




# ESPECIFICACIONES TÉCNICAS PARTICULARES

**OBRA:**


**ADECUACION SEDE BULLRICH – SAP**

**ANEXO IV – CONTROL DE ACCESOS**

**LÍNEA: SOFSE CENTRAL**

	ELABORÓ	REVISÓ	APROBÓ
NOMBRE	SAMA SERGIO ARIEL		
FIRMA			
FECHA	17/11		

Arq. **FERNANDO MAMOTIUK**  
TRENES ARGENTINOS  
OPERACIONES

<b>TRENES ARGENTINOS OPERACIONES</b>   Ministerio de Transporte Presidencia de la Nación	<b>GERENCIA GENERAL ADMINISTRATIVA</b>	
	<b>ADECUACIÓN SEDE BULLRICH</b>	<b>SC-GGA-ET-04</b>
	<b>ETAPA 2</b>	
	<b>ANEXO IV – CONTROL DE ACCESO</b>	
		<i>Revisión 00</i>
		10/2017
		Página 2 de 24

## Sistema de Gestión de Seguridad Integrado Especificaciones técnicas

### 1. Descripción del Sistema

#### 1.1. Introducción

La aplicación del Sistema de Seguridad Integrado deberá ser un sistema modular, con redes de alarmas, y sistemas de automatización de edificios y control de accesos, capaz de gestionar grandes corporaciones con múltiples sitios remotos, monitoreo de alarmas, sistemas de video, identificación fotográfica, buscadores, guard tour, servidores digitales de video y controles para CCTV. El sistema deberá permitir una fácil expansión o modificación de las entradas, salidas y estaciones de control remotas.

#### 1.2. Servidor Central


El sistema de control de accesos estará completamente integrado al sistema de Accesos central cuyo servidor principal y base de datos estará ubicado en la Estación Constitución, y podrá ser accedido tanto desde el centro de control de constitución, retiro o localmente vía Web station para su total operación. La provisión comprende el alta de este sistema en el servidor central de la estación Constitución y su configuración completa.

El control del sistema en la computadora central deberá ser a través de un programa de software de un solo servidor, deberá proveer la completa integración de todos los componentes, y deberá ser modificable en cualquier momento, dependiendo de las necesidades de la instalación. La reconfiguración se deberá realizar en línea, a través de la programación del sistema, sin que sean necesarios cambios en el hardware.

#### 1.3. Sistema Operativo

El programa de software deberá ser de 32-bit, cliente/servidor de 3 niveles, y deberá ser una aplicación ODBC basada en las herramientas y estándares de Microsoft. El programa de software deberá operar en uno de los siguientes entornos: Windows 7, Windows 8, Windows 8.1, Windows Server 2008 (SP2), Windows Server 2008 R2, o Windows Server 2012.

  
 Arq. FERNANDO MAMOTIUK  
 TRENES ARGENTINOS  
 OPERACIONES

<b>TRENES ARGENTINOS OPERACIONES</b>   Ministerio de Transporte Presidencia de la Nación	<b>GERENCIA GENERAL ADMINISTRATIVA</b>	
	<b>ADECUACIÓN SEDE BULLRICH</b>	
	<b>ETAPA 2</b>	
	<b>ANEXO IV – CONTROL DE ACCESO</b>	
		<b>SC-GGA-ET-04</b>
		<b>Revisión 00</b>
		10/2017
		Página 3 de 24

#### 1.4. Entornos Virtuales

La operación en entornos virtuales deberá ser soportada. Se deberá implementar la seguridad y protección anti-piratería del software a través de un medio que permita la transferencia de un entorno virtual entre plataformas de hardware con restricciones. Se requiere el uso de números de serie del software y registro a través de internet.

#### 1.5. Servidor del Sistema

El programa de software deberá estar conformado por múltiples servidores incluyendo, pero sin limitarse a, servidor de base de datos y comunicaciones, y estación de trabajo de clientes. Los servidores deberán ser capaces de ser instalados en una o más PCs de una red, permitiendo la distribución de los procesos y actividades del sistema.

#### 1.6. Base de Datos

La arquitectura de la base de datos deberá ser Microsoft SQL Server 2008 R2 como estándar, y deberá poder utilizar Microsoft SQL Server 2005 o 2008 si fuera necesario.


#### 1.7. Comunicación

El sistema deberá tener la capacidad de comunicarse con los paneles de control de accesos y alarmas integrados a través de conexiones LAN/WAN, utilizando un protocolo de comunicación TCP/IP estándar en la industria: Comunicaciones Seriales Aisladas EIA-485 o Interfaz de Conexión con Marcado a Módem. El sistema deberá encriptar toda la información transmitida desde el servidor de comunicaciones. El controlador del sistema deberá tener una conexión Ethernet integrada, no instalada como interfaz de dispositivos auxiliares o de terceros.

#### 1.8. Cuentas del Sistema / Particiones de la Base de Datos

El software del sistema deberá soportar múltiples particiones, permitiendo el acceso separado a TODOS los componentes de un sitio. El sistema deberá poseer una partición global para el uso de todas las particiones. Los Usuarios, Cronogramas y Niveles de Acceso deberán ser globales para una fácil administración y para permitir su asignación a controladores del sistema individuales. Los Usuarios, Niveles de Acceso y Cronogramas globales deberán poder ser utilizados por múltiples controladores y poder ser asignados a cualquier Nivel de Acceso o Cronograma local.

  
 Sr. FERNANDO MAMOTIU  
 TRENES ARGENTINOS  
 OPERACIONES

<b>TRENES ARGENTINOS OPERACIONES</b>   Ministerio de Transporte Presidencia de la Nación	<b>GERENCIA GENERAL ADMINISTRATIVA</b>		179
	<b>ADECUACIÓN SEDE BULLRICH</b>		<b>SC-GGA-ET-04</b>
	<b>ETAPA 2</b>		<i>Revisión 00</i>
	<b>ANEXO IV – CONTROL DE ACCESO</b>		10/2017
			<i>Página 4 de 24</i>

### 1.9. Planos Gráficos de Planta

El programa de software deberá utilizar Íconos Gráficos para representar los dispositivos de hardware, controladores del sistema y módulos remotos en el sistema. Los íconos deberán utilizarse en los planos de las plantas y vistas de planta para proveer una interfaz de usuario para controlar y monitorear el sistema.

Los dispositivos que se encuentren en un plano deberán poder ser visualizados como una lista ordenada en una ventana separada o una columna dentro de la misma página, o por selección a través de una opción de mostrar lista. La selección de una opción para ver una lista no debería cambiar la vista del plano.

Los planos gráficos de planta deberán tener un mínimo de 30 íconos por defecto, representando varios objetos y dispositivos. Los planos gráficos de planta deben soportar un número ilimitado de íconos gráficos personalizados por el usuario.

Los íconos gráficos se crearán a partir de archivos estándar tipo XAML u OBJ.

### 1.10. Alarmas

El sistema deberá soportar respuestas manuales a las alarmas que se disparen en el sistema. Cada alarma deberá ser capaz de iniciar una cantidad de distintas acciones, como la activación de dispositivos remotos, control de puertas y la activación de archivos WAV.


Todos los eventos dentro del sistema DEBEN ser configurables como alarmas y DEBEN tener mensajes individuales para cada evento.

