

# Interacción, otras funciones posibles y relación con el CCTV

**Ing. Luis Cosentino**

Consultor Independiente  
lcosentino@fibertel.com.ar



En el número anterior terminamos con la descripción técnica de los controles de accesos, tanto desde el punto de vista de las placas controladoras como desde su interconexión y el software que los manejan. En este capítulo hablaremos de la interacción de los controles de acceso con otras áreas, relacionadas o no con la seguridad electrónica.



## ■ 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 - RNDS N° 52

Software de los sistemas de control de accesos

### Capítulo 9

Interacción del control de accesos con CCTV

9.1. Distintas aplicaciones

9.2. Grados de integración

### Capítulo 10

Otras funciones posibles con un control de accesos

10.1. Ejemplos

### Capítulo 11

Comparaciones y relaciones del control de acceso con otras disciplinas o aplicaciones

11.1. Control de Acceso vs. Presentismo / Tiempo y asistencia

11.1.1. Etapas

11.2. Relación con la seguridad física.

11.3. Relación con el CCTV

## Capítulo 9

### Interacción del control de accesos con CCTV

La tendencia actual en seguridad electrónica, como en casi todas las otras actividades relacionadas con informática, apunta a poder integrar la mayor cantidad de funciones bajo el mismo sistema/programa. En este caso la tendencia actual es poder manejar todas las áreas de la seguridad electrónica (Control de Accesos, CCTV, Intrusión e Incendio) desde la «misma pantalla».

Esto presenta dos ventajas intuitivas: por un lado sólo es necesario aprender a manejar un único programa, lo cual facilita la operación y la formación de operadores; y por el otro, en la misma pantalla puede obtenerse información sobre el estado de todos los sistemas, evitando así tener que operar múltiples sistemas desde múltiples computadoras.

Como se mencionó, este hecho por sí mismo justifica la integración del control de acceso con el resto de áreas de la seguridad electrónica. Pero la integración con el Circuito Cerrado de Televisión (CCTV) permite resolver problemáticas de control de accesos que de otra forma no podrían ser bien resueltas.

Muchas veces se necesita controlar el acceso a una puerta que comunica con el exterior. Estas puertas suelen estar construidas con materiales que no permiten ver con claridad desde el interior quien o quienes están del lado de afuera intentando acceder. En estos casos, disponer de una cámara para poder observar lo que está sucediendo en el exterior es fundamental. Cabe preguntarse, entonces, como debería ser esa integración.

La primera solución, y más económica, sería colocar un portero eléctrico. Esto no ofrece ningún nivel de integración y si bien ahora será posible poder ver con ciertas limitaciones del otro lado de la puerta, la solución es sólo parcial, dado que no se estaría dejando un registro de las imágenes sino que sólo se estaría mirando una muy pequeña porción de imagen del exterior, no pudiendo evitar la intrusión cuando una persona aproveche la apertura de la puerta para forzar el ingreso.

Una solución integrada más apropiada descarta el uso de una cámara de baja calidad y poca resolución (como las de los porteros eléctricos) e incluye al menos dos cámaras exteriores, una para observar con

Continúa en página 172

Viene de página 168

detalles a la persona que se está identificando y otra para tener un panorama general del exterior, y al menos una cámara interior para tener una imagen panorámica de lo que sucede cuando esa persona ingresa.

Además, sería deseable almacenar la información de esas cámaras al menos 10 segundos antes y hasta 30 segundos después del ingreso, para poder recrear los acontecimientos en el caso que se produzca algún evento y que esto quedase vinculado con el evento del sistema de control de acceso.

Esta combinación de control de acceso, imágenes y grabación es lo que se denomina «ingreso con video asistido» y se lo utiliza -por ejemplo- en accesos a depósitos no atendidos.

