usar el módulo de video.

Paso 1: Ejecute "services.msc" para abrir el administrador de servicios.

Paso 2: Seleccione el inicio automático para "Windows Audio" y "Themes".

Paso 3: Ejecute el administrador de servicios y de clic en [Agregar Funciones], marque la casilla de "Desktop Experience" y de clic en [Instalar]. Reinicie el servidor después de realizar la instalación.

6. El video descargado al disco local no puede ser reproducido:

Seleccione un reproductor de video de terceros para reproducir el video, de lo contrario no podrá ser reproducido normalmente.

7. Cuando el navegador es Chrome v4.2 o superior, el sistema mostrará un mensaje para instalar los controlad ores, aunque ya hayan sido instalados.

Los controladores NPAPI antiguos están deshabilitados en Chrome v4.2 o superior. Debe abrir el navegador e ingresar "chrome://flags/#enable-npapi"en la barra de dirección para habilitar los controles.

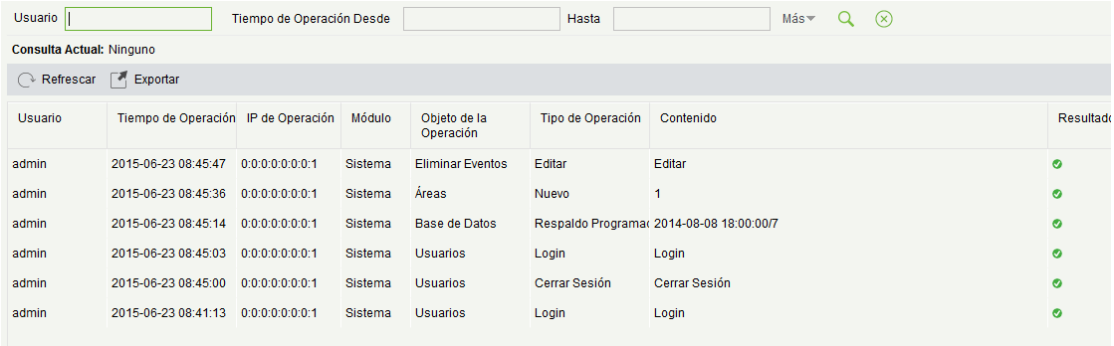
10 Gestión de Sistema

Los ajustes del sistema incluyen la gestión de usuarios del sistema y sus privilegios, gestión de la base de datos, gestión de Áreas, parámetros del sistema, configuración de correo electrónico, bitácora de eventos entre otros.

10.1 Gestión Básica

10.1.1 Bitácora de Eventos

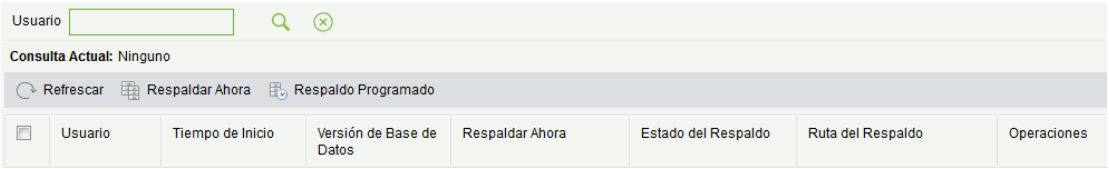
De clic en [Sistema] > [Gestión Básica] > [Bitácora de Eventos]:



Los registros de operación del sistema se muestran en esta interfaz. Puede filtrar los datos.

10.1.2 Base de Datos

De clic en [Sistema] > [Gestión Básica] > [Base de Datos]:



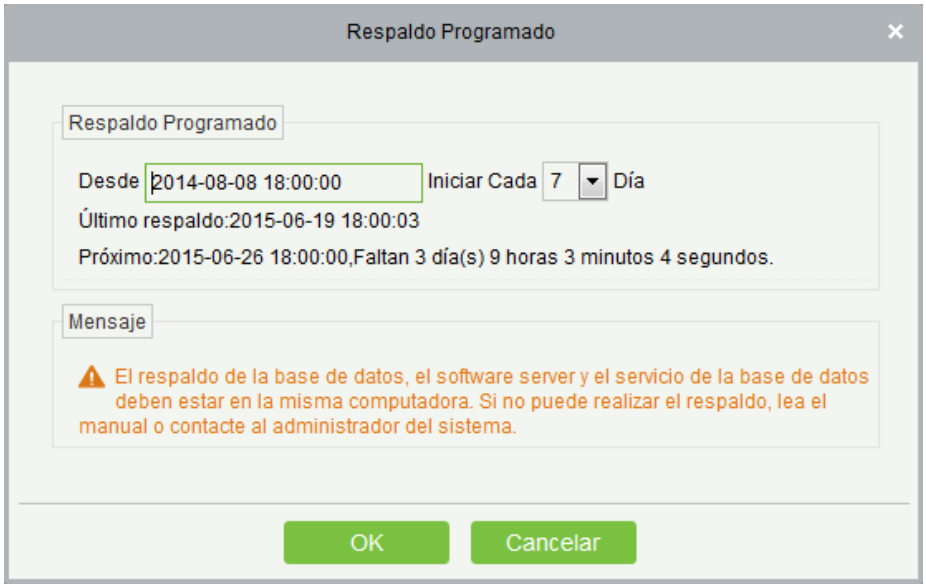
Se muestran los registros de operación de los respaldos de la base de datos. Es posible respaldar ahora, programar un respaldo automático o borrar según sea necesario.

- Respaldar Ahora

Respalda inmediatamente la base de datos en la ruta especificada.

- Respaldo Programado

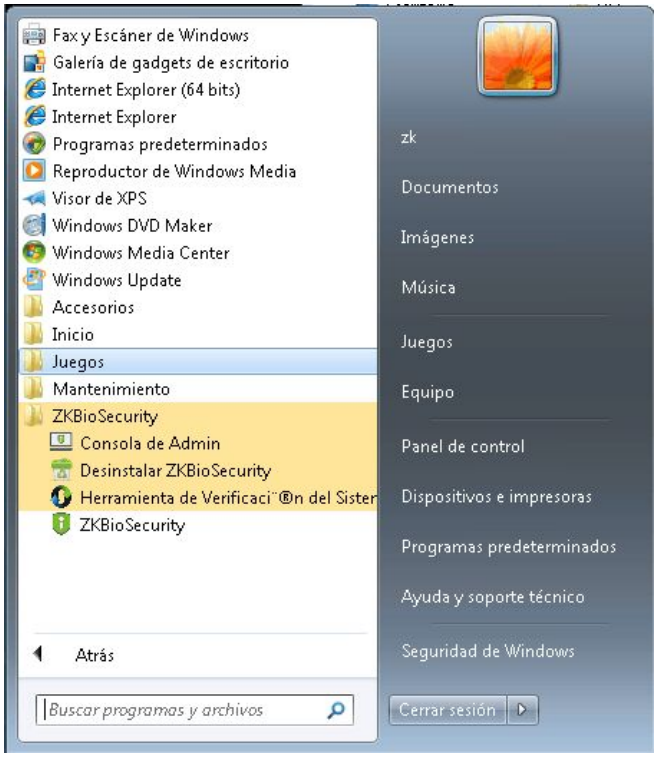
De clic en [Respaldo Programado]:

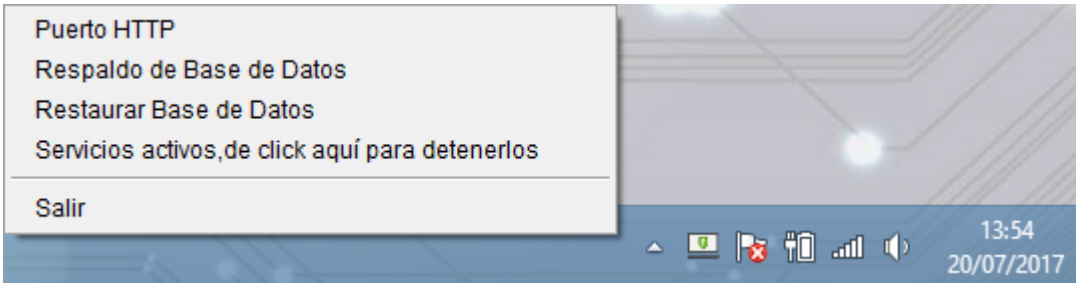


Introduzca el tiempo de inicio y el intervalo entre dos respaldos programados, luego de clic en [OK].

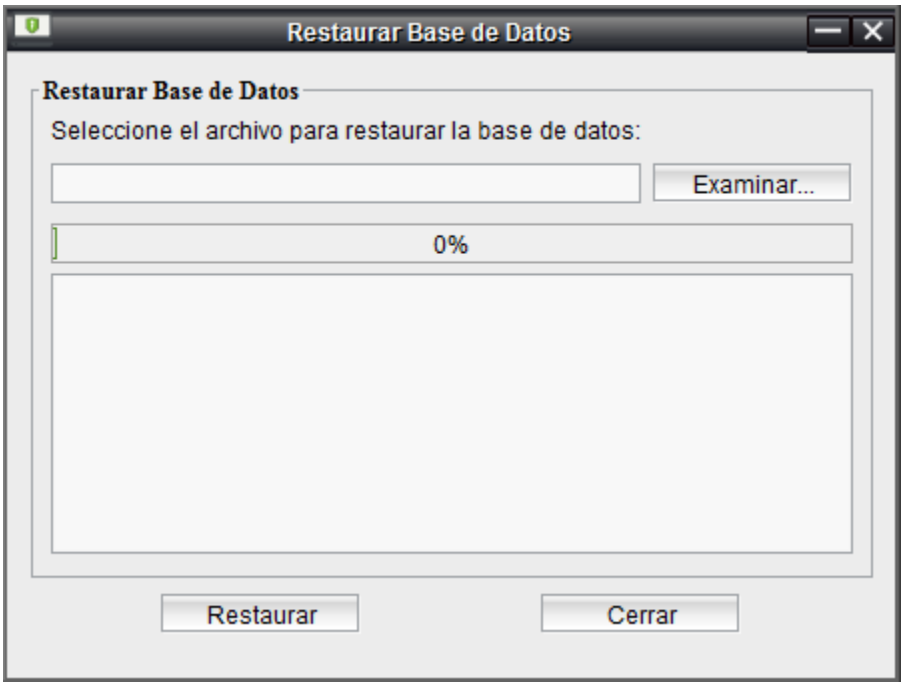
- Restaurar base de datos

1. De clic en el botón de inicio de Windows →[Todos los Programas]→[ZKBioSecurity]→ y ejecute la "Consola de Admin". Encontrará el ícono de "Consola de Admin" en la barra de tareas como se muestra a continuación, de clic derecho en el ícono y luego clic izquierdo en Restaurar "Base de Datos".