### 1.11. Prioridad de Alarmas

La prioridad de una alarma no está limitada y debe ser una lista numérica configurable por el usuario. La prioridad de una alarma puede ser asignada a cualquier alarma y determina el orden en que se muestra la alarma.

### 1.12. Exhibición de Alarmas / Entradas de Zona

El sistema deberá proveer monitoreo de alarmas / entradas de zona tanto supervisado como no supervisado. Cuando se reconozca una alarma, el sistema debe ser capaz de cambiar a un plano de planta. El sistema debe ser capaz de armar o desarmar un área que contenga una alarma / entrada de zona tanto de manera manual como automática, por la hora o día de la semana.

<b>TRENES ARGENTINOS OPERACIONES</b>   Ministerio de Transporte Presidencia de la Nación	<b>GERENCIA GENERAL ADMINISTRATIVA</b>	
	<b>ADECUACIÓN SEDE BULLRICH</b>	
	<b>ETAPA 2</b>	
	<b>ANEXO IV – CONTROL DE ACCESO</b>	
	<b>SC-GGA-ET-04</b>	<i>Revisión 00</i>
	10/2017	Página 5 de 24

### 1.13. Control de Accesos

Las funciones de control de accesos deberán incluir validación de acuerdo a la hora, día de la semana, cronograma de vacaciones y verificación de número de tarjeta, recuperación manual fotos de soportes para tarjetas y validación de accesos basada en una verificación positiva de una tarjeta, de una tarjeta y un PIN, tarjeta o PIN, o solo PIN. El sistema de control de accesos DEBE ser capaz de prevenir el acceso a una puerta o área en función de la habilidad del usuario para armar o desarmar el área a la que están accediendo o dejando. El sistema debe soportar la función anti-passback para un mínimo de 128 puertas desde cualquier controlador del sistema y permitir un modo de operación a través de software y a través de hardware.

Para el Control de Acceso del edificio de Av. ALEM 1074, se deberá controlar una puerta tipo Blindex existente, lectora, controladora, electro imán y botón de salida. El mismo tiene que estar comunicado con la central de RETIRO y CONSTITUCION.

### 1.14. Transmisión de Video en vivo


Se DEBE poder mostrar la transmisión de video en vivo de un sistema de CCTV y/o servidor digital en una pantalla de computadora. La ventana de video en vivo permitirá al usuario cambiar el tamaño y ubicación de la misma en la pantalla. Se deberán poder enviar controles al sistema de CCTV y/o servidor digital desde la ventana de video en vivo.

### 1.15. Eventos de Alarma


Los eventos de alarma con prioridades definidas podrán aparecer en el frente de la pantalla en una ventana de evento de Alarma para atraer la atención del operador. La ventana emergente deberá mostrar el nombre del evento (lector, punto de alarma, soporte para tarjeta o sistema de alarmas), hora, fecha, sitio, cuenta, si es una alarma de tarjeta el número de tarjeta, el tipo de evento y el nombre del soporte para tarjetas. Un contador deberá mostrar también la cantidad de veces que el evento se reportó al monitor de Eventos de Alarma antes de que el mismo se reconozca o resuelva. Las instrucciones referentes al evento deberán ser accesibles al clicar dos veces sobre el mismo.

### 1.16. Ventana de Evento de Alarma Personalizada

La ventana de Evento de Alarma deberá permitir al operador iniciar una tanto una respuesta física al evento como una respuesta escrita. Las respuestas incluirán, pero sin limitarse a: reconocer, limpiar, abrir un plano de planta pre-programado, energizar, desenergizar, pulsar, pulsar por un tiempo

  
 Arq. FERNANDO MAMOTIUK  
 TRENES ARGENTINOS  
 OPERACIONES



<b>TRENES ARGENTINOS OPERACIONES</b>   Ministerio de Transporte Presidencia de la Nación	<b>GERENCIA GENERAL ADMINISTRATIVA</b>	
	<b>ADECUACIÓN SEDE BULLRICH</b>	<b>SC-GGA-ET-04</b>
	<b>ETAPA 2</b>	
	<b>ANEXO IV – CONTROL DE ACCESO</b>	
		<i>Revisión 00</i>
		<i>10/2017</i>
		<i>Página 6 de 24</i>

determinado, añadir un comentario, recuperar video del evento, derivar/bypass o remover derivación/remover bypass.

**1.17. Niveles de Seguridad de Operador**

Se podrá definir los niveles del sistema a los que tendrá acceso cada operador individual a través de las contraseñas asignadas. Las operaciones del sistema para operadores individuales incluirán, pero sin limitarse a: sesiones de tiempo limitado, cuentas disponibles o selección del lenguaje al iniciar la sesión. Las acciones del operador van desde no tener derechos de visualización ni control, o monitoreo básico, hasta control total del sistema incluyendo programación.

**1.18. Programación del Sistema**

La programación del sistema deberá ser amigable con el usuario, y podrá ser realizada por personal sin experiencia previa en computadoras. El sistema utilizará buzones para toda la información requerida por el sistema previamente ingresada.

La programación deberá realizarse a través de MENUS e incluirá información de "Ayuda" o "Tutorial" en línea, como así también ejemplos de ingreso de datos en línea. La Ayuda deberá estar disponible al presionar la tecla F1. Al utilizar el acceso a la Ayuda a través de F1, el menú de Ayuda proveerá información detallada relativa a la operación que el usuario está realizando sin necesidad de incluir ningún parámetro de búsqueda adicional.

**1.19. Configuración del Hardware**


Luego de la instalación, el usuario podrá realizar cambios de configuración del hardware. Estos cambios de configuración del hardware incluirán, pero sin limitarse a: tiempo de apertura de una puerta, tiempo de forzado de un contacto de puerta, nombre de zona y lectoras, dónde y cuándo es válido un soporte de tarjetas, y la habilidad de adicionar o modificar las bases de datos de las tarjetas como se desee sin la necesidad de los servicios de un contratista o el fabricante.

**1.20. Procesamiento Distribuido**

Todos los componentes de control utilizarán "Procesamiento Distribuido". El procesamiento distribuido incluirá la posibilidad de descargar los parámetros operativos a cualquier controlador del sistema, permitiendo de esta manera que el controlador del sistema tenga funciones completamente operativas independientes de la computadora de control de acceso integral al sistema.

Arq. FERNANDO MAMOTIUK  
TRENES ARGENTINOS  
OPERACIONES



<b>TRENES ARGENTINOS OPERACIONES</b>   Ministerio de Transporte Presidencia de la Nación	<b>GERENCIA GENERAL ADMINISTRATIVA</b>		182
	<b>ADECUACIÓN SEDE BULLRICH</b>		<b>SC-GGA-ET-04</b>
	<b>ETAPA 2</b>		<b>Revisión 00</b>
	<b>ANEXO IV – CONTROL DE ACCESO</b>		10/2017
			<i>Página 7 de 24</i>

## 2. Capacidades del Sistema

### 2.1. Introducción

El Sistema de Gestión de Seguridad Integrado deberá poseer las capacidades enumeradas en la sección siguiente.

### 2.2. Capacidades del Sistema

La siguiente sección especifica las capacidades máximas que pueden ser alcanzadas por un Sistema de Gestión de Seguridad Integrado.