Una explicación más detallada supone que quien desea ganar acceso presenta su tarjeta en el lector externo del depósito. El sistema reconoce la tarjeta y llama la atención del operador del control de accesos, que puede encontrarse físicamente a varios kilómetros de distancia, presentándole los datos almacenados de esa tarjeta en la base de datos con la correspondiente foto y, al mismo tiempo, le presenta las imágenes en vivo de dos cámaras del lugar: una que toma el primer plano de la persona y otra que toma la panorámica del exterior. Una vez que el operador verifica las condiciones de ingreso, procede a abrir la puerta en forma remota o denegar el acceso. El sistema de control de acceso dejará registrado el ingreso y mantendrá un vínculo con la videograbadora que registró las imágenes para poder recrear lo sucedido cuando sea necesario.

### 9.1. Otras aplicaciones

Hay otras aplicaciones en las cuales la integración del control de acceso con el CCTV es muy útil. Por ejemplo:

- La entrada/salida de socios de un country. En esos casos, en general, cuando un socio/propietario presenta su tarjeta, la barreira se abre permitiéndole el acceso. Los sistemas que no integran video no permiten registrar lo sucedido y por lo tanto, si en lugar de ser un socio es otra persona quien maneja el vehículo, no quedará registro de lo sucedido.

- Cuando se utilizan tarjetas para fichar el ingreso y egreso de una fábrica con fines de control horario. En esos casos puede colocarse una cámara justo encima del lector para poder grabar la imagen de quien presenta la tarjeta frente al lector. Se necesita un vínculo entre el control de acceso y el CCTV para poder correlacionar rápida y fácilmente la imagen con el registro del control de acceso. Si bien esta integración de video con control de acceso es relativamente reciente, existen equipos en el mercado que ofrecen estas prestaciones y se los encuentra en toda la gama de prestaciones/precios.

### 9.2. Grados de integración

Al hablar de integración de sistemas podemos mencionar diferentes grados de integración. Desde el punto de vista teórico deben analizarse dos formas extremas de integración, desde los sistemas denominados sistemas «débilmente integrados» hasta los «fuertemente integrados».

Se dice que dos o más sistemas son «débilmente integrados» cuando su integración es a nivel de contactos, es decir que se utiliza una salida de un sistema para accionar una entrada del otro. De esta forma se obtiene, a lo sumo, un grado de sincronización de eventos pero no es posible intercambiar información más detallada.

Se dice que dos o más sistemas son «fuertemente acoplados» cuando estos comparten protocolos comunes que les permiten comunicarse mediante el intercambio de información y/o comandos.

En el primer caso, y volviendo a nuestro ejemplo, será posible utilizar un contacto de salida del control de accesos para activar

una entrada de alarma de la videograbadora con el objeto de almacenar las imágenes por un tiempo dado a partir de que se detecte el paso de la tarjeta frente a la lectora. En el segundo método, el hecho de poder intercambiar información permite que el control de acceso no solo guarde un registro donde se indique en que porción del disco se grabó la información de video correspondiente al momento que se paso la tarjeta, sino que incluso podrá enviar un comando a la grabadora para aumentar la calidad de imagen y la cantidad de cuadros por segundo mientras dure el acceso video asistido.

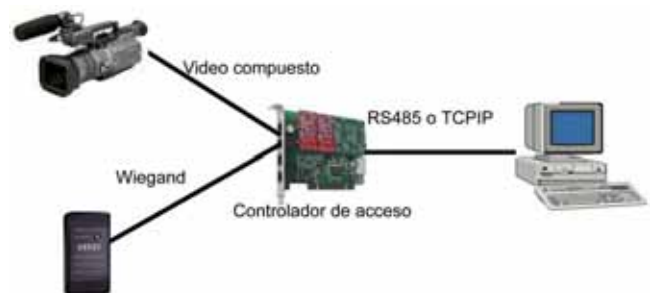
Cuando se necesite recuperar la información almacenada, en el primer caso deberá ubicarse el registro del evento que desea analizarse en el sistema de control de accesos, del cual se obtendrá fundamentalmente la fecha y hora, las que se utilizarán como clave de búsqueda en la videograbadora para localizar las imágenes correspondientes. Asumiendo que ambos relojes están suficientemente bien sincronizados se podrá recrear la situación.