2. En la ventana emergente, de clic en "Examinar" para seleccionar archivo de respaldo para restaurar la base de datos.



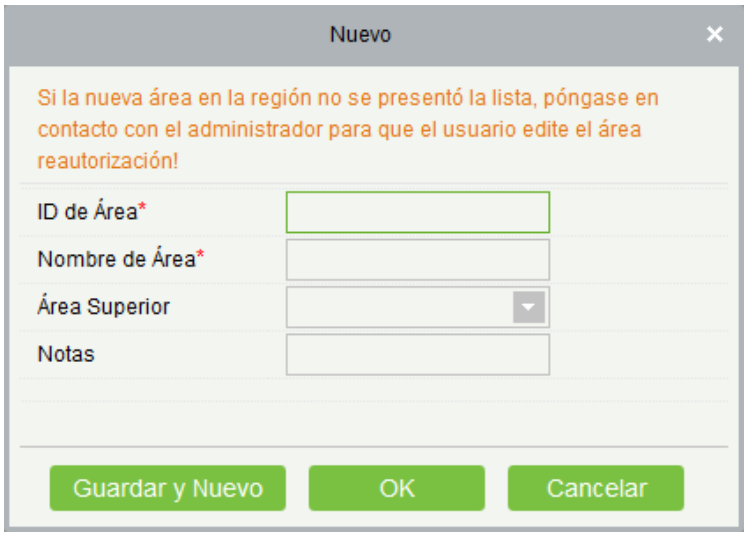
10.1.3 Áreas

Las áreas sirven para agrupar los dispositivos. Después de definir las áreas, es posible filtrar los dispositivos por área en la interfaz de monitoreo en tiempo real.

El sistema tiene por defecto un área llamada "Nombre de Área" con el número 1. Puede editar el nombre.

- Agregar un Área

De clic en [Sistema] > [Gestión Básica] > [Áreas] > [Nuevo]:



Descripción de los campos:

ID de Área: Número de Área. Debe ser único.

Nombre de Área: Cualquier caracter. Máximo 30 caracteres.

Área Superior: Determina la estructura del sistema.

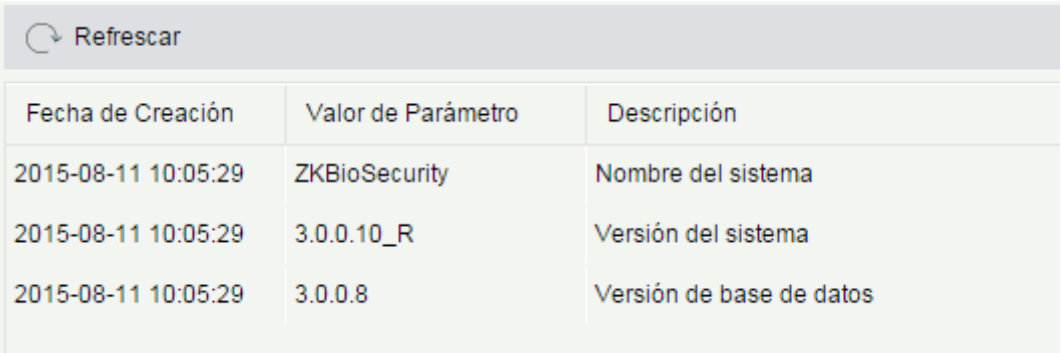
De clic en [OK] para guardar.

- Editar/Borrar un Área

De clic en [Editar] o [Borrar] como sea necesario.

10.1.4 Parámetros del Sistema

De clic en [Sistema] > [Parámetros del Sistema]:



Fecha de Creación	Valor de Parámetro	Descripción
2015-08-11 10:05:29	ZKBioSecurity	Nombre del sistema
2015-08-11 10:05:29	3.0.0.10_R	Versión del sistema
2015-08-11 10:05:29	3.0.0.8	Versión de base de datos

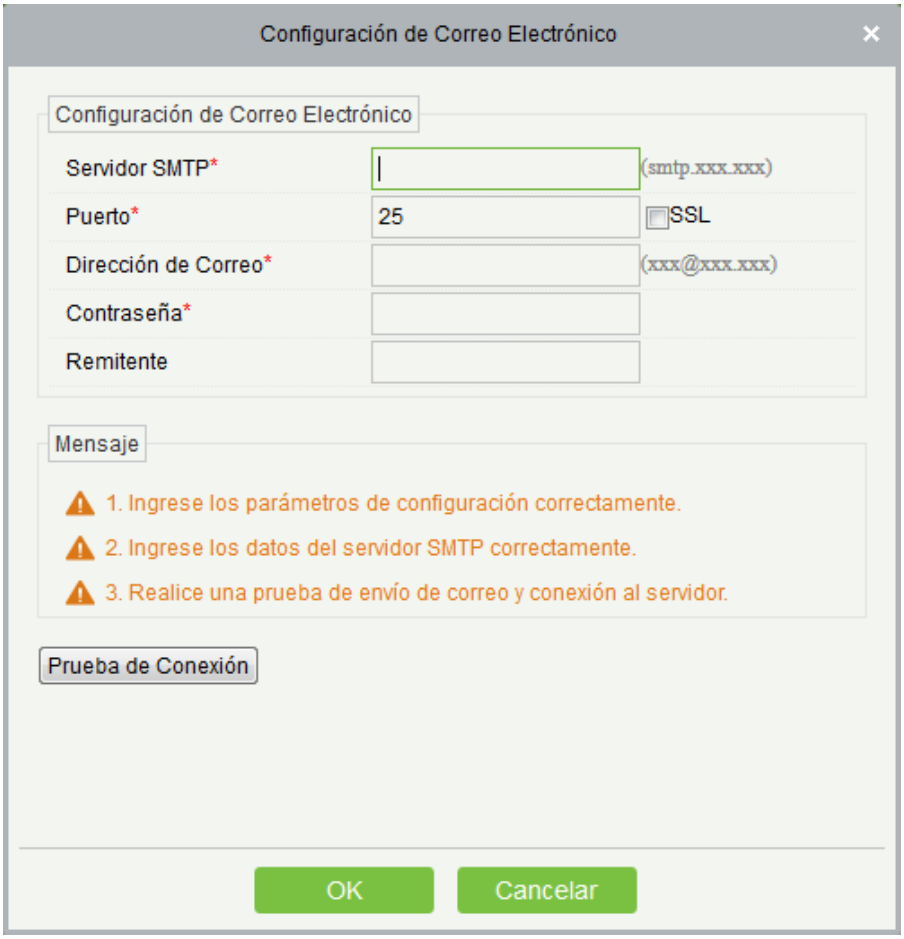
De clic en [Editar] para modificar el nombre del sistema.

10.1.5 Correo Electrónico

Configura el correo electrónico del servidor para el envío de información. Los correos de los destinatarios se

configuran en Vínculos.

De clic en [Gestión Básica] > [Correo Electrónico] > [Configuración de Correo Electrónico]:

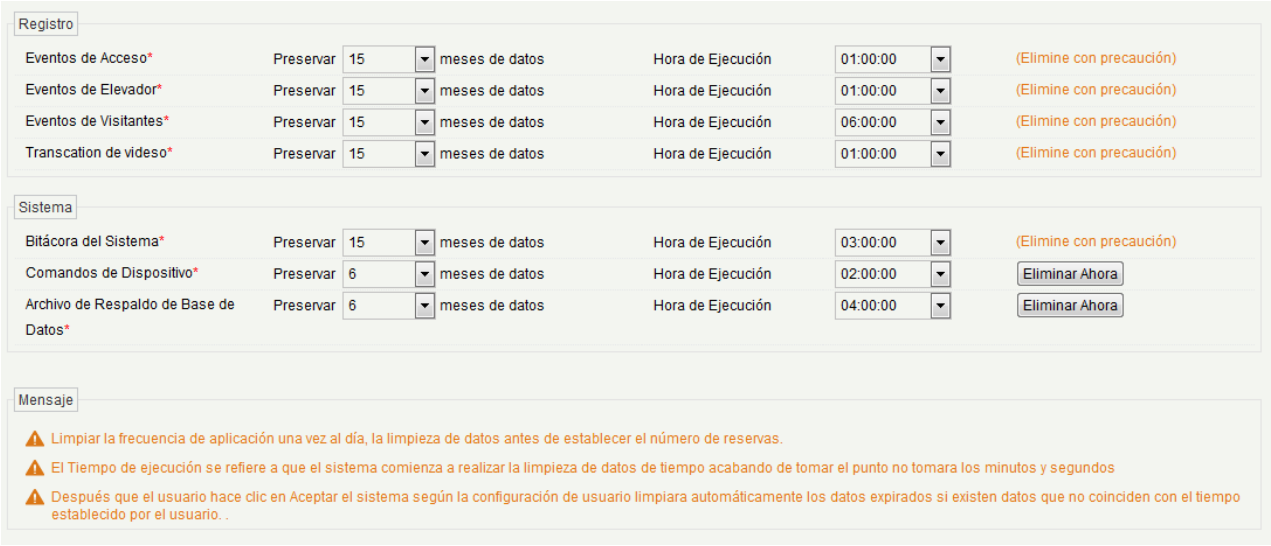


✍Nota: El nombre de dominio del correo electrónico y el servidor SMTP debe ser el mismo. Por ejemplo, si el correo electrónico es: test@gmail.com, el servidor SMTP debe ser: smtp.gmail.com.

10.1.6 Eliminar Eventos

La configuración de limpieza de datos se puede establecer. El volumen de datos aumentará conforme el uso del sistema. Para ahorrar espacio de almacenamiento en los discos es necesario limpiar periódicamente los datos antiguos generados por el sistema.

