

# Software de los sistemas de control de accesos

**Ing. Luis Cosentino**

Consultor Independiente  
lcosentino@fibertel.com.ar



Diseñada como una ayuda para técnicos, instaladores y estudiantes, ofrecemos a nuestros lectores una serie de conceptos y fundamentos sobre el control de accesos, sus elementos y funciones. Un detallado estudio de mercado y un ejemplo de diseño son los complementos de esta obra que seguramente será de suma utilidad para nuestros lectores.



## ■ Índice

### Capítulo 1 - RNDS N° 45

*Introducción al control de accesos*

### Capítulo 2 - RNDS N° 45

*Qué es un control de accesos. Utilidades*

### Capítulo 3 - RNDS N° 45

*Breve referencia histórica*

### Capítulo 4 - RNDS N° 45

*Esquema básico de un control de accesos*

### Capítulo 5 - RNDS N° 46 / N° 47 / N° 48

*Dispositivos de identificación*

### Capítulo 6 - RNDS N° 49

*Elementos adicionales de entrada y salida*

### Capítulo 7 - RNDS N° 51

*Unidades de control o controladores*

### Capítulo 8

*Software de los sistemas de control de accesos*

#### 8.1. Prestaciones básicas

#### 8.2. Organización de los software de control de accesos

##### 8.2.1. Arquitectura Stand alone

##### 8.2.2. Arquitectura Cliente-Servidor

##### 8.2.3. Arquitectura Servidor web

#### 8.3. Modularidad.

#### 8.4. Bases de datos.

##### 8.4.1. Motores de bases de datos utilizados por los controles de accesos

##### 8.4.2. Interfase/Interrelación entre las bases de datos existentes en las empresas y las utiliza das por el control de accesos.

#### 8.5. Vínculo de los controladores con el software

**E**n el presente apartado se discuten las generalidades de los software de control de acceso, no solo desde el punto de vista de su organización, partición en módulos como de los motores de bases de datos utilizados, sino también sobre sus prestaciones básicas.

Al mirar las ofertas de productos en el mercado se puede notar que las placas que ofrecen la mayoría de los fabricantes del mismo segmento tienen prestaciones similares. Por lo tanto, son las características de los software las que van a definir las capacidades y prestaciones de los productos que se ofrecen. Esto hace que los fabricantes consideren al software como la clave del éxito de su producto.

Para el presente análisis se tienen en cuenta 5 factores: las prestaciones básicas, la topología del software de aplicación, sus diferentes módulos, las bases de datos tanto la de configuración como la de eventos y la conexión de la red de controladores a la PC.

ma, la forma que ofrecen para cargar los datos de los usuarios, las bandas horarias, las categorías, etc.

En lo que respecta a los usuarios, se considera un usuario a aquella persona que pretende ganar acceso en determinadas puertas/áreas. Los sistemas simples suelen guardar cierta información filiatoria básica y permitirle asociar una tarjeta por usuario. Los sistemas más sofisticados permiten que un mismo usuario posea varias tarjetas, incluso con prioridades diferentes.

En cuanto a la información que se almacena de los usuarios, cabe destacar que en una misma aplicación, por ejemplo el control de accesos de una empresa, los datos que deben almacenarse dependen de la categoría del usuario. Por ejemplo, si se trata de un empleado es necesario saber su documento, domicilio, número de legajo, etc., mientras que si se trata de un contratado externo será necesario conocer su ART, si posee vehículo habrá que saber si su registro está al día o si tiene la categoría necesaria para manejarlo, etc. En otras palabras, la información a almacenar del usuario depende más del tipo

### 8.1. Prestaciones básicas

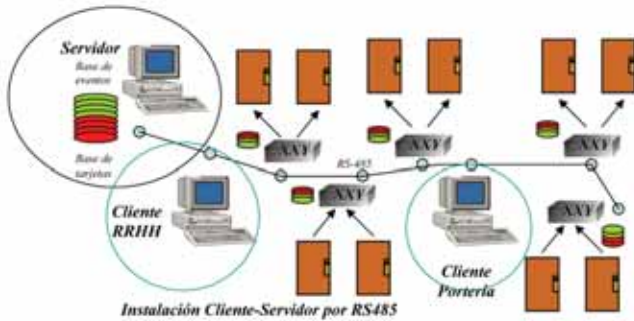
Las prestaciones básicas comprenden la estructura general del programa,

*Continúa en página 168*

Viene de página 168

físico remoto mientras que estén en la misma red lógica.