En el segundo caso y dado que la integración es total, en la misma pantalla se obtendrá tanto la información del acceso como las imágenes grabadas.

Dentro de los sistemas de control de accesos que integran video pueden encontrarse dos tipos maneras de integración: aquellas cuyas placas poseen entradas de video compuesto y aquellas que integran video ya digitalizado utilizando el protocolo TCP/IP.

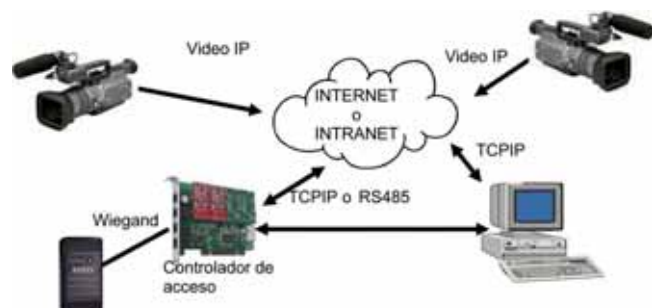
Las ventajas del primer método es que puede utilizarse cualquier cámara tradicional analógica, pero hay que cablearla hasta el controlador de control de accesos y, si se desea grabar el video, también hay que cablear hasta la grabadora.

#### Integración a nivel Hardware



El segundo método, si bien utiliza cámaras de mayor prestación (cámaras IP) y consiguientemente de mayor costo, la comodidad del cableado y las prestaciones superiores justifican la mayor inversión, dado que por medio del protocolo TCP/IP no sólo pueden conectarse cámaras sino que también pueden conectarse videograbadoras, encoders, etc. Desde el punto de vista de la instalación, sólo hay que cablear las cámaras hasta la boca de red más cercana.

#### Integración a nivel TCP-IP



Continúa en página 176

Viene de página 172

**Capítulo 10**

Otras funciones posibles con un control de accesos

Como mencionamos en el capítulo anterior, la integración con las otras áreas de la seguridad electrónica nos permite ofrecer una funcionalidad mayor que atienda a las necesidades de seguridad de nuestros clientes. El tema de este capítulo está relacionado con funciones que generalmente son de otra área, que no corresponde específicamente a la seguridad y se trata de algunos controles simples y automatismos menores, que pueden ser realizadas por los controles de accesos, evitando así tener que colocar PLC's u otros equipos ad-oc con las ya mencionadas desventajas de los sistemas no integrados.

Estos controles simples podrían ser considerados como funciones elementales de domótica, pero de ninguna manera se pretende decir que es posible resolver el control inteligente de edificios con las funciones adicionales que poseen los sistemas de control de accesos.

Desde el punto de vista comercial, no es muy frecuente que los clientes soliciten este tipo de prestaciones en una cotización de un control de accesos, simplemente porque no se imaginan que se pueden resolver con los mismos equipamientos. Es por eso que proactivamente podemos ofrecer algunas de estas prestaciones que pueden implementarse con un bajo costo adicional e incrementar el valor agregado de nuestros servicios.

**10.1. Ejemplos**

Según sea la aplicación pueden citarse los siguientes casos:

**Industriales o corporativas**

- La sirena de aviso de cambio de turno en una fábrica
- Controles de iluminación rudimentarios (desactivación del circuito de iluminación de la administración en horarios nocturnos, activación de la iluminación exterior en determinados horarios, etc).
- Utilización de entradas para monitorear a que hora se abren ciertos ficheros.