De clic en [Gestión Básica] > [Eliminar Eventos]:

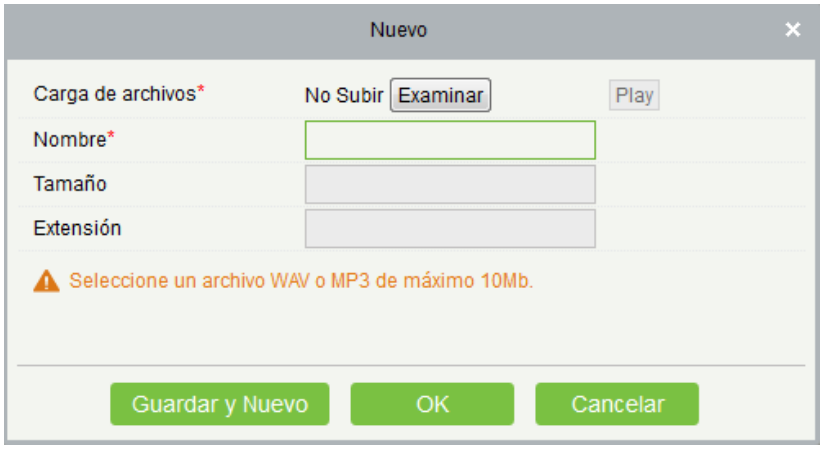


El sistema ejecuta la operación de limpieza después de dar clic en [OK]. Si no da clic en [OK], el sistema no realizará la limpieza de datos.

✍Nota: Para reducir la carga del sistema y no afectar el rendimiento normal, se sugiere establecer la hora de limpieza de datos a la 01:00 am.

10.1.7 Archivos de Audio

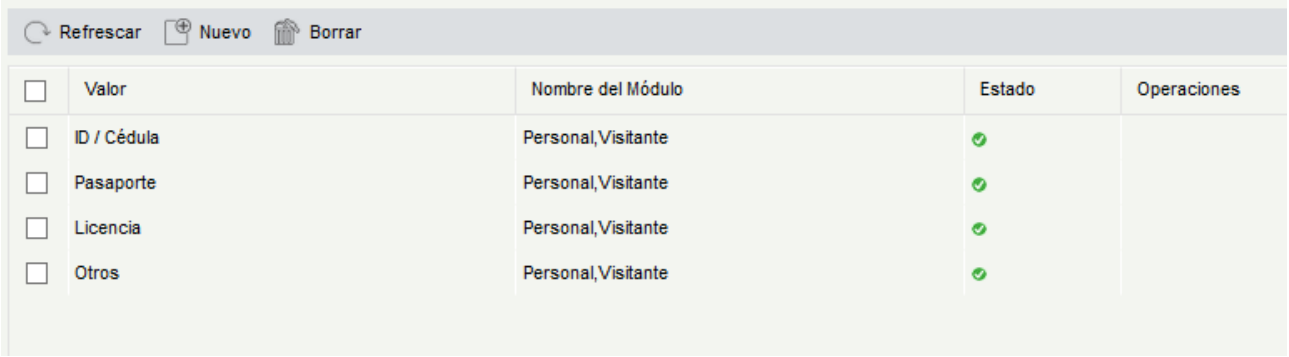
De clic en [Gestión Básica] > [Archivos de Audio] > [Nuevo]:



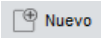
Es posible subir un archivo de audio del disco local. El archivo debe ser formato wav o mp3 y no exceder de 10Mb.

10.1.8 Tipos de Documento

Los tipos de documento están disponibles para el registro en el Sistema. Es posible agregar, eliminar y deshabilitar los tipos de documento/identificación como se muestra a continuación:



- Agregar

De clic en 

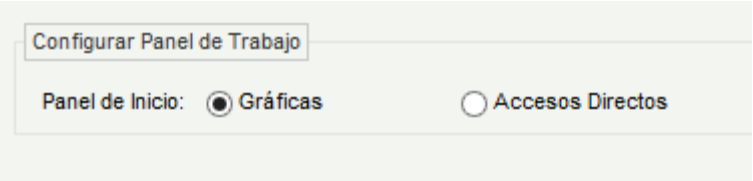
para introducir el nombre del documento y de clic en [OK] para guardar.

- Eliminar/Habilitar/Deshabilitar

Seleccione el Tipo de Documento y de clic en [Borrar]/ [Habilitar]/ [Deshabilitar], para realizar la acción requerida. "√" significa habilitar el documento y "—" significa deshabilitarlo.

10.1.9 Parámetros

Configure los parámetros relacionados con el Sistema como se muestra a continuación:



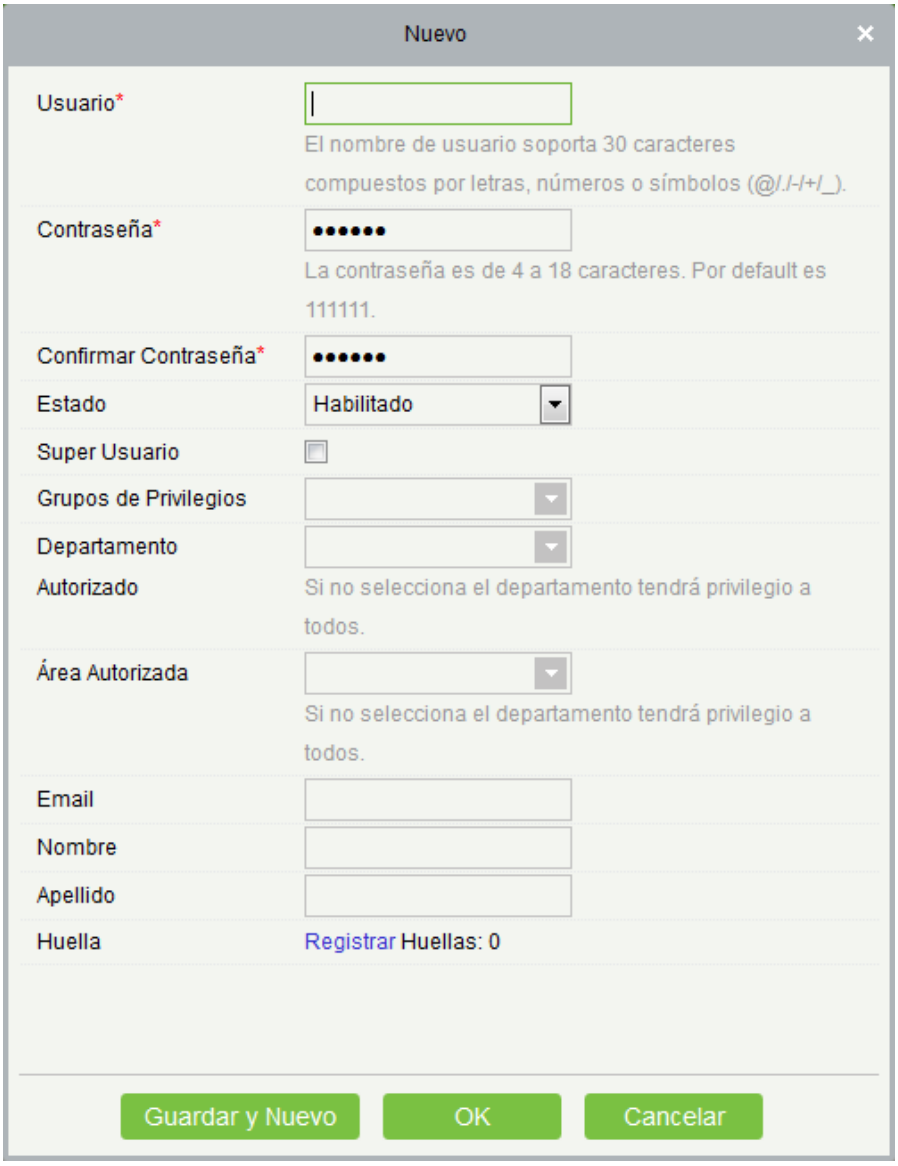
Configurar Panel de Trabajo: Puede seleccionar el Panel de Gráficas o Accesos Directos como la interfaz de inicio del Sistema.

10.2 Privilegios

10.2.1 Usuarios

Agregue nuevos usuarios y asigne niveles para los usuarios del sistema.

1. De clic en [Sistema] > [Privilegios] > [Usuarios] > [Nuevo]:



Descripción de los campos:

Usuario: Cualquier caracter hasta máximo 30.

Contraseña: La longitud debe ser entre 4 y 18 dígitos. La contraseña defecto es 111111.

Estado: Habilita o Deshabilita el usuario en el sistema.

Súper Usuario: Habilita o Deshabilita al usuario para tener los niveles de súper usuario.

Grupo de Privilegios: Los usuarios que no son Súper Usuario requieren un grupo de privilegios para obtener los privilegios del grupo. El grupo debe ser establecido en Grupo de Privilegios.

Departamento Autorizado: Si no selecciona alguno, indica que el usuario posee todos los privilegios de departamentos por defecto.

Área Autorizada: Si no selecciona alaguna, significa que el usuario posee todos los privilegios de áreas por defecto.

Huella: Registra la huella digital o huella de coacción. El usuario puede iniciar sesión en el sistema pulsando la huella registrada. Si el usuario pulsa la huella de coacción, recibirá la alarma y enviará la señal de alerta al sistema.

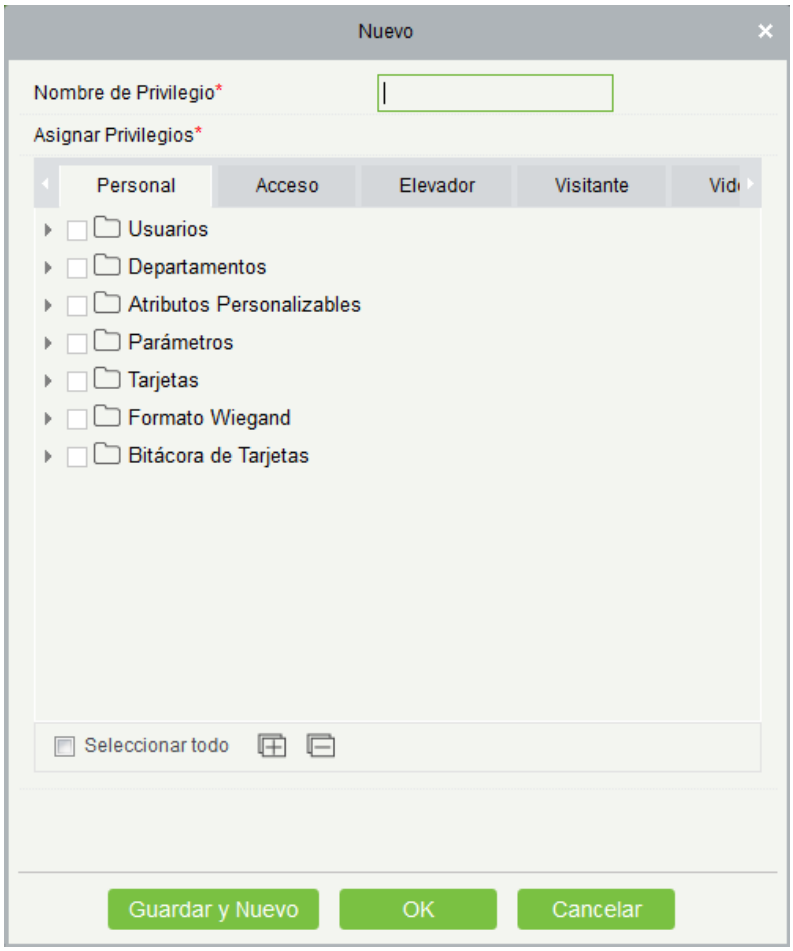
2. Después de edita, de clic en [OK] para agregar el usuario y se mostrará en la lista.