- Hasta 5 millones de usuarios
- Niveles de acceso ilimitados
- Grupos de puertas ilimitados
- Grupos de áreas de alarmas ilimitados
- Cronogramas ilimitados
- Planos de nivel ilimitados
- Reportes de estado ilimitados

### 2.3. Servidor / Estación de Trabajo


El Sistema requerirá un servidor de archivos de control maestro y será capaz de soportar hasta 20 ubicaciones de control concurrentes (con sesión iniciada), estaciones de identificación fotográfica, o estaciones de trabajo, utilizando software y hardware para redes LAN/WAN.

Las licencias de estación de trabajo son concurrentes y están determinadas por el número total de clientes que tengan la sesión iniciada.

El software de las estaciones de trabajo puede ser implementado en cualquier estación de trabajo, limitado únicamente por las restricciones del licenciamiento del servidor.

### 2.4. Instalación

El software del sistema podrá ser instalado en cualquier estación de trabajo, siempre que no se violen los requerimientos de la licencia. Sólo podrán iniciar sesión, en cualquier momento, la cantidad de usuarios que permita la licencia.

<b>TRENES ARGENTINOS</b> <b>OPERACIONES</b>   Ministerio de Transporte Presidencia de la Nación	<b>GERENCIA GENERAL ADMINISTRATIVA</b>		183
	<b>ADECUACIÓN SEDE BULLRICH</b>		<b>SC-GGA-ET-04</b>
	<b>ETAPA 2</b>		<b>Revisión 00</b>
	<b>ANEXO IV – CONTROL DE ACCESO</b>		10/2017 Página 8 de 24

### 2.5. Dispositivo de Hardware de Seguridad

El sistema no utilizará ningún dispositivo de hardware de seguridad (dongle) para los componentes del servidor o estaciones de trabajo. La seguridad del software se proveerá a través de un número de serie del software, que será utilizado en el momento de la instalación, y a través del registro de los componentes del servidor del sistema.

### 2.6. Control del Sistema

El control general del control de accesos, sistemas de buscadores, y monitoreo de alarmas se realizará a través de software, lo que permite la completa integración entre los componentes de seguridad y control de accesos. El sistema no dependerá de la operación del servidor, estación de trabajo u otras computadoras externas para tomar decisiones o ejecutar acciones de control de accesos.

### 2.7. Descargas del Servidor de Archivos de Comunicación

El servidor de archivos podrá operar con o sin comunicación con el hardware, y sólo deberá soportar la descarga de archivos cambiados o modificaciones.

### 2.8. Conexión Directa


Las capacidades del Controlador Integrado de Accesos y Alarmas en conexión directa con una PC con Windows deberán ser como mínimo:

- 256 Lectoras por Controlador Integrado del Sistema
- Controladores Integrados ilimitados por sitio
- Capacidad para 65.000 usuarios en cualquier controlador
- Usuarios Globales configurables en el sitio
- Niveles de Acceso global
- 250 áreas de procesamiento completo de alarmas y reportes
- 16 Ascensores
- 128 Niveles de ascensores

### 2.9. Expansión Modular

El sistema será expandible en incrementos modulares hasta su capacidad total. El software deberá soportar el licenciamiento modular para partes clave, y en incrementos pequeños o grandes. Se deberán proveer las licencias de servidor



<b>TRENES ARGENTINOS OPERACIONES</b>  	<b>GERENCIA GENERAL ADMINISTRATIVA</b>		184
	<b>ADECUACIÓN SEDE BULLRICH</b>		<b>SC-GGA-ET-04</b>
	<b>ETAPA 2</b>		<b>Revisión 00</b>
	<b>ANEXO IV – CONTROL DE ACCESO</b>		10/2017
			<i>Página 9 de 24</i>

de comunicaciones para expandir las capacidades del sistema cuando sea necesario. La actualización de la licencia de un usuario o la cantidad de servidores de comunicación no requerirá ningún software adicional.

### 2.10. Actualización de Firmware

Todo el firmware de los módulos permitirá su actualización online a través de una utilidad de actualización en la PC servidor. Todos los controladores del sistema deberán tener la capacidad de actualizar firmware a través de una comunicación RS-485 o TCP/IP.

## 3. Capacidades del Sistema

### 3.1. Introducción

Las siguientes capacidades funcionales son consideradas esenciales para el sistema descrito en esta especificación. Estas capacidades son consideradas estándar, sin necesidad de ningún agregado de software ni hardware.

### 3.2. General

Las siguientes secciones explican las funciones generales que se relacionan con el sistema integrado de control de accesos y gestión de alarmas.

3.2.1. Todas las bases de datos tendrán la capacidad de AGREGAR, BORRAR, VER o EDITAR información.

3.2.2. Proveer capacidades de almacenamiento para todos los eventos del sistema y transacciones de los operadores en forma recuperable, y accesibles a través de conexiones estándar en la industria como ODBC o SQL.

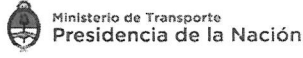
3.2.3. Registrar todos los eventos con fecha y hora (tiempo de registro) y registrar todos los eventos con fecha y hora del momento en que ocurrió el evento en el hardware (tiempo de campo).

3.2.4. El sistema será capaz de operar como una aplicación verdadera de cliente/servidor.

3.2.5. Capacidad de exportar las transacciones del sistema seleccionadas al portapapeles o disco a través de un botón de "exportar", configuración de un filtro de eventos, operación de una aplicación externa que genere un archivo.

3.2.6. Permitir al usuario realizar cambios en las configuraciones del sistema como, pero sin limitarse a: tiempo de apertura de una puerta, tiempo que permanece desbloqueada una puerta, nombre de una puerta, nombre de una

185

<b>TRENES ARGENTINOS OPERACIONES</b>   Ministerio de Transporte Presidencia de la Nación	<b>GERENCIA GENERAL ADMINISTRATIVA</b>	
	<b>ADECUACIÓN SEDE BULLRICH</b>	<b>SC-GGA-ET-04</b>
	<b>ETAPA 2</b>	<b>Revisión 00</b>
	<b>ANEXO IV – CONTROL DE ACCESO</b>	10/2017 Página 10 de 24

lectora, cuándo y dónde es válido un soporte para tarjetas, y la capacidad de agregar o modificar bases de datos de tarjetas en cualquier momento.

3.2.7. Soportar “Anti-passback Global”, permitiendo que un soporte para tarjetas ingrese/salga cualquier lector de tarjetas definido en el mismo panel inteligente de control integrado.

3.2.8. Las funciones Anti-passback deberán incluir modos hard (sin perdones), soft (permitiendo el acceso pero generando un evento de alarma) y temporizados para todas las lectoras del controlador inteligente, en una lectora específica o tarjeta por un período de tiempo configurable.

3.2.9. La función Anti-Passback podrá ser reiniciada siguiendo un cronograma programado.

3.2.10. La función de emergencia deberá operar cuando se utilice un PIN que haya sido configurado como un usuario de emergencia o u usuario ingrese su número de PIN incrementado en una unidad.