En la figura se puede apreciar una instalación cliente servidor donde la conexión de los controladores con el servidor es utilizando RS-485 y donde se tienen 5 controladores y 2 estaciones de trabajo.

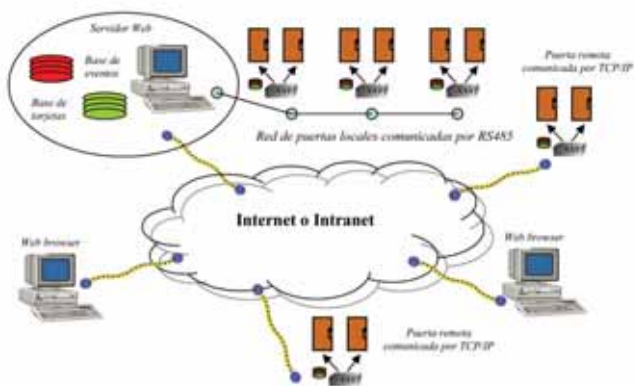


### 8.2.3. Arquitectura Servidor web

La arquitectura servidor Web en varios aspectos es similar a la de Cliente servidor, pero el servidor está organizado como un servidor Web y por lo tanto no será necesario instalar a los clientes, ya que solo se necesita de un navegador de Internet para acceder a la información. Si el servidor Web se publica en Internet será posible acceder al sistema desde cualquier lugar disponiendo de un navegador y las claves correspondientes.

Si bien esta última forma de organización es la mejor, algunas veces es necesario que para su correcta operación se instalen funciones Active-X en las estaciones de trabajo. En algunas empresas medianas y grandes estas instalaciones están limitadas o prohibidas por las reglas internas de seguridad informática.

En la figura se puede observar una instalación de tipo servidor Web pero con un sistema mixto de conexión de los controladores. Hay una pequeña subred RS-485 con 3 controladores y dos controladores remotos conectados vía TCP/IP. También se pueden observar 2 computadoras accediendo al servidor Web ejecutando un Internet browser.



### 8.3. Modularidad.

Es muy difícil de asegurar si la modularidad de los softwares en general se debe a una estrategia comercial planeada o a un crecimiento más o menos caótico basado en satisfacer las

necesidades específicas de los clientes, pero la realidad es que hoy la mayoría de ellos están organizados en forma modular.

Siempre es necesario un módulo básico donde se incluyen las altas baja y modificaciones y la configuración del sistema (definición de puertas, lectoras, áreas, bandas horarias, etc.) como así también algunos reportes elementales. A partir de ahí cada mercado vertical tiene sus propias necesidades, que requieren de soluciones específicas.

Por ejemplo, los edificios de oficinas popularizaron los «módulos de visitas», que tienen por objeto autorizar el acceso temporario cuando una persona. En este caso un visitante fue dado de alta y un empleado otorgó una autorización pertinente. A diferencia de los casos habituales, donde un usuario normal posee siempre la misma tarjeta, el visitante recibirá una tarjeta diferente cada vez que haga una visita. Lo que es deseable de un módulo de visitas es que sea ágil en la asignación la tarjeta y poder tener un reporte permanente de quienes son los visitantes que están presentes.

Lo que debe tenerse bien presente a la hora de especificar un módulo de visitas es la necesidad que se debe atender, no es lo mismo la portería de una empresa que tiene un edificio propio que aquella que comparte el edificio con otras empresas, o donde las visitas ingresan con vehículos o herramientas, o donde las visitas son en realidad contratistas que trabajarán durante un período determinado.

Otro módulo difundido en nuestro medio es el de Guardias o Portería, cuyo objetivo es poder tener ingresos asistidos o ingresos monitoreados mientras se observa el listado de eventos que se producen en tiempo real.

Se dice que un ingreso es monitoreado cuando el guardia puede observar en la pantalla y al mismo tiempo, la foto que está registrada en la base de datos de la persona que acaba de presentar su tarjeta y una imagen de video en vivo, que le permita comparar si se trata de la misma persona. Un ingreso asistido es similar al anterior, pero será el guardia quien luego de verificar la identidad del portador de la tarjeta explícitamente proceda a dar la orden de apertura de la puerta en forma remota. En otras palabras, la diferencia está en que en el ingreso asistido la puerta permanece cerrada hasta que el guardia proceda a su apertura, mientras que en el monitoreado el ingreso es automático cuando el usuario habilitado presenta su tarjeta.