De clic en [Editar] o [Borrar] como sea necesario.

10.2.2 Privilegios

Al usar el sistema, el súper usuario o administrador necesita asignar diferentes niveles a los usuarios nuevos. Para evitar configurar los usuarios uno por uno, puede configurar los privilegios con niveles específicos en la gestión de privilegios y asignarlos al agregar usuarios. Un súper usuario tiene todos los niveles o privilegios, puede asignar privilegios a nuevos usuarios y establecerlos según sea necesario.

1. De clic en [Sistema] > [Privilegios] > [Privilegios] > [Nuevo]:



2. Introduzca el nombre y asigne los permisos para el privilegio.

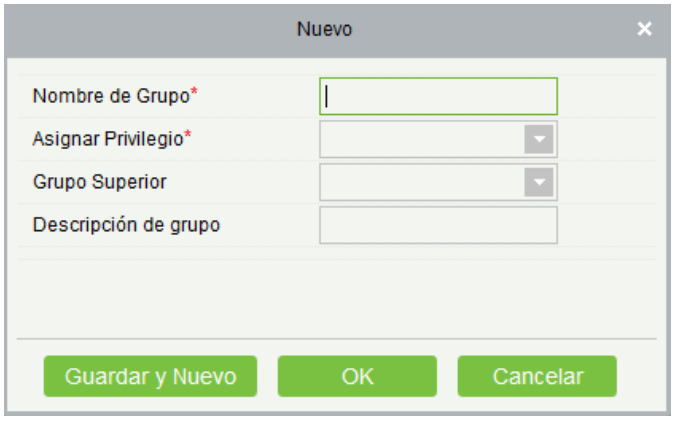
3. De clic en [OK] para guardar.

10.2.3 Grupo de Privilegios

Puede agregar grupos de privilegios al sistema. Un grupo de privilegios tiene todos los niveles asignados en los privilegios del grupo. Un grupo válido puede ser asignado directamente al agregar un usuario nuevo. Incluye todos los niveles para usar los módulos del sistema. EL súper usuario defecto tiene todos los niveles o privilegios, puede

asignar privilegios a nuevos usuarios y establecerlos según sea necesario.

1. De clic en [Sistema] > [Privilegios] > [Grupos de Privilegios] > [Nuevo]:

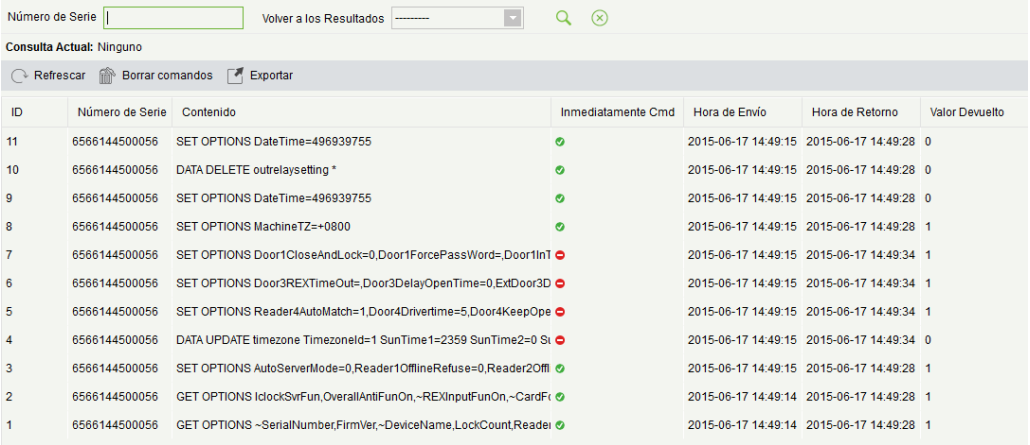


2. Introduzca el nombre, asigne los privilegios y seleccione el grupo superior.

3. De clic en [OK] para guardar.

10.3 Comunicación

De clic en [Sistema] > [Comunicación] > [Comando de Dispositivos], se mostrará la lista de comandos.



ID	Número de Serie	Contenido	Inmediatamente Cmd	Hora de Envío	Hora de Retorno	Valor Devuelto
11	6566144500056	SET OPTIONS DateTime=496939755	✓	2015-06-17 14:49:15	2015-06-17 14:49:28	0
10	6566144500056	DATA DELETE outrelaysetting *	✓	2015-06-17 14:49:15	2015-06-17 14:49:28	0
9	6566144500056	SET OPTIONS DateTime=496939755	✓	2015-06-17 14:49:15	2015-06-17 14:49:28	0
8	6566144500056	SET OPTIONS MachineTZ=+0800	✓	2015-06-17 14:49:15	2015-06-17 14:49:28	1
7	6566144500056	SET OPTIONS Door1CloseAndLock=0,Door1ForcePassWord=,Door1InT	⊖	2015-06-17 14:49:15	2015-06-17 14:49:34	1
6	6566144500056	SET OPTIONS Door3REXTimeOut=,Door3DelayOpenTime=0,ExtDoor3D	⊖	2015-06-17 14:49:15	2015-06-17 14:49:34	1
5	6566144500056	SET OPTIONS Reader4AutoMatch=1,Door4Drivertime=5,Door4KeepOpe	⊖	2015-06-17 14:49:15	2015-06-17 14:49:34	1
4	6566144500056	DATA UPDATE timezone TimezoneId=1 SunTime1=2359 SunTime2=0 St	⊖	2015-06-17 14:49:15	2015-06-17 14:49:34	0
3	6566144500056	SET OPTIONS AutoServerMode=0,Reader1OfflineRefuse=0,Reader2Offl	✓	2015-06-17 14:49:15	2015-06-17 14:49:28	1
2	6566144500056	GET OPTIONS IclockSvrFun,OverallAntiFunOn,~REXInputFunOn,~CardF	✓	2015-06-17 14:49:14	2015-06-17 14:49:28	1
1	6566144500056	GET OPTIONS ~SerialNumber,FirmVer,~DeviceName,LockCount,Reader	✓	2015-06-17 14:49:14	2015-06-17 14:49:28	1

Si el valor regresado es mayor o igual a 0, el comando fue emitido exitosamente. Si el comando regresado es menor de 0, el comando no pudo ser emitido.

Borrar Comandos: Limpia la lista de comandos.

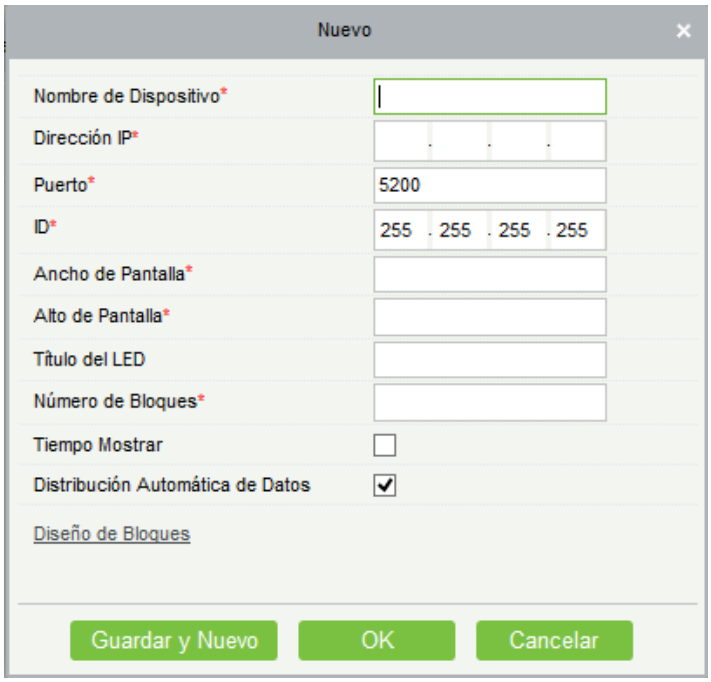
Exportar: Exporta la lista de comandos.