3.2.11. Regla de dos usuarios, cuando se requiere que dos usuarios válidos no idénticos sean utilizados dentro de un período de tiempo programable para permitir el acceso a un área o una puerta. Un usuario debe poder ser configurado como un proveedor o usuario dual maestro de custodia.

3.2.12. Capacidad de mostrar cuando un soporte para tarjetas que utiliza la lectora ha accedido (abierto) a la puerta, o si la tarjeta fue utilizada pero la puerta no fue abierta.

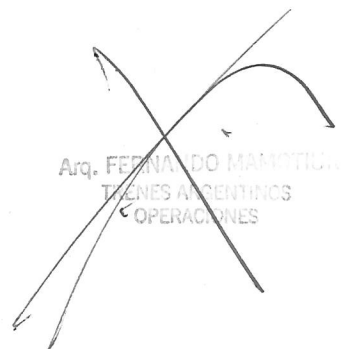
3.2.13. Modo de operación de un cerrojo donde la primera tarjeta válida desbloquea la puerta y la segunda vuelve a bloquearla.


3.2.14. Proveer sistemas de diagnóstico de hardware que sean fácilmente seleccionables, y muestren configuraciones del sistema o comandos que no fueron aceptados por ninguno de los componentes de hardware conectados.

3.2.15. Debe haber una clara identificación del estado del hardware en la barra de estado de la aplicación de cliente.

3.2.16. Proveer un modo de operación del sistema que requiera que el operador ingrese una respuesta a un evento al reconocerlo desde la ventana de alarmas.

3.2.17. Proveer un modo de operación del sistema que permita la limpieza automática de las alarmas reconocidas.

  
Arq. FERNANDO MAMOTI  
TRENES ARGENTINOS  
OPERACIONES

<b>TRENES ARGENTINOS OPERACIONES</b>  	<b>GERENCIA GENERAL ADMINISTRATIVA</b>		186
	<b>ADECUACIÓN SEDE BULLRICH</b>		<b>SC-GGA-ET-04</b>
	<b>ETAPA 2</b>		<i>Revisión 00</i>
	<b>ANEXO IV – CONTROL DE ACCESO</b>		10/2017
			<i>Página 11 de 24</i>

3.2.18. Proveer un modo de operación del sistema en el cual los eventos no reconocidos harán que la computadora reproduzca continuamente un archivo de audio y muestre una notificación de alarma hasta que todas las alarmas no reconocidas sean reconocidas. Una opción de silencio momentáneo permitirá que el tono audible sea silenciado por hasta 60 segundos al seleccionar la ventana de alarmas. La barra de estado mostrará el número total de alarmas en el sistema y un botón de acceso directo dirigirá al operador a la ventana de lista de alarmas.

3.2.19. Cuando un evento reconocido está en el registro de alarmas, pero no fue borrado, será re emitido automáticamente requiriendo un reconocimiento cuando el evento cambie a una condición de alarma o problema.

3.2.20. Proveer un modo de operación del sistema en el que no se permita que un operador borre una alarma sin antes restaurarla a la normalidad.

3.2.21. Capacidad para permitir al operador controlar manualmente las salidas del sistema. Las funciones manuales incluirán energizar, desenergizar, energizar por un tiempo determinado, o energizar pulsando el relé de salida. El tiempo del pulso será programable con tiempos de encendido y apagado específicos para un ciclo de trabajo.

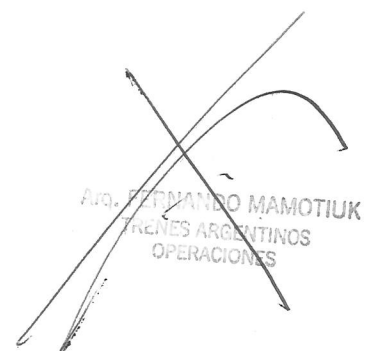
3.2.22. Capacidad para permitir al operador controlar manualmente los sistemas de puertas. Las funciones de control manual incluirán bloquear, desbloquear, deshabilitar salida, deshabilitar entrada, deshabilitar entrada y salida, desbloqueo asegurado.

3.2.23. Mostrar automáticamente las imágenes de video almacenadas de un soporte para tarjetas cuando se muestre una ventana emergente de puertas, mostrando una vista en vivo y video archivado de la cámara asociada.

3.2.24. La ventana emergente de imágenes de video se activará en función de la configuración de la puerta. El tamaño de las ventanas emergentes deberá ser un parámetro ajustable por el operador.

3.2.25. Soportar múltiples tecnologías de lectoras de tarjetas, incluyendo:

- Proximidad
- Wiegand
- Biométricos
- Cinta magnética
- Código de barras

  
 Ato. FERNANDO MAMOTIU  
 TRENES ARGENTINOS  
 OPERACIONES



<b>TRENES ARGENTINOS OPERACIONES</b>  	<b>GERENCIA GENERAL ADMINISTRATIVA</b>	
	<b>ADECUACIÓN SEDE BULLRICH</b>	<b>SC-GGA-ET-04</b>
	<b>ETAPA 2</b>	
	<b>ANEXO IV – CONTROL DE ACCESO</b>	<b>Revisión 00</b>
		10/2017
		Página 12 de 24

- Teclados
- Tarjeta/teclado (PIN)
- ID de vehículos de alta velocidad y amplio rango
- Smart Card (Mifare o formatos abiertos similares)

3.2.26. Proveer un medio para backups automáticos programados de cualquier archivo de la base de datos, o de toda la base de datos. Se deberá proveer un medio para restaurar estos archivos a través de un programa como SQL Server Management Studio o similar.

3.2.27. Capacidad de comunicarse con módems utilizando Windows TAPI y poseer la configuración de los módems y sus funciones (marcado, sólo alarma, salida por SMS) dentro del sistema.

3.2.28. La comunicación entre el servidor de comunicaciones del control de accesos y los paneles de control inteligentes remotos debe utilizar un protocolo de comunicación TCP/IP y debe ser parte del panel de control. El software y el servidor no deben ser restringidos de ninguna manera por el número de dispositivos de hardware que se puedan comunicar con él.

3.2.29. Todos los comandos y actualizaciones de los paneles deberán ser verificados y serán reprocesados si las comunicaciones fallan. En el caso de que un panel no reciba correctamente las comunicaciones, se activará un evento.


3.2.30. Toda la programación de información en los controladores del sistema deberán ocurrir de manera automática, con la opción de realizar una descarga manual seleccionable por controlador.

3.2.31. Capacidad de mostrar el estado de los controladores y su último estado de descarga en línea. Fecha y hora de la última descarga se almacenarán en el controlador. La última dirección IP con la que el controlador se comunicó con el servidor se almacenarán en un registro de Última Dirección IP en el archivo del controlador.

3.2.32. Capacidad para iniciar una llamada a un sistema de buscadores al recibir una condición de evento. Una condición de evento se definirá como cualquier evento y NO DEBE limitarse a eventos de los controladores.

