

## **Los controles de Acceso Físico en el Sector Residencial de Colombia.**

**Autor:**

CESAR AUGUSTO GARZON LOAIZA

CURSO 38

**REPUBLICA DE COLOMBIA**  
**UNIVERSIDAD MILITAR NUEVA GRANADA**  
**FACULTAD DE RELACIONES INTERNACIONALES ESTRATEGIA Y**  
**SEGURIDAD**  
**ESPECIALIZACION EN ADMINISTRACION DE LA SEGURIDAD**

**Los controles de Acceso Físico en el Sector Residencial de Colombia.**

Trabajo de Grado como requisito para optar al grado de  
Especialista en la Administración de la Seguridad

**Autor:**

CESAR AUGUSTO GARZON LOAIZA  
CURSO 38

**Asesor o Tutor:**

DR.JULIAN ANDRES PUENTES B.

Bogotá D.C

Abril de 2013

**Nota de aceptación del trabajo de grado:**

---

---

---

---

---

**Jurado:**

---

---

## INDICE GENERAL

<b>RESUMEN.....</b>	<b>5</b>
<b>INTRODUCCION.....</b>	<b>8</b>
<b>CLASES DE SISTEMAS DE CONTROL DE ACCESO.....</b>	<b>9</b>
<b>Sistemas biométricos.....</b>	<b>10</b>
<b>Control de Acceso Autónomo.....</b>	<b>11</b>
<b>Control de Acceso con Software.....</b>	<b>12</b>
<b>UTILIDADES DE IMPLEMENTAR EL CONTROL DE ACCESO DE PERSONAS.....</b>	<b>15</b>
<b>QUE CONTROL DE ACCESO ES MAS SEGURO PARA EL SECTOR RESIDENCIAL.....</b>	<b>17</b>
<b>CONCLUSIONES.....</b>	<b>19</b>
<b>BIBLIOGRAFIA.....</b>	<b>21</b>

**UNIVERSIDAD MILITAR NUEVA GRANADA**  
**FACULTAD DE RELACIONES INTERNACIONALES ESTRATEGIA Y**  
**SEGURIDAD**  
**ESPECIALIZACION EN ADMINISTRACION DE LA SEGURIDAD**  
**TRABAJO DE GRADO**

**Los controles de Acceso Físico en el Sector Residencial de Colombia.**

Autor: Cesar Augusto Garzón Loaiza

Tutor: DRA. JULIAN ANDRES PUENTES B.

Fecha: Abril, 2013 \_\_\_\_\_

**-RESUMEN-**

La alta rotación de vigilantes en el sector residencial, ha generado riesgos de intrusión, los cuales pueden ser disminuidos con los sistemas de control de acceso, que desde el punto de vista técnico, son todos los dispositivos para controlar, comprobar, identificar y permitir el paso de personas, vehículos u objetos a un área de seguridad para prevenir riesgos sobre las personas, objetos e instalaciones, definición dada en su libro Manual para el Director de Seguridad, quinta edición, 2009, del Consultor Manuel Sánchez Gómez Mérelo.

Los “tipos de accesos”, son clasificados en dos categorías, así: **Accesos físicos y Accesos Virtuales**. También se subdividen según la lectora utilizada y que contemplaremos mas adelante.

Los controles de acceso son de gran importancia en copropiedades que carecen de presupuesto para un servicio de vigilancia con hombres, por cuanto representa una erogación anual de no menos de \$66´000.000, por servicio.

## INTRODUCCION

Dentro del presente documento describiremos las diferentes clases de controladoras de acceso de acuerdo a las lectoras existentes como son de tarjeta de banda magnética y de proximidad, de códigos, biométricas entre otros tipos y como sirven para en el mejoramiento de los niveles de seguridad de las copropiedades en Colombia.

La seguridad física requiere cada día de un mejor control de personal que ingresa a cualquier instalación, garantizando que los flujos de personal sean los debidamente autorizados para su desplazamiento entre varias dependencias internas ayudando a controlar los niveles de seguridad de cada unidad residencial. La implantación de los controles de acceso bien administrados y parametrizados son cada vez mas importantes en el desarrollo de proyectos de congregación de multitudes y en especial en el sector residencial bajo el Régimen de Propiedad Horizontal en Colombia ley 675 de 2001.