10.4 Gestión Extendida

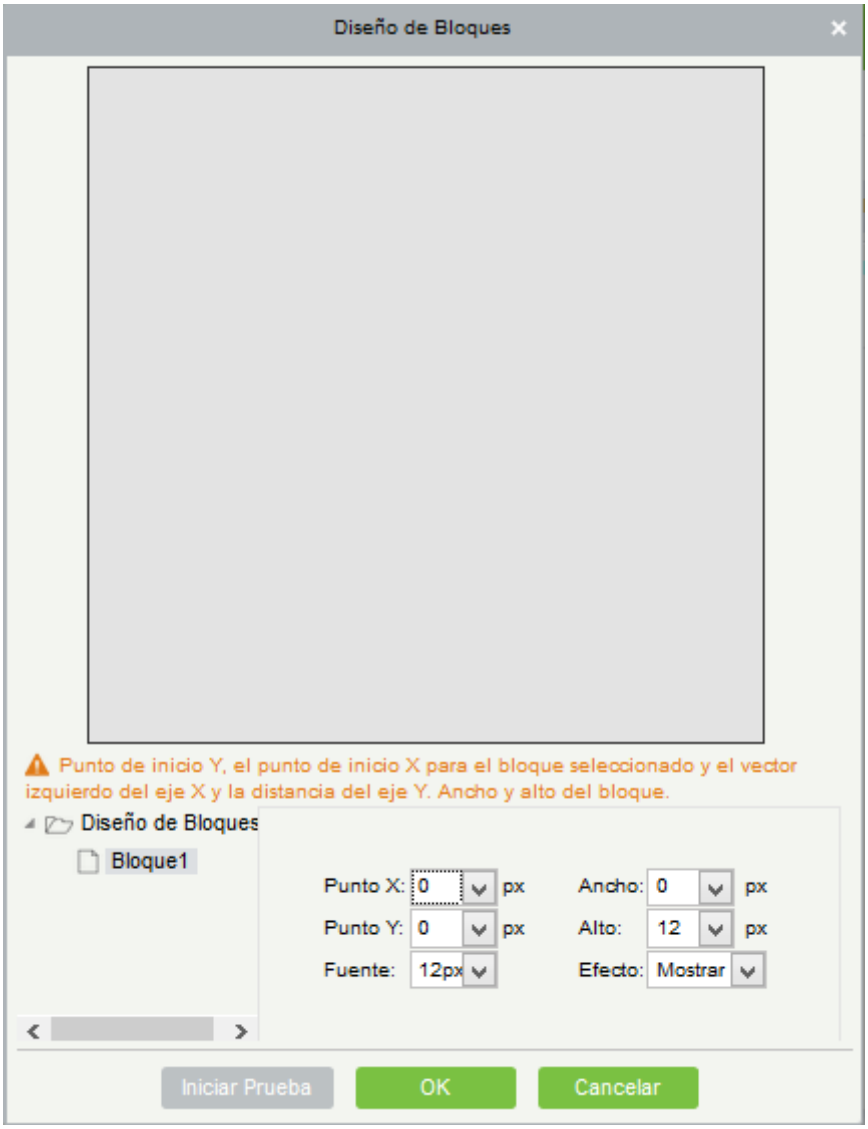
10.4.1 Dispositivos LED

- Agregar

De clic en [Sistema]> [Gestión Extendida]> [Dispositivos LED]> [Nuevo]. La página se muestra a continuación:



Nombre de Dispositivo: Nombre del dispositivo LED.
Dirección IP: Dirección IP del dispositivo LED.
Puerto: El puerto por defecto es el 5200.
Código de Acceso: El valor por defecto es 255.255.255.255.
Ancho de Pantalla: Ancho de la matriz de puntos (resolución).
Alto de Pantalla: Alto de la matriz de puntos (resolución).
Título de LED: Seleccione si desea mostrar un título. Si el parámetro se deja vacío, no se muestra título. Número de Bloques: Número de bloques en el que el dispositivo LED está dividido (Tenga en cuenta que los bloques no contienen el título y los bloques del sistema).
Distribución Automática de Datos: Por defecto este parámetro está habilitado. Se envían los datos del módulo de control de acceso al dispositivo LED solo cuando este parámetro está habilitado, de lo contrario, el contenido debe ser definido manualmente.
Diseño de Bloques: Después de dar clic en Diseño de bloques se muestra la siguiente ventana:



✍Nota:

1. Los parámetros deben configurarse para cada bloque.
2. El alto de cada bloque debe ser igual o mayor de 12, de lo contrario, las letras no se mostrarán completamente.
3. El alto total de todos los bloques no pueden ser mayor que el alto de la pantalla.

- Modificar

De clic en el nombre del dispositivo o en [Modificar] debajo de [Operaciones] para ir a la página de edición. Después de editar el dispositivo de clic en [OK] para guardar los cambios.

- Borrar

De clic en el nombre del dispositivo o en [Borrar] debajo de [Operaciones] en la lista de dispositivos y de clic en [OK] para borrar el dispositivo o de clic en [Cancelar] para cancelar la operación. Seleccione uno o más dispositivos y de clic en [Borrar] arriba de la lista y de clic en [OK] para borrar el dispositivo(s)seleccionado(s) o de clic en [Cancelar] para cancelar la operación.

- Habilitar o Deshabilitar

Seleccione un dispositivo y de clic en [Habilitar/Deshabilitar] para iniciar o detener el uso del dispositivo. Si el dispositivo es habilitado, se transmitirán los datos al dispositivo, de lo contrario no se transmiten datos. Sincronizar Todos los Datos

Sincroniza el diseño del bloque LED y los ajustes de los datos del Sistema al dispositivo. Seleccione un dispositivo, de clic en [Sincronizar Todos los Datos] y de clic en [Sincronizar] para sincronizar los datos.

- Reiniciar

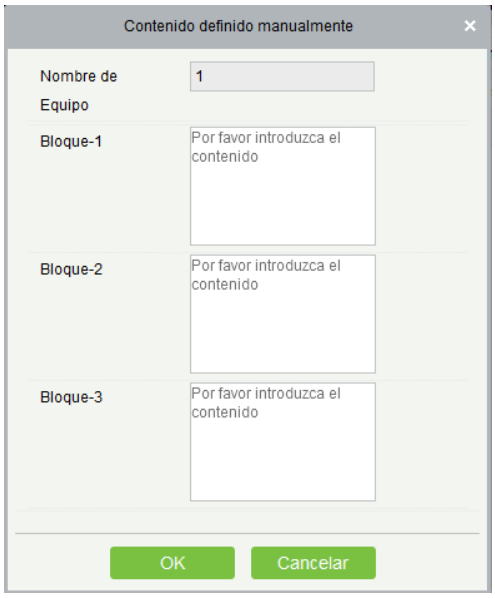
Después de reiniciar el dispositivo, la tarjeta de control LED será reiniciada, se limpiarán los datos en la pantalla y los datos guardados en el Sistema serán restaurados. Después de que el dispositivo reinicie exitosamente, de clic en [Sincronizar Todos los Datos] para mostrar todo el contenido distribuido en la pantalla LED.

- Modificar IP

Modifica la dirección IP del dispositivo. La IP por defecto de la tarjeta de control es 192.168.1.222.

- Contenido Definido Manualmente

Seleccione un dispositivo y de clic en [Contenido Definido Manualmente]. Se muestra la siguiente ventana:



✍Nota:

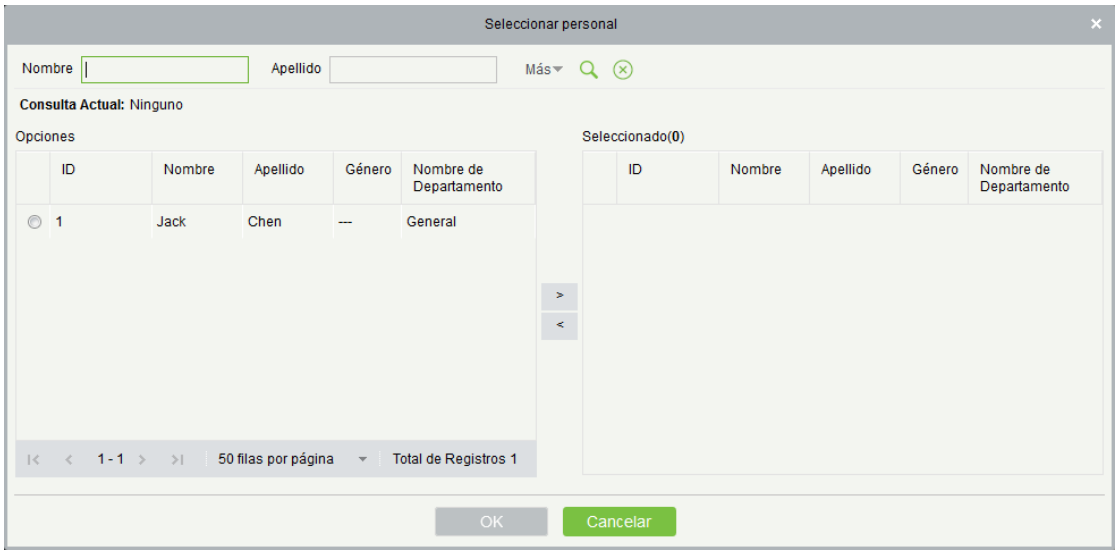
1. Al menos un bloque debe ser seleccionado para la distribución del contenido definido manualmente.
2. Después de seleccionar el contenido definido manualmente, el módulo de control de acceso no podrá enviar datos al dispositivo LED.

11 Anexos

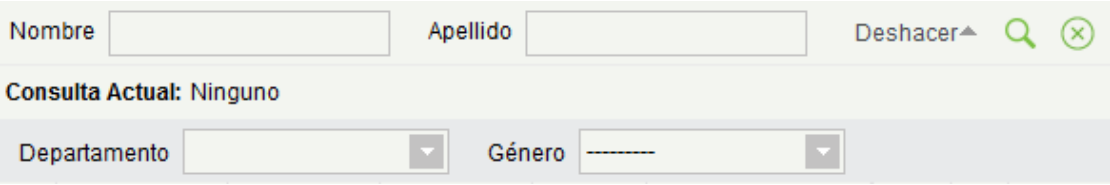
11.1 Operaciones Comunes

- Seleccionar Personal

La interfaz de selección de personal del sistema será siempre la siguiente:



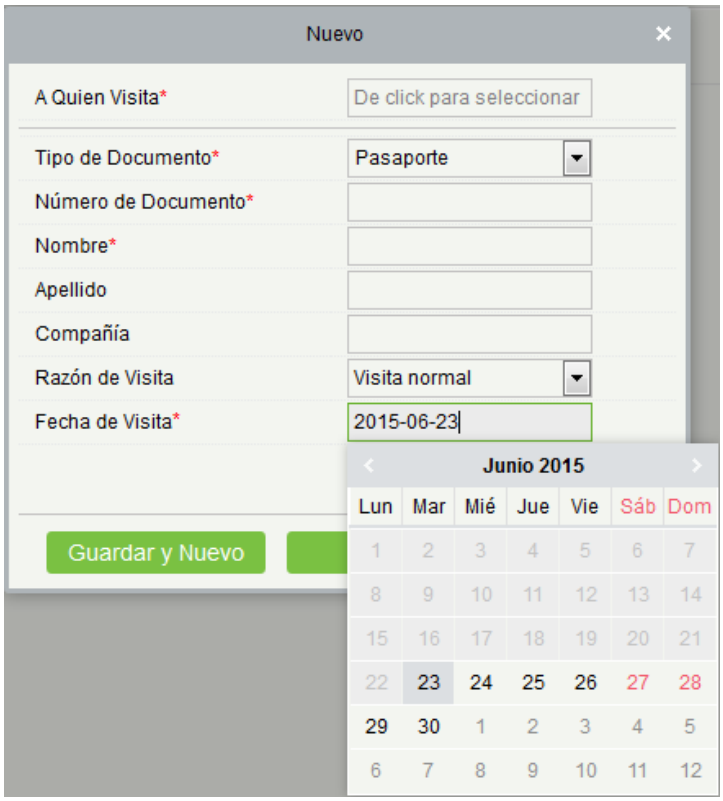
Puede seleccionar el personal en la lista alternativa o puede dar clic en [Mas] para filtrar por género o departamento.