Otro módulo es el diseño e impresión de credenciales, que será el utilizado para convertir una tarjeta blanca en una credencial con nombre, foto, etc. Este módulo debe tener las mismas restricciones de acceso que tiene el que habilita las tarjetas, porque permite la creación de credenciales.

Algunos sistemas de control de accesos poseen módulos de reportes y estadísticas para separar la tarea en quienes definen y los crean y quienes obtienen los resultados.

Otra ventaja de la organización en módulos es que facilita la capacitación de los operadores del sistema, dado que sólo verán los módulos a los que pueden acceder, evitando las tentaciones de navegar por el resto del programa.

### 8.4. Bases de datos.

En este punto cabrían dos aspectos diferentes a tener en cuenta, el primero está referido al motor de base de datos que utiliza el control de acceso para almacenar las configuraciones como los eventos y el segundo está relaciona-

Continúa en página 176

Viene de página 164

de tarea que desempeña que del usuario en sí. Solo los sistemas grandes permiten configurar la información que se requiere del usuario mientras que los sistemas menores utilizan el concepto de módulo independiente, es decir, poseen pantallas no configurables y si se necesita almacenar la información de la ART o del registro de conducir deberá adquirirse el módulo adicional correspondiente.

En lo referente a los permisos, prácticamente todos los sistemas de control de accesos utilizan el concepto de plantilla para facilitar su programación: se hace un modelo donde se colocan las puertas, bandas horarias, feriados, etc., para cada categoría de usuario que posea la aplicación. Así quedarán definidas las plantillas para los empleados administrativos, los obreros del turno mañana, los supervisores, etc. y luego bastará con asociar a los usuarios las plantillas que mejor se adapten a sus necesidades.

Un concepto similar se utiliza para asignar los perfiles de los operadores del sistema: los fabricantes poseen plantillas fijas o programables que definen las prioridades y atribuciones que pueden tener los operadores y un administrador será quien las asigne.

Un capítulo aparte merece la pantalla principal del sistema, que en términos generales dependerá del tipo de usuario. Un vigilador tendrá que poder ver quien está accediendo por la portería, mientras que en el departamento de recursos humanos se pretenderá tener fácil acceso a cargar la información de un nuevo empleado o a hacer un reporte de presentismo. Por eso es que el perfil del operador no sólo define las tareas que puede realizar sino también cuál será su pantalla base de trabajo.

Algunas prestaciones, que hace unos años parecían imprescindibles, fueron perdiendo importancia, aunque de tanto en tanto aparece una aplicación donde son necesarias. Se trata de los denominados mapas o planos que permiten tener el dibujo de la planta y las ubicación de las puertas y barreras en su posición exacta, que generalmente está asociada con la aplicación de busca personas. Esta aplicación parte de la base de definir muchas áreas dentro de la empresa de manera tal de poder saber en que área está cada persona en cada momento y reflejarlas en los mapas.

Otra aplicación que es ofrecida en muchos controles de acceso, pero que se utiliza poco, es el cacheo aleatorio, que consiste en la selección al azar de usuarios que pasan por un acceso para ser revisados más en profundidad.

Existen un gran número de aplicaciones que ofrecen los software de control de acceso, los que serán más o menos útiles dependiendo de las necesidades del cliente específico donde se este utilizando el sistema. Los sistemas nacionales suelen tener aplicaciones más adaptadas a las necesidades locales.

## 8.2. Organización de los software de control de accesos

En función de su organización, en el mercado se encuentran productos estructurados de tres formas.

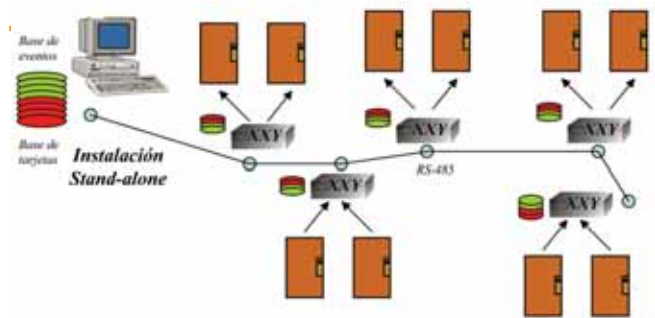
• **Arquitectura Stand alone:** Es aquella en donde todo el software está concentrado en la misma máquina.