3.2.33. Existirá un modo de operación para invitados que requerirá que una computadora le otorgue el acceso a las tarjetas "válidas". Un modo alternativo de invitados permitirá que la información de las tarjetas de acceso

  
 Arq. FERNANDO MAMOTIUK  
 TRENES ARGENTINOS  
 OPERACIONES

<b>TRENES ARGENTINOS OPERACIONES</b>   Ministerio de Transporte Presidencia de la Nación	<b>GERENCIA GENERAL ADMINISTRATIVA</b>	
	<b>ADECUACIÓN SEDE BULLRICH</b>	<b>SC-GGA-ET-04</b>
	<b>ETAPA 2</b>	
	<b>ANEXO IV – CONTROL DE ACCESO</b>	
		<i>Revisión 00</i>
		10/2017
		Página 13 de 24

sea descargada a la vez que se desbloquean las puertas para tarjetas “válidas”.

3.2.34. Todos los archivos de la base de datos tendrán un historial que se mostrará al abrir el archivo, el historial deberá mostrar cada cambio en el archivo e incluirá, pero sin limitarse a: el nombre del operador, tiempo del cambio, tipo de transacción y que cambió en el archivo con la información anterior y nueva.

3.2.35. Todos los archivos de la base de datos tendrán un acceso directo a los eventos dentro de la base de datos, filtrado por archivo.

### 3.3. Usuario

La siguiente sección detalla los requerimientos para la operación de la base de datos del usuario y los parámetros de configuración.

3.3.1. La información de los soportes para tarjetas deberá incluir un número de tarjeta único de hasta 15 dígitos y opcionalmente, un número de identificación personal.

3.3.2. Permitir múltiples tarjetas por soporte para tarjetas. El mínimo será 8 registros por soporte para tarjetas.

3.3.3. Permitir un número ilimitado de campos que puedan ser configurados por el usuario.


3.3.4. Permitir un número ilimitado de pestañas definibles por el usuario.

3.3.5. Permitir opciones de tarjeta especiales, que incluyan pero sin limitarse a:

- Zona de referencia temporal, que defina el horario válido.
- Mostrar un mensaje de bienvenida a un usuario cuando inicie sesión a través de un teclado.
- Proveer una opción para llevar al usuario directamente al menú del teclado cuando éste inicie sesión a través de un teclado.
- Un tiempo de activación prolongado de puertas para usuarios con discapacidades físicas, que se programe por usuario y puerta.

3.3.6. Proveer una fecha/tiempo de activación y vencimiento específicas (años de validez).

3.3.7. Proveer una función de “Rastreo”. La función de “Rastreo” permitirá control de accesos normal, pero proveerá un evento de rastreo en el monitor del sistema.

<b>TRENES ARGENTINOS OPERACIONES</b>  	<b>GERENCIA GENERAL ADMINISTRATIVA</b>	
	<b>ADECUACIÓN SEDE BULLRICH</b>	<b>SC-GGA-ET-04</b>
	<b>ETAPA 2</b>	
	<b>ANEXO IV – CONTROL DE ACCESO</b>	
		<i>Revisión 00</i>
		10/2017
		Página 14 de 24

3.3.8. Capacidad de almacenar imágenes digitales de un soporte para tarjetas y usar la imagen digital para generar tarjetas de identificación, información de transacciones y reportes de usuarios.

3.3.9. Cuando se edite la información de una tarjeta, la información actualizada deberá ser enviada automáticamente al panel de control de accesos adecuado, cuando esté cableado, sin intervención del usuario. Si el puerto es de marcado, la entrada se almacenará en el disco, y se actualizará cuando se realice una conexión con el lazo remoto. Si se utiliza un cronograma, las actualizaciones de las tarjetas deberán enviarse de acuerdo al mismo.

3.3.10. Los números de tarjetas 0 y 65.535 no serán números de tarjeta válidos, ya que algunos dispositivos transmiten estos números al realizar una lectura incorrecta o como parte de un proceso de lectora de tarjetas de alto nivel.

3.3.11. Proveer una opción especial de reporte que esté directamente dentro de la pestaña del usuario, y genere un reporte de eventos basado en todos los eventos asociados con el usuario.

3.3.12. Debe tener una vista gráfica de los accesos a puertas y áreas de alarma que tiene un usuario, que muestre la lista de puertas con un cronograma de siete días. Una barra verde indicará el acceso a la hora mostrada.

3.3.13. Cuando se agregue un nivel de acceso a un usuario, el operador podrá seleccionar y arrastrar el nivel al usuario, o seleccionar un grupo de niveles y asignarlos.

3.3.14. La vista de grupos presentará a los usuarios en una vista de árbol de acuerdo al archivo de usuarios asignados.


**3.4. Niveles de Acceso**

La siguiente sección detalla los requisitos para la operación de los niveles de acceso y parámetros de configuración.

3.4.1. Capacidad para definir un cronograma específico de operación para que el nivel de acceso permita al usuario al que fue asignado acceder a los recursos programados.

3.4.2. Capacidad para asignar recursos a los niveles de acceso seleccionando y arrastrando, utilizando los siguientes registros:

  
 Arq. FEDERICO MAMOTIUK  
 TRENES ARGENTINOS  
 OPERACIONES

<b>TRENES ARGENTINOS OPERACIONES</b>   Ministerio de Transporte Presidencia de la Nación	<b>GERENCIA GENERAL ADMINISTRATIVA</b>	
	<b>ADECUACIÓN SEDE BULLRICH</b>	<b>SC-GGA-ET-04</b>
	<b>ETAPA 2</b>	
	<b>ANEXO IV – CONTROL DE ACCESO</b>	Revisión 00 10/2017 Página 15 de 24

- Asignar cualquier número de grupos de puertas de los grupos de puertas configurados.
- Armar grupos de áreas que permitan al usuario acceder a las áreas de alarmas sólo para armar.
- Grupos de áreas de desarmado que permitan al usuario acceder a las áreas de alarmas para armar y desarmar las áreas.
- Asignar ascensores específicos.
- Asignar un grupo de plantas a las cuales el nivel de acceso permitirá acceder.

3.4.3. Proveer una plantilla de un nivel de acceso determinado, en la que se puedan hacer modificaciones para guardarla como un nuevo nivel. La cantidad de plantillas no será limitada y podrá ser copiada al agregar nuevos niveles de acceso.

3.4.4. Proveer un control de accesos con estructura de árbol, para los archivos que estén agrupados en esa misma configuración.

3.4.5. La información de uso debe ser mostrada en una pestaña que liste la localización de todos los lugares de referencia del nivel de acceso. Esta lista de referencia no necesariamente debe ser específicamente ejecutada, y debe mostrarse en una vista tipo grilla.

### 3.5. Grupos de Puertas

La siguiente sección detalla los requisitos para la operación de los grupos de puertas y parámetros de configuración.

3.5.1. Los nombres de los grupos de puertas consistirán en una entrada que permita un nombre personalizado de hasta 250 caracteres.

3.5.2. Capacidad para asignar una puerta con solo arrastrarla y soltarla en la ventana de grupo de puertas. La selección será filtrada por archivo de grupo y sólo se mostrarán las puertas que pertenezcan al archivo de grupo.

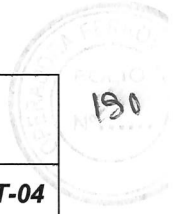
3.5.3. Programar un cronograma para cualquier puerta programada en el grupo de puertas.


3.5.4. Mostrar el nombre del controlador en el que está localizada la puerta en el grupo de puertas y en la ventana de selección.