De clic en > para mover el personal seleccionado a la lista de selección. Si desea cancelar el movimiento, de clic en <.

- Configurar Fecha y Hora

De clic en fecha y hora:

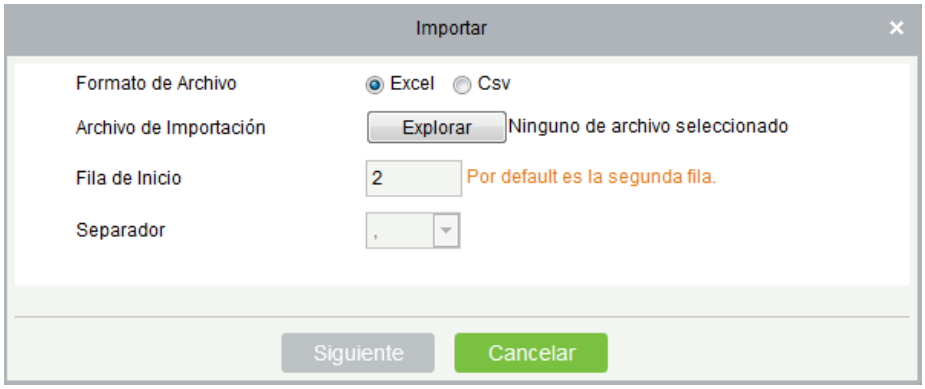


Para seleccionar el año, de clic en ◁ o ▷. Seleccione el mes y día correspondiente.

- Importar (tome la importación de la lista de personal como ejemplo).

Si tiene un archivo de personal en su ordenador, puede importarlo al sistema.

1. De clic en [Importar]:



Descripción de los campos:

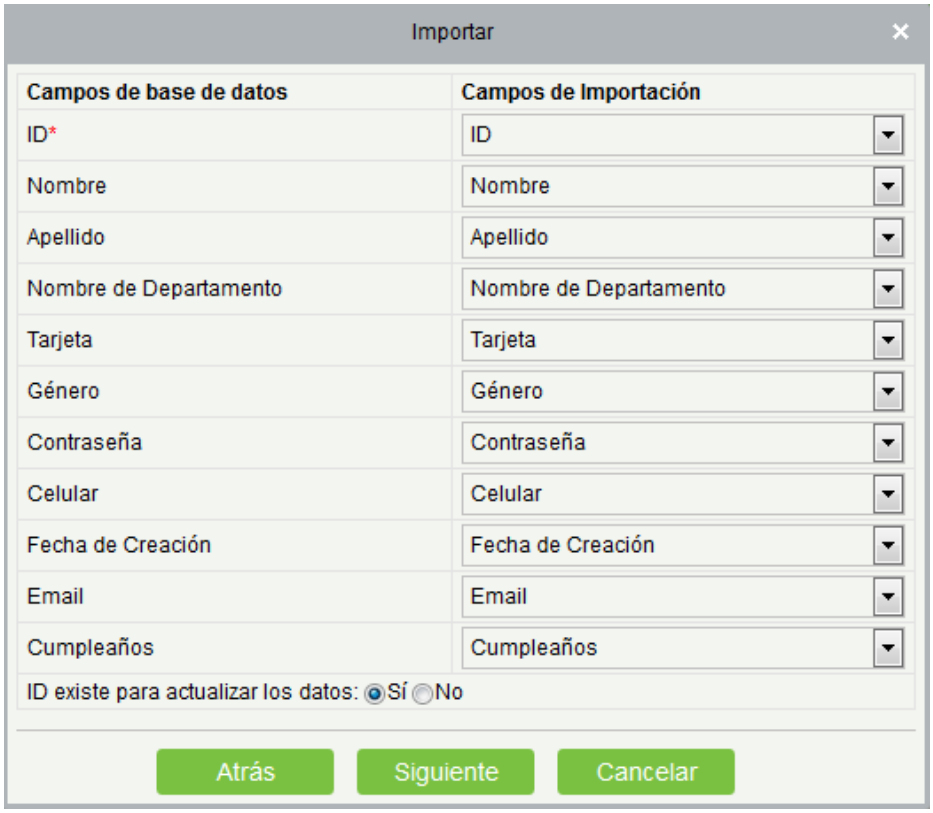
Formato del Archivo: Seleccione el formato del archivo para importar.

Archivo de Destino: Seleccione el archivo para importar.

Fila de Inicio: Indica cual es la primera fila que se importará.

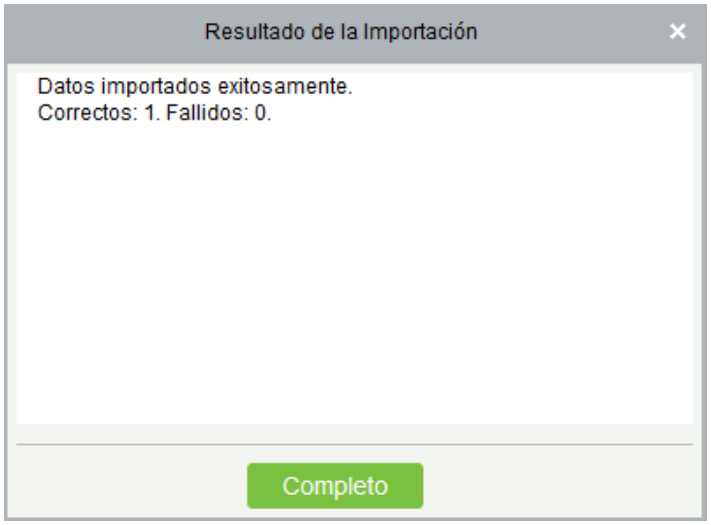
Separador: Indica el delimitador del archivo CSV. Solo "." y "-" están disponibles.

2. De clic en [Siguiente]:



3. Seleccione los campos para importar al sistema. "----------" indica que los campos no se importarán.

4. De clic en [Siguiente]:



Los datos han sido importados exitosamente.

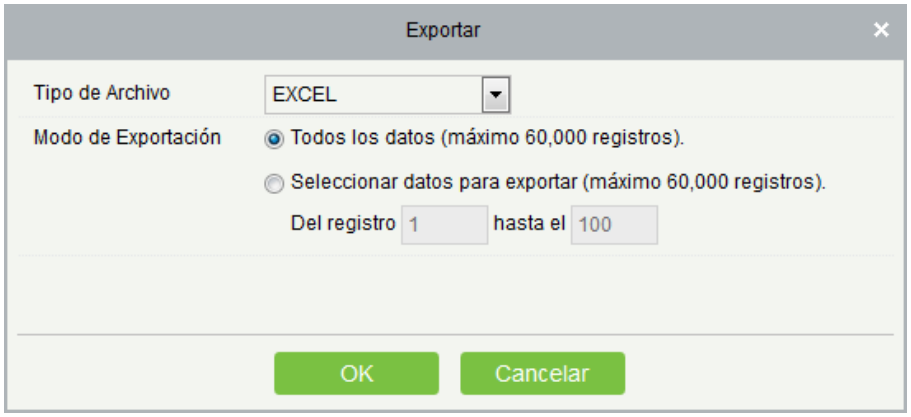
✍Nota:

1) Al importar la tabla de departamento, nombre de departamento y ID de departamento no pueden estar vacíos, solo el departamento superior puede estar vacío. ID duplicado no afecta la operación, puede ser modificado manualmente.

2) Al importar la tabla de personal, el ID de usuario es necesario. Si un ID de usuario ya existe en la base de datos, no será importado.

- Exportar (tome la exportación de la lista de personal como ejemplo)

1. De clic en [Exportar]:



2. Seleccione el formato de archivo y modo de exportación para exportar. De clic en [OK].

3. Puede ver el archivo en el disco local.

✍Nota: 10000 registros se pueden exportar por defecto, puede ingresar manualmente como sea necesario.

11.2 Tipo de Evento de Acceso

- Eventos Normales

Apertura con verificación normal: En modo de verificación [Solo Tarjeta], el usuario que tenga asignado un nivel de acceso válido que presente la tarjeta en el lector, podrá abrir la puerta durante el horario activo y se mostrará el evento normal.

Apertura normal con huella digital: En modo de verificación [Solo Huella] o [Tarjeta o Huella], el usuario que tenga asignado un nivel de acceso válido que presente la tarjeta o pulse la huella en el lector, podrá abrir la puerta durante el horario activo y se mostrará el evento normal.

Apertura con Tarjeta y Huella: En modo de verificación [Tarjeta y Huella], el usuario que tenga asignado un nivel de acceso válido que presente la tarjeta y pulse la huella en el lector, podrá abrir la puerta durante el horario activo y se mostrará el evento normal.

Apertura con Botón de Salida: Al presionar el botón de salida durante el horario activo, abrirá la puerta y se mostrará el evento normal.

Presionar el Botón de Salida (bloqueado): Indica el evento normal activado al presionar el botón de salida cuando éste se encuentra bloqueado.

Tarjeta Durante Horario de Apertura Programado: En un horario de apertura programado (normalmente abierto) ya sea por un horario normal de apertura, primera apertura, o por apertura remota normalmente abierto, un usuario con nivel de acceso válido que presente la tarjeta en el lector mostrará el evento.

Pulsar Huella Durante Horario de Apertura Programado: En un horario de apertura programado (normalmente abierto) ya sea por un horario normal de apertura, primera apertura, o por apertura remota normalmente abierto, un usuario que tiene nivel de acceso válido que pulse la huella en el lector mostrará el evento normal.

Primera Apertura Normalmente Abierto con Tarjeta: En modo de verificación [Solo Tarjeta], el usuario que tenga asignado el privilegio de primera apertura, que presente la tarjeta en el lector durante el horario válido, abrirá la puerta y se mostrará el evento normal.