**Profesionales o comerciales**

- Manejo de la iluminación exterior o de la vidriera
- Activación forzada de la alarma a una determinada hora

**Ingresos vehiculares**

- Lógica de manejo de aperturas y cierres de barreras mediante detectores de masa metálica o barreras infrarrojas.
- Manejo de semáforos
- Manejo de sirenas y luces.

**Residenciales**

- Manejo de la iluminación exterior o refuerzo de iluminación interior en determinadas bandas horarias.
- Activación/desactivación de riego por aspersión, filtros de pilas, etc.

Para implementar estas aplicaciones será necesario que el control de accesos elegido permita combinar sus entradas y salidas con funciones de programación, temporizadores, bandas horarias etc., para poder implementar lógicamente la secuencia necesaria, y deberán colocarse las interfases adecuadas para poder manejar los niveles de potencia requeridos a partir de bajas señales, que es lo que entregan la mayoría de los controles de accesos.

Este tipo de prestaciones no sólo se encuentra en los controles de accesos de gran porte sino que muchos de pequeño y medio porte también. Lo que varía de equipo en equipo es la forma en que se programan las mismas, pero en general vinculan una salida con los estados de las entradas, las bandas horarias y alguna condición de acceso.

Supongamos que deseamos sonar una sirena en una fábrica anunciando los cambios de turno, que se producen a las 8:00 y a las 17:00 de lunes a viernes y a las 13:00 los sábados, y se preten-

de activar una sirena durante 15 segundos.

Deberá definirse una banda horaria llamada «cambio de turno» que se active de lunes a viernes de 8:00 a 8:01 y de 17:00 a 17:01, los sábados de 13:00 a 13:01 y que no se active los domingos. Lo que haremos es conectar una sirena a la «salida disponible 1» del control de acceso, teniendo la precaución de verificar que la tensión y corriente que la sirena necesita para funcionar correctamente puedan ser provistas por la «salida disponible 1» del control de acceso. En caso contrario, deberá colocarse un relé de paso y definir una función que active dicha salida durante 15 segundos toda vez que se active la banda horaria «cambio de turno».

Acciones más complejas requerirán programaciones complicadas, pero con la información del manual y el soporte del fabricante siempre es posible realizarlas.

**Capítulo 11**

Comparaciones y relaciones del control de acceso con otras disciplinas o aplicaciones

**11.1. Control de Acceso vs. Presentismo / Tiempo y asistencia**

Hasta ahora hemos hablado de control de accesos, pero en una gran cantidad de casos lo que nuestro cliente en realidad quiere es un control horario además del control de accesos.

Muchas veces se confunden los términos y se asume que es lo mismo, pero en este apartado trataremos de ver que es un control horario y cual es su relación con el control de accesos.

Como punto de partida, el control horario tiene un objetivo completamente diferente del control de accesos, dado que no pretende aceptar o impedir el ingreso de una persona sino registrar a que hora se produjo el mismo. Tanto es así que los controles de accesos poseen una lista blanca de personas habilitadas para ingresar por determinada puerta mientras que los relojes de personal, como se denominan a las terminales de control de presentismo, poseen una lista negra de personas que no deben registrar su ficha.

Los relojes de personal, de acuerdo con las leyes laborales, necesitan mostrarle al usuario en un display la fecha y la hora a la cual están efectuando el registro mientras que los controles de accesos no necesitan tener displays en los lectores.

Para el control horario, una hora de permanencia en la empresa no siempre significa lo mismo, mientras que para el control de accesos sí. En otras palabras, un empleado cuyo horario de trabajo es de 8:00 a 18:00, desde el punto de vista del control de accesos podría no tener inconvenientes en ingresar a las 7:00. Pero desde el punto de vista del control horario, dado que la hora de 7:00 a 8:00 podría ser considerada como una hora extra trabajada.

En general, el proceso de liquidación de sueldos consta de las siguientes etapas

- Registro de las horas efectivamente trabajadas
- Clasificación de esas horas según las políticas laborales de la empresa
- Cálculo del salario básico
- Cálculo del salario real a partir de otros beneficios, aportes y descuentos.