3.5.5. Proveer una estructura de árbol en los archivos que se agrupen utilizando las configuraciones de archivo de grupos.

3.5.6. La información de uso debe ser mostrada en una pestaña que liste la localización de todos los lugares de referencia del grupo de puertas. Esta lista

Arq. FERNANDO MAMOTILLA  
TRENES ARGENTINOS  
OPERACIONES



<b>TRENES ARGENTINOS OPERACIONES</b>   Ministerio de Transporte Presidencia de la Nación	<b>GERENCIA GENERAL ADMINISTRATIVA</b>	
	<b>ADECUACIÓN SEDE BULLRICH</b>	<b>SC-GGA-ET-04</b>
	<b>ETAPA 2</b>	<b>Revisión 00</b>
	<b>ANEXO IV – CONTROL DE ACCESO</b>	10/2017 Página 16 de 24

de referencia no necesariamente debe ser específicamente ejecutada, y debe mostrarse en una vista tipo grilla.

### 3.6. Grupos de Áreas

La siguiente sección detalla los requisitos para la operación de los grupos de áreas y parámetros de configuración.

3.6.1. Los nombres de los grupos de áreas consistirán en una entrada que permita un nombre personalizado de hasta 250 caracteres.

3.6.2. Capacidad para asignar un área con solo arrastrarla y soltarla de una ventana al grupo de puertas de cualquier controlador.

3.6.3. Programar un cronograma para cualquier área programada en el grupo de puertas.

3.6.4. Mostrar el controlador en el que está localizada la puerta en el grupo de puertas y en la ventana de selección.

3.6.5. Proveer una estructura de árbol en los archivos que se agrupen utilizando las configuraciones de archivo de grupos.

3.6.6. La información de uso debe ser mostrada en una pestaña que liste la localización de todos los lugares de referencia del grupo de áreas. Esta lista de referencia no necesariamente debe ser específicamente ejecutada, y debe mostrarse en una vista tipo grilla.

### 3.7. Grupos de Plantas

La siguiente sección detalla los requisitos para la operación de los grupos de plantas y parámetros de configuración.

3.7.1. Los nombres de los grupos de plantas consistirán en una entrada que permita un nombre personalizado de hasta 250 caracteres.


3.7.2. Capacidad para asignar una planta al grupo de plantas con solo arrastrarla y soltarla de una ventana.

3.7.3. Mostrar el controlador en el que está localizada la planta en el grupo de plantas y en la ventana de selección.

3.7.4. Proveer una estructura de árbol en los archivos que se agrupen utilizando las configuraciones de archivo de grupos.

  
Arq. FERNANDO M. SUTILLI  
TRENES ARGENTINOS  
OPERACIONES



<b>TRENES ARGENTINOS OPERACIONES</b>  	<b>GERENCIA GENERAL ADMINISTRATIVA</b>	
	<b>ADECUACIÓN SEDE BULLRICH</b>	
	<b>ETAPA 2</b>	
	<b>ANEXO IV – CONTROL DE ACCESO</b>	
		<b>SC-GGA-ET-04</b>
		<i>Revisión 00</i>
		10/2017
		Página 17 de 24

**3.8. Grupos de Archivos**


La siguiente sección detalla los requisitos para la operación de los grupos de archivos y parámetros de configuración.

- 3.8.1. Los grupos de archivos deberán permitir la asignación de cualquier nombre al grupo de archivos.
- 3.8.2. Los grupos de archivos con múltiples anidamientos mostrarán ramas y sub-ramificaciones bajo el archivo maestro como un árbol.
- 3.8.3. Un ÍCONO mostrará un grupo de archivos expandibles o una carpeta cuando sea seleccionado.
- 3.8.4. Los grupos de archivos pueden ser asignados a los siguientes archivos:
  - Usuarios
  - Niveles de Acceso
  - Grupos de Puertas
  - Grupos de Plantas
  - Controladores
  - Puertas
  - Ascensores
  - Grupos de Ascensores


**3.9. Monitoreo de Alarmas – Visualización sólo de Alarmas**

La siguiente sección detalla los requisitos para la operación de la ventana de monitoreo y visualización de alarmas.

- 3.9.1. Reportar puntos de actividad de alarmas.
- 3.9.2. Colores de alarmas que se hayan activado, configurables desde la ventana de alarmas.
- 3.9.3. Capacidad de acceder al plano de planta por defecto de cualquier punto de alarma al hacer click derecho sobre la alarma.
- 3.9.4. Capacidad para derivar entradas en el sistema para prevenir una alarma.
- 3.9.5. Ejecutar notificaciones de alarmas en todos los modos de operación.
- 3.9.6. Capacidad para reconocer cualquier alarma, tarjeta o actividad de lectoras, con prioridades.
- 3.9.7. Capacidad para mostrar la actividad del sistema con las prioridades más altas al inicio de la lista, con un número ilimitado de opciones de prioridad.

  
 Ato. FERNANDO MAC...  
 TRENES ARGENTINOS  
 OPERACIONES



<b>TRENES ARGENTINOS OPERACIONES</b>   <small>Ministerio de Transporte Presidencia de la Nación</small>	<b>GERENCIA GENERAL ADMINISTRATIVA</b>	
	<b>ADECUACIÓN SEDE BULLRICH</b>	<b>SC-GGA-ET-04</b>
	<b>ETAPA 2</b>	
	<b>ANEXO IV – CONTROL DE ACCESO</b>	
		<i>Revisión 00</i>
		10/2017
		Página 18 de 24

3.9.8. Capacidad para permitirle al operario reconocer y limpiar alarmas desde la notificación. Antes del reconocimiento, el usuario deberá estar habilitado para seleccionar una respuesta por alarma. El sistema ofrecerá un medio para requerir el reconocimiento de una alarma antes de que pueda ser borrada.

3.9.9. Proveer una visualización de las transacciones más corrientes en tiempo real.

3.9.10. Capacidad para proveer un monitoreo dinámico de los puntos de alarma en tiempo real en la computadora terminal de visualización de video del sistema.

3.9.11. Proveer un filtro de visualización de alarmas estructurado como una lista, permitiendo al usuario seleccionar dispositivos individuales o grupos de dispositivos a visualizar y asignar a cualquier ventana de alarmas o eventos configurable.

3.9.12. Proveer una condición de problema y evento asociado advirtiendo al operador que las comunicaciones dentro del sistema se han interrumpido y proveer un medio para mostrar esta situación al operador.

3.9.13. Proveer una alarma de “Fallas de Panel de Comunicación” si se pierde la comunicación con un panel.

3.9.14. Proveer una visualización en tiempo real de las alarmas utilizando un click derecho para crear un reporte en tiempo real inmediatamente.

### **3.10. Lista de Estados**

La siguiente sección detalla los requisitos para la operación de la lista de estados que puede ser aplicada a cualquier panel de una ventana de estados y permitir el control a un operador.


3.10.1. Capacidad de permitir actualizaciones dinámicas del estado en tiempo real en la ventana de visualización en la computadora cliente del sistema.

3.10.2. Detalles de color y textos específicos para el estado de un dispositivo.

3.10.3. El árbol de control será creado por el usuario y permitirá el control manual de todos los dispositivos del sistema. Al hacer click derecho sobre un dispositivo en el árbol el operario será capaz de iniciar la acción apropiada de una lista de opciones.