• **Arquitectura Cliente-Servidor:** Esta arquitectura permite instalar las bases de datos central con el software en una máquina generalmente denominada «servidor» y la interfase de usuarios, es decir los *clientes*, que pueden ser más de uno, se ejecutan desde máquinas separadas, que se vincularán con el servidor por estar en la misma red lógica.

• **Arquitectura Servidor Web:** Es similar a la de *Cliente-servidor*, pero el servidor está organizado como un servidor Web y por lo tanto no será necesario instalar a los clientes, ya que solo se necesita de un navegador de Internet para acceder a la información.

### 8.2.1. Arquitectura Stand alone

La arquitectura stand-alone es aquella en donde todo el software está concentrado en la misma máquina. Es decir que la aplicación, las bases de datos y las conexiones de los controladores residen en la misma PC, que a su vez, es desde el único lugar donde se lo puede y debe operar. Esta organización se utiliza en los sistemas de baja performance, dado que son de tipo monousuarios y donde no es inconveniente realizar una tarea por vez. Su única ventaja radica en la simplicidad de instalación y operación, mientras que sus desventajas son evidentes frente a las otras opciones. De todas formas se los sigue utilizando en sistemas pequeños.



### 8.2.2. Arquitectura Cliente-Servidor

Esta arquitectura permite instalar las bases de datos central con el software en una máquina generalmente denominada «servidor» y la interfase de usuarios, es decir los *clientes*, que pueden ser más de uno, se ejecutan desde máquinas separadas, que se vincularán con el servidor por estar en la misma red lógica. En este caso deberán realizarse tantas instalaciones como clientes más uno (el servidor) se tenga. La ventaja de esta organización es que cada cliente puede estar corriendo una aplicación sin necesidad de interferir con el resto. Por ejemplo, en una fábrica ubicada en un mismo sitio con dos porterías, donde el control de accesos también se utiliza para obtener los registros de tiempo y asistencia, la instancia «servidor» estará instalada en la sala de servidores y su mantenimiento y backup será responsabilidad del departamento de informática; en cada portería habrá una PC corriendo una instancia «cliente» con el módulo de portería y visitantes; en el departamento de recursos humanos habrá otra instancia cliente corriendo el módulo de Altas Bajas y Modificaciones (ABM), reportes de presentismos y diseño de credenciales mientras que en la oficina central de seguridad podrá existir otra terminal de cliente monitoreando y supervisando la seguridad en general. Estos sistemas, si bien son un poco más complejos de instalar, son más flexibles que los de la arquitectura stand alone porque permiten tener varios usuarios simultáneos e incluso algunos de ellos pueden acceder desde cualquier lugar

Continúa en página 172

Viene de página 172

do con la interrelación entre el motor de base de datos que utilizan los usuarios para su sistema de gestión y los que utilizan los controles de accesos.

#### 8.4.1. Motores de bases de datos utilizados por los controles de accesos

Las bases de datos utilizadas por los sistemas de control de accesos donde se almacenan las configuraciones y los usuarios son de tamaño acotado a la máxima capacidad de usuarios y puertas, mientras que la de los eventos suele crecer indefinidamente.

Los sistemas de bajo costo, por razones lógicas, utilizan motores de bases de datos gratuitos, los que no siempre son los más estables, sobre todo cuando su tamaño crece sin control. Algunos fabricantes utilizan motores de bases de datos propios, mientras que otros permiten opciones de utilizar motores existentes como SQL, MySQL, etc.

En control de accesos no es común el uso de motores de bases de datos grandes como Oracle o Informix, aunque la integración con ellas es deseable por las grandes empresas y la mayoría de las veces los buenos integradores consiguen excelentes resultados.

Si hubiera que hacer algún tipo de recomendación, en sistemas de control de accesos pequeños, podrán utilizarse motores de bases de datos gratuitos teniendo la precaución de hacer backups en forma regular y se deberá ser cuidadoso de mantenerla en un tamaño razonable efectuando purgas periódicas. Ahora bien, si existirán múltiples usuarios concurrentes y un tráfico considerable, se recomienda la utilización de motores de bases de datos confiables y acordes a las necesidades.

#### 8.4.2. Interfase/Interrelación entre las bases de datos existentes en las empresas y las utilizadas por el control de accesos.