**11.1.1. Etapas**

A modo de ejemplo explicaremos cada una de las etapas, sin que esto deba considerarse como una regla.

El registro de las horas efectivamente trabajadas es lo que hace el control de accesos cuando la persona se identifica mediante -por ejemplo- su tarjeta de proximidad. Esta etapa del proceso es efectuada con el objetivo de registrar el momento en que sucede y eventualmente activar o no alguna puerta que permita el ingreso a la fábrica o a determinado sector. Para que esto sea

Continúa en página 180

Viene de página 176

cumplido de manera fehaciente la puerta en cuestión debería tener una lectora para registrar/abrir la entrada y otra para la salida. De esta forma es simple solicitar un reporte al control de accesos, indicando como hora de ingreso la que corresponde a la lectora de entrada y hora de salida la que corresponde al lector de salida. Se recomienda quitar el picaporte de esa puerta para evitar que las personas puedan retirarse olvidándose de presentar su tarjeta. Algunos controles de accesos permiten generar un reporte que es útil cuando solo se coloca una lectora para abrir y cerrar la puerta, que consiste en considerar que el primer evento válido del día de una tarjeta es considerado como su ingreso y que el último del día es considerado como su salida. Si bien en muchos casos se utiliza este método, la realidad indica que es menos seguro que el de colocar dos lectoras.

Una vez generado el reporte de horas de un empleado, deben aplicarse las políticas laborales de la empresa. Por ejemplo, suponiendo que los ingresos y egresos de diferentes días se producen a de 7:53 a 17:02, 8:02 a 19:40, etc. En ese caso la política laboral de la empresa puede establecer que toda diferencia en más o menos hasta 30 minutos será desconsiderada, por eso una vez filtrado el reporte original los horarios serán redondeados y quedarán como 8:00 a 17:00 y 8:00 a 19:30.

Una vez efectuada esta primera tarea, deben interpretarse las horas trabajadas, identificando cuales son normales y cuales son extras. Por ejemplo, la política de la empresa dice que el empleado puede trabajar hasta 3 horas extras por semana y que su horario normal es de 8:00 a 17:00. Una vez aplicado este segundo criterio, quedará registrado que se cumplió correctamente con las horas trabajadas del primer día y que se acumuló 1 hora y media extra en el segundo. Al momento de efectuar la liquidación de la semana, deberá verificarse que la suma de horas extras no supere las 3, que es el máximo permitido por la empresa.

Una vez elaborado este reporte se procede al cálculo del salario básico, tomando la cantidad de días y horas trabajadas y calculando, según el importe por hora de trabajo, el importe a percibir. En esta etapa se tendrá en cuenta que días y horarios se efectuaron las horas extras para saber si se las debe pagar al 50% o al 100%.

Por último, se calcula el salario real teniendo en cuentas las leyes laborales vigentes, premios, incentivos, salarios familiares, etc.

Como puede verse, el concepto de presentismo es completamente diferente al de control de acceso, que solo puede entregarle al departamento de recursos humanos un listado indicando las horas en las cuales el empleado pasó su tarjeta por el lector o registró su huella en el equipo.

### 11.2. Relación con la seguridad física.

Esta es una discusión que poco a poco va desapareciendo. Hace unos pocos años, las empresas de seguridad física, y fundamentalmente quienes las dirigían, no siempre confiaban en la seguridad electrónica. Era bastante común escuchar decir que «los sistemas fallan», lo que era igualmente cierto pero no se escuchaba que «los hombres también».

Una explicación podría ser que los fabricantes de productos de seguridad electrónica no invirtieron lo suficiente en la formación de la porción del mercado que «utilizaba» sus productos. Es bastante común ver como las empresas líderes del mercado de seguridad electrónica periódicamente dictan cursos de diseño e instalación de sus equipos. Pero es muy raro ver que se dicten cursos de operación de los mismos para los usuarios. En otras palabras, existe oferta de cursos para los integradores e instaladores pero no para los vigiladores u operadores de seguridad.