~~Arq. FERNANDO MAMOTIUS  
TRENES ARGENTINOS  
OPERACIONES~~



<b>TRENES ARGENTINOS OPERACIONES</b>   Ministerio de Transporte Presidencia de la Nación	<b>GERENCIA GENERAL ADMINISTRATIVA</b>	
	<b>ADECUACIÓN SEDE BULLRICH</b>	<b>SC-GGA-ET-04</b>
	<b>ETAPA 2</b>	<b>Revisión 00</b>
	<b>ANEXO IV – CONTROL DE ACCESO</b>	10/2017
		<b>Página 19 de 24</b>

3.10.4. El árbol de control en una lista de estados permitirá la adición de cualquier combinación de tipos y no estará limitada a algún tipo específico. La mezcla de puertas, salidas, entradas y áreas será posible en una lista de estados.

3.10.5. La lista de estados deberá agregar un filtro opcional que pueda asignarse para mostrar el estado un SOLO tipo específico de dispositivo. Como un ejemplo, deberá ser posible mostrar sólo puertas que están siendo forzadas para abrirlas ocultando las otras puertas de la lista.

### 3.11. Base de Datos de Operadores

La siguiente sección detalla los requisitos para la operación de los operadores y los niveles de seguridad asociados.

3.11.1. El software permitirá la asignación de niveles de operadores para definir los componentes del sistema que cada operador puede ver, operar, cambiar o eliminar.

3.11.2. Definir las cuentas a las que un operador tiene acceso.

3.11.3. Capacidad para registrar las acciones de un operador en los archivos de historial.

3.11.4. Proveer un lenguaje por defecto en base al inicio de sesión de un operador.

3.11.5. Proveer períodos específicos de tiempo en los que un operador puede iniciar sesión.

### 3.12. Paneles

La siguiente sección detalla los requisitos del hardware integrado en el panel de control conectado al servidor de comunicaciones.

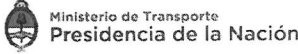
3.12.1. Capacidad de programar todas las funciones del sistema localmente utilizando un teclado LCD conectado al sistema.

3.12.2. Capacidad de programar descripciones, tiempos de derivación, y tiempos transitorios de derivación para todos los puntos de alarma del sistema.

3.12.3. Capacidad para programar descripciones, tiempos de pulsos, y tiempos de energización de los relés de salida del sistema utilizador para el control de puertas y otras funciones auxiliares.

  
Sr. FERNANDO MAMOTIUK  
TRENES ARGENTINOS  
OPERACIONES

185

<b>TRENES ARGENTINOS OPERACIONES</b>   Ministerio de Transporte Presidencia de la Nación	<b>GERENCIA GENERAL ADMINISTRATIVA</b>	
	<b>ADECUACIÓN SEDE BULLRICH</b>	<b>SC-GGA-ET-04</b>
	<b>ETAPA 2</b>	<b>Revisión 00</b>
	<b>ANEXO IV – CONTROL DE ACCESO</b>	<b>10/2017</b>
		<b>Página 20 de 24</b>


- 3.12.4. Capacidad de programar descripciones para todas las lectoras de tarjetas del sistema.
- 3.12.5. Monitorear puntos de alarma supervisados y no supervisados, con la habilidad de seleccionar por punto cuál punto será supervisado y definir si el punto es un contacto normal cerrado o normal abierto.
- 3.12.6. Capacidad para conectar la condición de cualquier punto de alarma con un relé de salida.
- 3.12.7. Capacidad para conectar la condición de cualquier punto de alarma con otro punto de alarma.
- 3.12.8. Capacidad para conectar cualquier punto de alarma para mostrar una cámara en un monitor del sistema.
- 3.12.9. Capacidad para programar alarmas y asociar las alarmas entrantes con salidas relacionadas.
- 3.12.10. Proveer un retardo programable de hasta 255 segundos para todos los puntos de alarma del sistema. El sistema no reportará la condición de alarma hasta que haya transcurrido el período de retardo.
- 3.12.11. Bajo ninguna circunstancia existirá una limitación en los códigos de cualquier dispositivo de lectura o módulo de expansión de lectoras. Se deberán soportar múltiples formatos de lectura a través de todos los paneles y dispositivos.
- 3.12.12. Soportar hasta 128 lectoras por Módulo Inteligente de Control.

**3.13. Reportes**

La siguiente sección detalla los requisitos para la operación de la utilidad para reportes y filtro de operaciones.

- 3.13.1. Los reportes directos de transacciones se mostrarán en una pestaña y estarán disponibles para, pero sin limitarse a: Usuarios, Puertas, Entradas, Salidas y Áreas y al ser seleccionados le darán al operador la posibilidad de generar las últimas 500 transacciones filtradas por el archivo seleccionado. Las transacciones se mostrarán como una lista ordenada en una vista de grilla o con un formato de visualización que permita filtrar por tipo en cualquier texto o información de la transacción.
- 3.13.2. Las transacciones directas soportarán la selección de una vista previa de impresión que mostrará los resultados filtrados del archivo. Todas las

~~Arg. FERNANDO MAMOTILLI  
TRENES ARGENTINOS  
OPERACIONES~~

<b>TRENES ARGENTINOS OPERACIONES</b>   Ministerio de Transporte Presidencia de la Nación	<b>GERENCIA GENERAL ADMINISTRATIVA</b>	
	<b>ADECUACIÓN SEDE BULLRICH</b>	<b>SC-GGA-ET-04</b>
	<b>ETAPA 2</b>	
	<b>ANEXO IV – CONTROL DE ACCESO</b>	
		<i>Revisión 00</i>
		10/2017
		Página 21 de 24

vistas previas de impresión permitirán la impresión en una impresora instalada. Deberá soportar la exportación a los siguientes formatos de archivo PDF, Excel, TIF, JPG, PNG, HTML, RTF, XML y CSV.

3.13.3. Capacidad de crear reportes imprimibles de las transacciones del sistema seleccionadas de la base de datos con cualquier rango de fechas y horas.

3.13.4. Capacidad para generar un reporte de transacciones para el estado de un punto(s) de alarma, Un punto de alarma se definirá como Abierto, Cerrado, Dañado, y Cortado.

3.13.5. Capacidad para generar un reporte del historial de alarmas del sistema. El estado de una alarma del sistema será definida por el panel conectado e incluirá cualquier transacción del panel.

3.13.6. Capacidad de generar un reporte histórico de un usuario directamente desde la pestaña de transacciones principal o desde la opción de vista de eventos del menú de usuario.

3.13.7. Capacidad de generar un reporte de transacciones para las actividades de operador(es) del sistema. El reporte incluirá hora, fecha, nombre del operador, el dispositivo asociado con la acción y el tipo de acción ejecutada por el operador. Las actividades incluirán, pero sin limitarse a:

(1) Alarmas reconocidas y limpiadas, control de puertas, edición o agregado de archivos, derivación de entradas, actualizaciones de módulos y red, y cualquier comando manual en un dispositivo.

3.13.8. Proveer reportes de la base de datos completa que contengan toda la información programada en los archivos de datos del sistema, permitiendo la exportación directa desde el archivo a través del portapapeles un archivo CSV especialmente generado.