Primera Apertura Normalmente Abierto con Huella: En modo de verificación [Solo Huella] o [Huella o Tarjeta], el usuario que tenga asignado el privilegio de primera apertura, que pulse la huella en el lector durante el horario válido, abrirá la puerta y se mostrará el evento normal.

Primera Apertura Normalmente Abierto con Huella y Tarjeta: En modo de verificación [Huella y Tarjeta], el usuario que tenga asignado el privilegio de primera apertura, que presente la tarjeta y pulse la huella en el lector durante el horario válido, abrirá la puerta y se mostrará el evento normal.

Fin de Horario de Apertura Programado: Al final del horario de apertura, la puerta se cerrará en automático.

Apertura Remota Normalmente Abierto: Se muestra el evento cuando se realiza la apertura remota de puerta con la opción normalmente abierto.

Detener Apertura Normalmente Abierto: Se muestra el evento cuando se presenta una tarjeta válida o se usa la opción de detener la apertura de forma remota.

Desactivar Horario de Apertura Programada: Se muestra el evento al presentar una tarjeta válida en el lector de la puerta cinco veces consecutivas (debe ser el mismo usuario) o al seleccionar [Desactivar Horario de Apertura

Programada] en operaciones remotas.

Activar Horario de Apertura Programada: Se muestra el evento si al desactivar el horario de apertura programada, se presenta una tarjeta válida en el lector de la puerta cinco veces consecutivas (debe ser el mismo usuario) o al seleccionar [Activar Horario de Apertura Programada] en operaciones remotas.

Apertura Multi-Usuario (con Tarjeta): En modo de verificación [Solo Tarjeta], se puede usar la combinación multi-usuario para abrir la puerta. Después de verificar la última tarjeta, se mostrará el evento normal.

Apertura Multi-Usuario (con Huella): En modo de verificación [Solo Huella] o [Huella o Tarjeta], se puede usar la combinación multi-usuario para abrir la puerta. Después de verificar la última huella, se mostrará el evento normal.

Apertura Multi-Usuario (con Huella y Tarjeta): En modo de verificación [Huella y Tarjeta], se puede usar la combinación multi-usuario para abrir la puerta. Después de verificar la última combinación de tarjeta y huella, se mostrará el evento normal.

Apertura con Contraseña de Emergencia: La contraseña de emergencia (también conocida como súper contraseña) establecida para la puerta puede ser usada para abrir la puerta. Este evento normal se mostrará después de verificarse la contraseña de emergencia.

Apertura durante Horario Normalmente Abierto: Si la puerta tiene configurada un horario de apertura normalmente abierto, la puerta se abrirá automáticamente y se mostrará el evento.

Vínculo Accionado: Se muestra después de que tome efecto la configuración de un vínculo.

Detener Alarma: Se muestra cuando el usuario detiene la alarma de la puerta respectiva exitosamente.

Apertura Remota: Se muestra cuando el usuario realiza la apertura remota de puerta exitosamente.

Cerrado Remoto: Se muestra cuando el usuario realiza el cerrado remoto de puerta exitosamente.

Apertura de Salida Auxiliar: Se muestra cuando toma efecto la configuración de un vínculo que se selecciona como acción abrir una salida auxiliar.

Cerrado de Salida Auxiliar: Se muestra cuando toma efecto la configuración de un vínculo que se selecciona como acción cerrar una salida auxiliar o cuando se cierra manualmente la salida en [Configuración de Puerta] > [Cerrar Salida Auxiliar].

Puerta Abierta Exitosamente: Se muestra cuando el sensor de la puerta detecta que la puerta ha sido abierta apropiadamente (después de una verificación correcta, apertura con botón, etc.).

Puerta Cerrada Exitosamente: Se muestra cuando el sensor de la puerta detecta que la puerta ha sido cerrada apropiadamente.

Entrada Auxiliar Desconectada: Se muestra al desconectarse una entrada auxiliar.

Entrada Auxiliar Conectada: Se muestra al conectarse o poner en corto una entrada auxiliar.

Dispositivo Inicializado: Se muestra cuando un dispositivo es inicializado (El evento no se muestra en el monitoreo en tiempo real, pero se puede ver en el reporte de eventos).

- Eventos Anormales

Intervalo Demasiado Corto: Cuando el intervalo entre la lectura de dos tarjetas es menor que el intervalo configurado, se mostrará el evento.

Intervalo Demasiado Corto de Huellas: Cuando el intervalo entre la lectura de dos huellas es menor que el intervalo configurado, se mostrará el evento.

Puerta en Horario Inactivo (Tarjeta): En modo de verificación [Solo Tarjeta], si un usuario con privilegio para abrir la puerta presenta la tarjeta en horario inactivo, se mostrará el evento anormal.

Puerta en Horario Inactivo (Huella): Si un usuario con privilegio para abrir la puerta pulsa la huella en el lector en horario inactivo, se mostrará el evento anormal.

Puerta en Horario Inactivo (Botón de Salida): Si se presiona el botón de salida para abrir la puerta en horario inactivo, se mostrará el evento anormal.

Fuera de Horario: Si un usuario con privilegio para abrir la puerta presenta la tarjeta durante un horario inválido, se muestra el evento anormal.

Acceso no Autorizado: Si un usuario presenta una tarjeta registrada en el lector, pero no cuenta con permiso para abrir esa puerta, se mostrará el evento anormal.

Anti-Passback: Se muestra el evento cuando la función anti-passback toma efecto.

Esclusamiento: Anti-Passback: Se muestra el evento cuando la función de esclusamiento toma efecto.

Verificación Multi-Usuario (Tarjeta): Se muestra el evento anormal cuando ocurre una verificación multi-usuario para abrir la puerta, al presentar la penúltima tarjeta (ya sea verificada o no).

Verificación Multi-Usuario (Huella): Se muestra el evento anormal cuando ocurre una verificación multi-usuario para abrir la puerta, al pulsar la penúltima huella (ya sea verificada o no).

Tarjeta No Registrada: Se muestra cuando en un lector se presenta una tarjeta no registrada en el sistema.

Huella No Registrada: Se muestra cuando en un lector se pulsa una huella que no ha sido registrada o la información de la huella no ha sido sincronizada con el sistema.

Apertura de Puerta Expirada: Si el sensor de puerta detecta que ha expirado el tiempo de apertura de tiempo permitido y no se ha cerrado la puerta, se mostrará el evento anormal.

Tarjeta Expirada: Se muestra el evento cuando un usuario con nivel de acceso asignado, presenta la tarjeta en el lector después del tiempo de vigencia establecido y no puede ser verificado.

Huella Expirada: Se muestra el evento cuando un usuario con nivel de acceso asignado, pulsa la huella en el lector después del tiempo de vigencia establecido y no puede ser verificado.

Error de Contraseña: Se muestra el evento cuando se usa el modo de verificación [Tarjeta y Contraseña], contraseña de coacción o contraseña de emergencia para abrir la puerta.

Fallo al Cerrar Puerta Durante Horario Normalmente Abierto: Se muestra el evento cuando la puerta se encuentra en estado normalmente abierto, pero el usuario no puede cerrarla con [Cerrado Remoto].

Error en Modo de Verificación: Se muestra el evento cuando el modo de apertura de la puerta es diferente al establecido para la puerta.

Verificación en Segundo Plano Fallido: Se muestra cuando falla la verificación de Zona en APB Global.

Verificación en Segundo Plano Exitosa: Se muestra cuando la verificación de Zona en APB Global es exitosa.

Verificación en Segundo Plano Expirada: Cuando el valor de la Zona de APB Global no es devuelta a tiempo se muestra el evento anormal.

Verificación Multi-Usuario Fallida: Se muestra cuando al realizar una verificación multi-usuario para abrir la puerta no resulta exitosa.

- Eventos de Alarma

Apertura con Contraseña de Coacción: Se acciona la alarma al usar y verificar correctamente la contraseña de coacción para abrir la puerta.

Apertura con Huella de Coacción: Se acciona la alarma al usar y verificar correctamente la huella de coacción para abrir la puerta.

Alarma de Apertura con Coacción: Se acciona la alarma al usar y verificar correctamente la contraseña o huella de coacción para abrir la puerta.

Puerta Abierta Accidentalmente: Excepto todos los eventos normales, si el sensor de puerta detecta que la puerta ha sido abierta, se accionará la alarma.

Apertura de Tiempo Expirada: Se acciona esta alarma cuando la puerta abierta no es cerrada en el tiempo establecido.

Alarma de Tamper: Se acciona esta alarma cuando un dispositivo AIO es saboteado y se activa el tamper.

Tarjeta Inválida: Se acciona esta alarma cuando se presenta una tarjeta inválida en un lector cinco veces consecutivas.

✍Nota: Es posible definir el nivel de cada evento, ya sea normal, anormal o alarma.

11.3 Tipos de Eventos de Elevador

- Eventos Normales

Apertura Normal: Se muestra el evento cuando un usuario con nivel de acceso de elevador válido realiza una verificación exitosa con tarjeta en modo de verificación [Solo Tarjeta] o [Huella o Tarjeta].

Verificación Durante Horario de Apertura Programado: Se muestra el evento después de que un usuario con privilegio para establecer el periodo normalmente abierto o se activa la función normalmente abierto remoto y un usuario con nivel de acceso de elevador válido realiza una verificación con tarjeta o huella exitosa.

Liberación Remota: Se muestra cuando un usuario realiza la liberación remota de un botón exitosamente.

Bloqueo Remoto: Se muestra cuando un usuario realiza el bloqueo remoto de un botón exitosamente.

Desactivar Horario de Apertura Programada: Se muestra el evento cuando un usuario realiza esta operación en la página de Liberación Remota de Botón cuando un piso se encuentra en estado normalmente abierto.

Activar Horario de Apertura Programada: Se muestra el evento si el usuario realiza esta operación en la página de Liberación Remota de Botón cuando no están desactivados los horarios normalmente abiertos.

Apertura con Huella: Se muestra el evento cuando un usuario con nivel de acceso de elevador válido realiza una verificación exitosa con huella en modo de verificación [Solo Huella] o [Huella o Tarjeta].

Pulsar Huella Durante Horario de Apertura Programado: Se muestra el evento después de que un usuario con privilegio para establecer el periodo normalmente abierto o se activa la función normalmente abierto remoto y un usuario con nivel de acceso de elevador válido realiza una verificación con huella exitosa.