Dentro de la experiencia profesional del autor se han encontrado que parte de la inseguridad en los sectores residenciales de Colombia se genera en la falta de un control de acceso a la copropiedades y de movimiento de personas en el interior de la misma, originado en el desconocimiento de los residentes debido a la alta tasa de rotación de personal en el sector de la vigilancia privada.

Aunque el Protocolo de Seguridad en el Sector Residencial expedido por la Superintendencia de Vigilancia y Seguridad Privada el pasado 9 de mayo del año 2.011 exige tener un listado actualizado de residentes,<sup>1</sup> esto en la práctica muchas veces no se cumple, por cuanto el administrador no alcanza

---

<sup>1</sup> Superintendencia de vigilancia y seguridad privada, Protocolo de operación: servicio de vigilancia y seguridad privada física – sector residencial. 9 de mayo de 2011.

a tener actualizado dicho documento, debido entre otras razones a que los mismo residentes se niegan a dar sus datos personales a los administradores, lo que permite se desactualicen dichos listados. Lo anterior, sumado al cambio frecuente de vigilantes genera que se pierda el conocimiento de los encargados del control de acceso, por cuanto no alcanzan a conocer de vista a todos los residentes cuando ya son cambiados del servicio.

A diario se encuentra personal deambulando en áreas y sitios donde pueden afectar propiedades privadas, equipos e instalaciones de áreas comunes, y lugares donde se puede presentar accidentes, que generan en demandas para la misma copropiedad y frente a los cuales se implementa rondas con vigilantes que aumentan los costos sin ser efectivos. Este esquema con vigilantes se podría reemplazar un control de acceso apropiado, automático y bien parametrizado, obteniendo mejores resultados, debido a que no se depende de la memoria y capacidad de retentiva de un vigilante con sus limitaciones propias de la naturaleza humana, y el riesgo por rotación del mismo.

Los controles de acceso permiten el flujo efectivo y seguro de grandes masas de personas, ayudando a controlar internamente los movimientos de personal en las áreas autorizadas o no.

Por lo tanto en el presente documento se entrará a conocer las diferentes clases de controles de acceso automático, pasando por los más sencillos como las tarjetas y/o claves de acceso, y llegando hasta los más modernos de tipo biométrico. De igual manera, se presentará el funcionamiento de estas controladoras de acceso de manera general, apoyada en bases de datos previamente configuradas a la implementación.

Al final recomendaremos el tipo de controladora de acceso más conveniente por costo y seguridad para las copropiedades, el cual será complemento y

apoyo a la vigilancia humana a la hora de permitir el acceso de las personas a un conjunto o edificio residencial. Sin embargo, el uso de las controladoras de acceso, se podrían complementar de mejor manera si se utiliza un vigilante o si por razones presupuestales no se pueda contratar vigilancia fija, se podría pensar en manejar accesos e forma de exclusas.

Recomendaremos como en edificios residenciales importante es tener el registro histórico exacto de tiempos y áreas de ingreso y salida de todas las personas que habitan, visitan o trabajan en conjuntos o edificios residenciales. Así como también, los intentos del personal de ingresar a sitios restringidos, descubriendo posibles intentos de intrusión, hurto o daños de propiedad privada.



## CLASES DE SISTEMAS DE CONTROL DE ACCESO

Para entrar a mirar las clases de control de acceso existentes, hablaremos de los componentes del mismo como lo son los paneles controladores que pueden interactuar entre si, el software de administración y los periféricos como chapas o cerraduras, sensores y elementos de identificación.

Estos pueden ser de acuerdo a su complejidad autónomos, es decir que no tienen un canal de comunicación directo con un puesto de control, y centralizados, cuando cuentan con una serie de equipos comunicados con un puesto de control del edificio o conjunto.

Lo que hace un control de acceso es autenticar a la persona que pide ingresar permitiéndole su ingreso siempre y cuando esa persona entregue o demuestre ser una de las personas registradas previamente en una base de datos.

Ahora bien que es la autenticación, esta se define como la verificación de que el usuario que trata de identificarse es válido o es el real.