### **3.14. Cronogramas**

La siguiente sección detalla los requisitos para la operación de los cronogramas y el proceso de programación de cronogramas.

3.14.1. Las definiciones de los cronogramas deberán incluir hora de inicio, hora final, días de la semana y anulación por vacaciones.

3.14.2. El número máximo de períodos definidos dentro de un cronograma será de al menos 8, y deberá permitir al menos 8 períodos de vacaciones por período.

Arq. ~~FERNANDO MAMOTIUK~~  
TRENES ARGENTINOS  
OPERACIONES

<b>TRENES ARGENTINOS OPERACIONES</b>   Ministerio de Transporte Presidencia de la Nación	<b>GERENCIA GENERAL ADMINISTRATIVA</b>	
	<b>ADECUACIÓN SEDE BULLRICH</b>	
	<b>ETAPA 2</b>	
	<b>ANEXO IV – CONTROL DE ACCESO</b>	
	<b>SC-GGA-ET-04</b>	
	<i>Revisión 00</i>	
	10/2017	
	Página 22 de 24	

- 3.14.3. La hora podrá definirse en un formato de 24 horas (militar).
- 3.14.4. El número mínimo de cronogramas que pueda asignarse a un panel será 1024.
- 3.14.5. Los nombres de los cronogramas podrán tener una longitud de al menos 256 caracteres.
- 3.14.6. Los cronogramas deberán tener una opción que los invalide en caso de que se active una salida del sistema.

### 3.15. Gráfico de Plano de Planta


La siguiente sección detalla los requisitos para la operación del plano de planta y gráficos.

- 3.15.1. Capacidad para importar gráficos de planos de planta almacenados en formato JPG, BMP y GIF.
- 3.15.2. Capacidad para asociar todos los íconos gráficos de un gráfico de plano de planta permitiendo al usuario controlar y monitorear el sistema.
- 3.15.3. Capacidad para permitir la conexión de gráficos de planos de planta en forma jerárquica o a través del uso de botones en los planos de planta individuales.
- 3.15.4. Todas las plantas serán visualizadas en una lista que muestre todos los íconos gráficos en orden jerárquico.

### 3.16. Localizaciones de los Paneles Remotos

La siguiente sección detalla los requisitos para la operación fuera de línea y general de los paneles conectados al servidor de comunicaciones en forma remota.


- 3.16.1. Los paneles de control deberán tener la capacidad de operar fuera de línea cuando la comunicación con un servidor de comunicaciones esté detenida, falle o se interrumpa completamente. En el modo fuera de línea, el panel de control integrado remoto de control de accesos y alarmas deberá almacenar el historial de eventos del panel. El número de eventos del historial se limitará a la capacidad de almacenamiento de buffer de los paneles, y no será menor a 2000 eventos históricos.
- 3.16.2. Capacidad de comunicarse automáticamente con la computadora de comunicaciones para reportar alarmas del sistema o cargar eventos almacenados.

<b>TRENES ARGENTINOS OPERACIONES</b>  	<b>GERENCIA GENERAL ADMINISTRATIVA</b>	
	<b>ADECUACIÓN SEDE BULLRICH</b>	<b>SC-GGA-ET-04</b>
	<b>ETAPA 2</b>	
	<b>ANEXO IV – CONTROL DE ACCESO</b>	
		<i>Revisión 00</i>
		<i>10/2017</i>
		<i>Página 23 de 24</i>

- 3.16.3. Capacidad de manejar al menos 250 sitios remotos.
- 3.16.4. Proveer un cronograma configurable por el usuario que agregue automáticamente tarjetas a una cantidad de sitios.
- 3.16.5. Proveer un cronograma del sistema que será utilizado por la computadora para comenzar automáticamente la carga y descarga de la información de los sitios remotos. La información a ser enviada al panel incluirá, pero sin limitarse a: cambios en la base de datos de tarjetas, horas, días y condición de los buffers de almacenamiento. Mientras el software del sistema esté conectado al sitio remoto, deberá testear, verificar y reportar cualquier pérdida de comunicación con el panel. Si la comunicación con un sitio es más prolongada de lo esperado, el sistema ajustará automáticamente el cronograma para permitir que se actualicen todos los sitios seleccionados.
- 3.16.6. Agregar el sitio a un cronograma de auto-marcado permitirá que el sistema marque una comunicación con el sitio remoto automáticamente en un momento determinado. El cronograma de auto-marcado se programa con la capacidad de marcar una sola vez, ahora, una vez por hora, diariamente, semanalmente, cada dos semanas, mensualmente, o nunca al sitio remoto.
- 3.16.7. Capacidad de permitir al operador programar cuándo ocurrirá la próxima actualización programada, en función de la fecha y hora.
- 3.16.8. La comunicación por marcado con sitios remotos deberá estar protegida por contraseñas. El sitio remoto le envía al sistema una ID de sitio, y el sistema responde con la contraseña apropiada. No se transmitirán comandos ni transacciones hasta que se verifique la línea de comunicación.
- 3.16.9. El sistema será capaz de recibir o enviar información a los paneles de control de accesos remotos a demanda.
- 3.16.10. La cantidad de intentos de re-marcado que se realizarán desde el sitio remoto será definida entre 1 y 5.
- 3.16.11. La capacidad de hacer una pausa entre intentos deberá poder programarse entre 1 y 120 segundos.
- 3.16.12. La capacidad para hacer una pausa antes de desconectarse deberá poder programarse entre 1 y 30 segundos.
- 3.16.13. La velocidad de las comunicaciones deberá ser de 38,4 kilo baudios.

  
 Arq. FERNANDO MAMOTIUK  
 TRENES ARGENTINOS  
 OPERACIONES



<b>TRENES ARGENTINOS OPERACIONES</b>   Ministerio de Transporte Presidencia de la Nación	<b>GERENCIA GENERAL ADMINISTRATIVA</b>	
	<b>ADECUACIÓN SEDE BULLRICH</b>	<b>SC-GGA-ET-04</b>
	<b>ETAPA 2</b>	<i>Revisión 00</i>
	<b>ANEXO IV – CONTROL DE ACCESO</b>	10/2017 <i>Página 24 de 24</i>

### 3.17. Redes

La siguiente sección detalla los requisitos para la operación de la red TCP/IP y el servidor de comunicaciones.

3.17.1. Capacidades de red (LAN o WAN) como característica estándar, definida por la licencia, no como una actualización de software o un agregado de hardware.

3.17.2. Proveer un servidor y licenciamiento para la configuración de hasta una estación de trabajo. Las licencias podrán ser adquiridas posteriormente, en cantidad necesaria, pero sin limitarse a ningún valor menor que 1.

3.17.3. Capacidad de una red del sistema de soportar usuarios concurrentes hasta el límite máximo. Por ejemplo, una estación de trabajo que agregue tarjetas y haga cambios de usuario, otra estación de trabajo que monitoree las alarmas, otra ejecutando reportes de la base de datos, otra controlando las puertas y las alarmas, y así sucesivamente.

3.17.4. La estación de trabajo tendrá la misma interfaz gráfica de usuario que la que funciona como en la máquina servidor.

  
Aro. FERNANDO MAMOTIUK  
TRENES ARGENTINOS  
OPERACIONES