Fin de Horario de Apertura Programado: Al final del horario, el botón se cerrará en automático.

Apertura Remota Normalmente Abierto: Se muestra el evento cuando se realiza la liberación remota del botón con la opción normalmente abierto.

Dispositivo Inicializado: Se muestra cuando un dispositivo es inicializado (El evento no se muestra en el monitoreo en tiempo real, pero se puede ver en el reporte de eventos).

Apertura con Contraseña: Se muestra el evento cuando un usuario con nivel de acceso de elevador válido realiza una verificación exitosa con contraseña.

Superusuario - Liberación de Botón: Se muestra el evento cuando un superusuario libera un botón exitosamente.

Liberación de Botones por Emergencia: Se muestra al liberar todos los botones para que los usuarios puedan seleccionar los pisos en caso de emergencia.

Superusuario - Liberación de Botón: Se muestra el evento cuando un superusuario bloquea remotamente un botón de forma exitosa.

Habilitar Botón de Control de Elevador: Reinicia la función de control de elevador.

Deshabilitar Botón de Control de Elevador: Deshabilita temporalmente la función de control de elevador.

Entrada Auxiliar Desconectada: Se muestra al desconectarse una entrada auxiliar.

Entrada Auxiliar Conectada: Se muestra al conectarse o poner en corto una entrada auxiliar.

- Eventos Anormales

Intervalo Demasiado Corto: Cuando el intervalo entre la lectura de dos tarjetas es menor que el intervalo configurado para el piso, se mostrará el evento.

Intervalo Demasiado Corto de Huellas: Cuando el intervalo entre la lectura de dos huellas es menor que el intervalo configurado para el piso, se mostrará el evento.

Puerta en Horario Inactivo (Tarjeta): En modo de verificación [Solo Tarjeta], si un usuario con privilegio para acceder al piso presenta la tarjeta en horario inactivo, se mostrará el evento anormal.

Fuera de Horario: Si un usuario con privilegio para acceder al piso presenta la tarjeta durante un horario inválido, se muestra el evento anormal.

Acceso Denegado: Si un usuario presenta una tarjeta registrada en el lector, pero no cuenta con permiso para acceder al piso, se mostrará el evento anormal.

Tarjeta No Registrada: Se muestra cuando en un lector se presenta una tarjeta no registrada en el sistema.

Tarjeta Expirada: Se muestra el evento cuando un usuario con nivel de acceso asignado, presenta la tarjeta en el lector después del tiempo de vigencia establecido y no puede ser verificado.

Huella Expirada: Se muestra el evento cuando un usuario con nivel de acceso asignado, pulsa la huella en el lector después del tiempo de vigencia establecido y no puede ser verificado.

Error de Contraseña: Se muestra el evento cuando se usa el modo de verificación [Tarjeta y Contraseña], contraseña de coacción o contraseña de emergencia para abrir la puerta.

Huella No Registrada: Se muestra cuando en un lector se pulsa una huella que no ha sido registrada o la información de la huella no ha sido sincronizada con el sistema.

Puerta en Horario Inactivo (Botón de Salida): Si se presiona el botón de salida para liberar el botón en horario inactivo, se mostrará el evento anormal.

Fallo al Cerrar Puerta Durante Horario Normalmente Abierto: Se muestra el evento cuando la puerta se encuentra en estado normalmente abierto, pero el usuario no puede bloquearlo con [Bloqueado Remoto].

Error de Formato Wiegand: Se muestra el evento cuando se presenta una tarjeta en un lector y el formato de la tarjeta o la configuración Wiegand no está configurada correctamente.

✍Nota: Es posible definir el nivel de cada evento, ya sea normal, anormal o alarma

11.4 Preguntas y Respuestas

P: ¿Cómo usar un enrolador de tarjetas?

R: Conecte el enrolador a la PC mediante un puerto USB. Luego seleccione el registro de tarjeta de personal individual o por lote. Para el registro individual mueva el cursor al campo de tarjeta y presente la tarjeta en el enrolador y se mostrará el número de tarjeta automáticamente.

P: ¿Para qué sirve la configuración de privilegios?

R: Tiene los siguientes usos: 1. Para unificar los niveles del mismo tipo y establecerlos a los usuarios nuevos. 2. Determinar que atributos del sistema pueden acceder los usuarios.

P: ¿Cómo hacer cuentas para todo el personal de finanzas de la compañía?

R: Primero debe crear un nuevo privilegio en el módulo de sistema y definir las funciones o niveles para este privilegio. Después debe crear un usuario, ingresar la información del usuario, seleccionar el privilegio y agregar la cuenta. Para otras cuentas, haga lo mismo.

P: En Windows Server 2003, el navegador IE browser muestra un error al acceder al sistema, ¿cómo resolverlo?

A: Este problema ocurre porque debe ajustar la configuración de seguridad. Si desea acceder al sistema, configure de la siguiente manera: de clic en Inicio – Panel de Control – Agregar o Remover Programas, seleccione [Agregar o quitar componentes de Windows] y de clic en la opción de [Configuración de seguridad mejorada de Internet Explorer], y desmarque. Luego de clic en [Siguiente] para removerla del sistema. Acceda de nuevo desde el navegador y el sistema se mostrará normalmente.

P: Al respaldar o restaurar la base de datos falla, ¿cuál puede ser la razón?

R:

Respaldo falla: Revise las variables del entorno del sistema, vaya a Propiedades > Variables de entorno del sistema y establezca como: "C:\Program Files\ZK BioSecurity3.0\MainResource\postgresql\bin:". "C:\Program Files" es la ruta de instalación, puede modificarla según sus necesidades.

Restaurar falla: Pueden ser diversas razones: La versión del sistema es obsoleta o muy nueva o la base de dato ha sido dañada. Necesitará revisar estos factores o reinstalar la base de datos.

11.5 Acuerdo de Licencia de Software para Usuario Final

Licencia:

Por medio de la presente, ZKTeco concede la licencia de uso de la aplicación de software bajo la aceptación de las siguientes condiciones: A excepción de las acciones autorizadas por los términos y condiciones de este Acuerdo de Licencia de Software para Usuario Final, sin aplicaciones, usos, duplicaciones, modificaciones, renta o transferencia de forma total o parcial del software.

Usted deberá garantizar:

1. El sistema se aplicará a una sola máquina;

2. Para fines de respaldo o gestión de documentos, usted deberá producir un duplicado, el cual deberá estar en un formato legible por la máquina, de este sistema;

3. Deberá transferir este sistema y el Acuerdo a terceros solo si acepta los términos y condiciones del Acuerdo. Si realiza alguna transferencia, los documentos originales, todos los documentos relacionados y todos los duplicados deberán ser transferidas a terceros. Cualquier documento no transferido y sus duplicados deberán ser completamente destruidos y eliminados;

4. Deberá aplicar este sistema a condición multi-usuario o sistema de Internet, solo después de cumplir uno de los pre-requisitos siguientes:

Se declara por escrito que el sistema será aplicado en condición multi-usuario o sistema de Internet;

o La licencia de uso ha sido comprada para todos los nodos y el nodo final de este sistema.

Usted deberá garantizar:

1. No deberá retransferir la licencia de este sistema;

2. No deberá realizar cualquier tipo de ingeniería inversa, desensamblaje o descompilación;

3. No deberá duplicar, o entregar este sistema, o cualquier parte de este sistema, a excepción de las acciones autorizadas por escrito por los términos y condiciones de este Acuerdo.

Su licencia se termina automáticamente, si usted transfiere este sistema, o cualquier parte de este sistema, o cualquier parte de la duplicación de este sistema a terceros.

Derechos de Autor y Propiedad de este sistema:

Los nombres de este sistema y sus todas sus duplicaciones coexisten con la empresa indicada en el CD-ROM o en este sistema. Este sistema y todos sus documentos relacionados poseen derechos de autor y están bajo protección legal de la "Ley de Derechos de Autor de la República Popular de China" y el "Tratado de la Organización Mundial de la Propiedad Intelectual". Usted no tiene el derecho a borrar la Proclamación de Derechos de Autor para este sistema, y deberá garantizar la duplicación de la Proclamación de Derechos de Autor para este sistema. Usted deberá estar de acuerdo en prevenir y detener cualquier forma de duplicación ilegal de este sistema y todos sus

documentos relacionados.

Garantía de Post-Venta:

Ofrecemos garantía de que, bajo condiciones normales de uso, en los 90 días consecutivos después de la compra, no existirán defectos de material o manual en el software. En caso de que defectos sean certificados, nuestra responsabilidad total será el cambio de software adquirido. Cualquier defecto causado por accidente, mal uso, o abuso no están cubiertos por nuestra garantía de post venta. Portadores intercambiados poseen el resto del período anterior de garantía o 30 días garantía consecutivo (si el periodo restante de la garantía es de menos de 30 días consecutivos).

Limitaciones en Nuestra Garantía:

No asumimos responsabilidad alguna de cualquier otra forma de garantía post-venta que exceda lo indicado en la sección de garantía de post-venta.

Responsabilidad Limitada:

La garantía declarada, ya sea por escrito o implicada, son el contenido completo de la garantía, incluyendo mercadotecnia y garantía de idoneidad para cualquier propósito particular. Nosotros, agentes, distribuidores, y cualquier otro afiliado no somos responsables de cualquier pérdida de ganancia, disminución de la capacidad de uso, interrupción del negocio, o cualquier daño directo, indirecto, especial o accidental causado por el uso de este sistema, y cualquier reclamación de compensación por alguna de las situaciones indicadas no serán admitidas, independientemente de la obediencia o desobediencia de este Acuerdo o si se nos informó previamente de cualquiera de las situaciones indicadas.

Terminación de la licencia:

Podremos terminar la licencia si cualquier término o condición de este Acuerdo es violado. Una vez que la licencia se termina, usted deberá eliminar este sistema, y todos los documentos relacionados, y todas las duplicaciones de este sistema y los documentos relacionados, o regresarlos a nosotros.

Leyes Aplicables y Normas Jurídicas Relacionadas:

Leyes y otras normas jurídicas relacionadas incluyen, pero no se limitan al "Reglamento de Protección de Propiedad Intelectual por la Administración Aduanera de la República Popular de China", "Ley de Derechos de Autor de la República Popular de China", "Ley de Patentes de la República Popular de China", etc.

Usted ya ha leído este contrato y acepta seguir estrictamente los términos y condiciones.