A pesar de ello, las empresas de seguridad física lentamente fueron incorporando productos de seguridad electrónica. Algunas veces porque las utilizan para su propio control interno, como el

control de rondas, o porque facilitan y perfeccionan su trabajo.

Desde el punto de vista estrictamente técnico los sistemas profesionales de seguridad electrónica no aumentaron su confiabilidad: Lo que sucedió es que poco a poco se fue entrenando a quienes los instalaban y operaban, obteniéndose así un resultado aparente similar. Sin embargo, actualmente hoy los sistemas fabricados por amateurs (de muy bajo costo y por ende baja calidad) y aquellos instalados por personal no capacitado son los que continúan alimentando el viejo estigma.

La seguridad electrónica aporta a la seguridad física dos cosas: la capacidad de señalar eventos para que se tomen las acciones necesarias y evitar así delitos o daños - tal es el caso de CCTV y de las centrales de robo y/o incendio- y la capacidad de auditoría que permite analizar «objetivamente» los hechos una vez que se produjeron.

Cuando se analiza la interacción del control de accesos con la vigilancia física es evidente que el control de accesos es el encargado de entregar la información que el vigilador necesita para tomar las decisiones adecuadas.

Supongamos el ingreso a una fábrica: toda vez que quien pretende ingresar presenta su tarjeta, el control de accesos obtiene de su base de datos la foto asociada y se la presenta al vigilador en la pantalla, dado que será éste quien deberá impedir el acceso, si es que decide que hay alguna inconsistencia entre la información almacenada y la persona que está ingresando.

Otro ejemplo indica que toda vez que se abre una puerta con una tarjeta válida, sólo un vigilador será quien impida que ingresen varias personas.

Si tomamos el ejemplo del ingreso a los countries, lo más frecuente es que los vigiladores anoten en una planilla los datos de los visitantes y contratistas que ingresan al mismo. Esta información así registrada es muy difícil de procesar mientras que si se cargase en un control de accesos, la próxima vez que dicha persona se presente, el vigilador no sólo tendrá sus datos ya cargados sino que podrá ver otra información estadística que le ayude a tomar la decisión de permitir el ingreso. Por ejemplo, cuando fue la última vez que ingresó, si tiene algún comentario por su comportamiento, multas, etc. a la vez que hace que el ingreso sea más rápido. En resumen, el sistema manual no colabora con la seguridad, dado que el vigilador no tiene información previa sobre el visitante y debe pasar más tiempo escribiendo los datos que cumpliendo su real misión, que es la de verificar que todo esté en correcto orden.

### 11.3. Relación con el CCTV

Con frecuencia los usuarios finales consideran a las cámaras y sistemas de CCTV como los elementos «modernos» de seguridad, cuando en realidad no siempre son los elementos adecuados para resolver sus problemas.

Si bien analizando las funciones básicas de cada uno de ellos resulta difícil encontrar los puntos en los cuales uno podría ser reemplazado por el otro, hay un par de cuestiones que son significativas. La primera que puede mencionarse es que el control de accesos se utiliza para impedir o no el acceso a determinada área, podríamos decir que es preventivo y on line, mientras que el CCTV tradicional se organiza en función de las imágenes grabadas y, por lo tanto, podríamos decir que su función es eminentemente «post mortem».

Cuando se lo analiza desde el punto de vista del mantenimiento o la falla, diríamos que si un control de accesos falla, en general la puerta que falla no se puede abrir o no se puede cerrar, lo cual motiva una reparación inmediata. En el caso de CCTV, en cambio, si una cámara o DVR falla, simplemente se pierde ese recurso pero no se afecta el normal flujo de personas y/o tareas. ■