Es bastante frecuente que cuando una empresa contrata a un nuevo empleado, el departamento de recursos humanos lo dará de alta en su sistema de gestión empresarial (ERP) donde colocará sus datos. Luego este mismo empleado deberá registrarse en la base de datos del sistema de seguridad para obtener su tarjeta y sus permisos de acceso a las diferentes puertas, para lo cual deberá otra vez colocar sus datos. Esto no sólo es una pérdida de tiempo, sino que algunas veces los datos no coinciden y genera un costo adicional porque obliga a mantener varias bases de datos con información redundante de sus empleados. Además puede suceder que cuando un empleado deja de trabajar, su registro en la base de datos se actualiza convenientemente mientras que si eso no ocurre en el sistema de seguridad, su tarjeta de acceso continuará abriendo las puertas.

La forma de evitar estos inconvenientes es mantener las bases de datos del sistema ERP y del sistema de seguridad sincronizadas. Esta es una tarea que deberá realizar el integrador porque ni los sistemas ERP ni los sistemas de control de accesos poseen integraciones automáticas a nivel base de datos, ni siquiera aunque ambas utilicen el mismo motor.

En términos generales esta interfase se realiza mediante procesos que detectan los cambios en la base de datos del ERP y actualizan a la del control de accesos utilizando los comandos de importación y exportación.

#### 8.5. Vínculo de los controladores con el software

En el mercado se encuentran tres alternativas, siendo que sólo en sistemas de mediano y gran porte es posible encontrar soluciones que combinan las alternativas anteriores.

Si se utilizan controladores comunicados por RS-485 será necesario que la red física se conecte en forma directa a un puerto del servidor o a algún concentrador de comunicaciones que funciona como vínculo lógico.

Si se utiliza TCP/IP, sólo será necesario que todos los controladores estén conectados a la misma red donde se encontrará el servidor. En este caso, el cableado será más simple porque deberá conectarse el controlador a la boca de red más cercana, siendo responsabilidad del departamento de informática la de mantener el vínculo activo. Desde el punto de vista lógico, la topología de la red es de tipo estrella.

La tercera alternativa consta de una solución que utiliza la red de Microsoft permitiendo el armado de una red lógica de controladores aunque físicamente estén conectados por puertos RS-232 o RS-485 de diferentes PC que forman parte de la red. En esta alternativa cada controlador o conjuntos de ellos se conectan a la PC más cercana, que en muchos casos será a la misma distancia que la boca de red más cercana. Desventaja: para que exista comunicación la PC deberá estar activa y conectada a la red.

Otro tema que muchas veces lleva a confusión está relacionado con el deseo de acceder al sistema desde varios sitios geográficamente distribuidos. En este caso se considera erróneamente que el hecho de especificar que la forma de conexión entre los controladores y el servidor sea por TCP/IP es condición suficiente. Si se desea obtener acceso desde cualquier sitio deberá especificarse que el servidor sea de tipo Web, independientemente de la conexión entre los controladores y dicho servidor.

Si se desea simplificar el cableado o no tener que mantener más que una red cableada en la empresa, la alternativa es el conexionado TCP/IP.

Supongamos una empresa que posee una fábrica en Salta y oficinas en Córdoba y pretende obtener reportes del sistema de control de accesos de la fábrica desde sus oficinas. En este caso será imposible utilizar un software stand alone, así que el análisis se concentrará en las otras dos modalidades.

- **Situación 1:** La empresa no posee una red corporativa que vincula ambos sitios. Para obtener un costo de operación bajo se decide utilizar Internet como vínculo. En ese caso será necesario colocar un sistema de control de accesos de tipo servidor Web en la fábrica y publicarlo en Internet. Así, desde cualquier parte del mundo será posible acceder al sistema, independientemente que los controladores que manejan los accesos de la fábrica se comuniquen con el servidor por TCP/IP o RS-485. Al no existir una red corporativa, agregar un controlador de accesos en la oficina de Córdoba no será sencillo aunque éste tenga interfase TCP/IP.

- **Situación 2:** La empresa posee una red corporativa que vincula ambos sitios. En este caso será conveniente el uso de controladores con interfase TCP/IP, de esta forma se podrá crecer dentro de la red lógica, independientemente de la ubicación física, de manera transparente. Si el software está organizado de manera cliente servidor o servidor Web, dependerá más de la política del departamento de informática que de una cuestión técnica, dado que ambos estarán accesibles desde en la intranet. ■