Hay cuatro clases de técnicas que permiten autenticar la identidad de un usuario, estas clases de técnicas se pueden usar individuales o combinadas<sup>2</sup> :

1. Algo que solamente el individuo conoce: por ejemplo una contraseña.
2. Algo que la persona posee: por ejemplo una tarjeta magnética.
3. Algo que el individuo es y que lo identifica unívocamente: por ejemplo las huellas digitales.

---

<sup>2</sup> [www.rnd.com.ar](http://www.rnd.com.ar), Ing. Luis Consentino consultor independiente. [consentino@fibertel.com.ar](mailto:consentino@fibertel.com.ar). Modelo EASI. Protección en profundidad.

4. Algo que solo el individuo es capaz de hacer: por ejemplo los patrones de escritura.

La fortaleza de la autenticación es mayor mientras más factores se adicionen, generalmente solo se utilizan hasta 3 factores:

- 1 factor = contraseña
- 2 factores = contraseña + token
- 3 factores = contraseña + token + biometría
- 4 factores = contraseña + token + biometría + localización geográfica (GPS)
- 5 factores = contraseña + token + biometría + localización geográfica + perfil de usuario

A continuación mostraremos los sistemas de acceso más importantes de acuerdo al tipo de lectora que se instale, así:

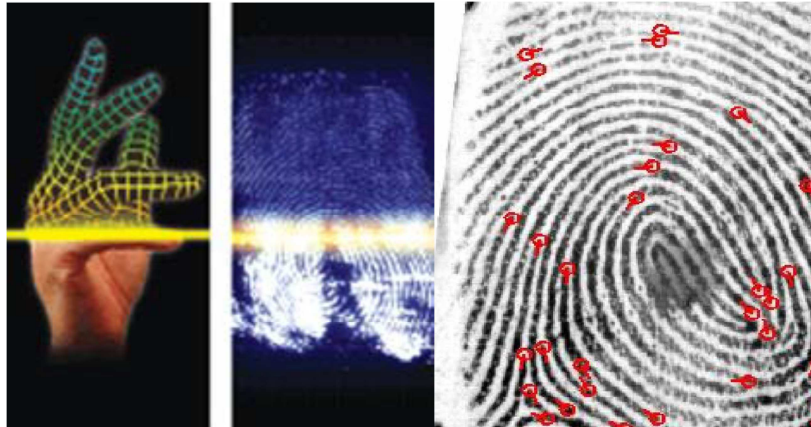
### **Sistemas biométricos**

Explicaremos el término biometría que es una tecnología que realiza mediciones en forma electrónica, guardando y comparando las características únicas para la identificación de las personas.

Mediante el almacenamiento en una base de datos de las características físicas de las personas y su posterior comparación se logra identificar las personas que coinciden con los datos almacenados. Estos lectores biométricos pueden identificar personas al establecer los patrones propios de manos, huellas digitales y voz.

En este tipo de lectora que mediante previo registro de características del ser humano las confronta y valida logrando individualizar e identificar al usuario de este sistema, sea por lectora de huellas, morfología de rostro o manos,

identidad de iris, o la suma de todas las anteriores características, dando una autorización de ingreso.



Ilustraciones de revista de negocios de seguridad. Buenos aires argentina.  
Director Claudio Marcelo Alfano Numero 64 oct/nov de 2011.

### **Control de Acceso Autónomo**

Las lectoras de Password / teclas son las mas utilizadas por su bajo costo, pues con una base de datos previa donde se registra el tipo de usuarios y sus contra señas, confronta la información de cada usuario almacenada en la base de datos, con la información de la persona que desea ingresar generando en caso positivo una apertura de puerta, ya sea por apertura de electro imán, cantonera eléctrica o talanquera, permitiendo el ingreso.

De manejo muy similar al anterior tipo de lectoras, son las lectoras de tarjeta de proximidad, la cual identifica por cercanía de 0 a 80 centímetros y de acuerdo a las necesidades del equipo, dejando registro de hora y fecha en el sistema y con la ayuda de una base de datos determinará y relacionara los datos correspondientes al usuario de la mencionada tarjeta.

Tiene una limitante en el almacenaje de eventos, que el computador puede tener por mucho mas tiempo ese record de todas la controladoras de acceso.

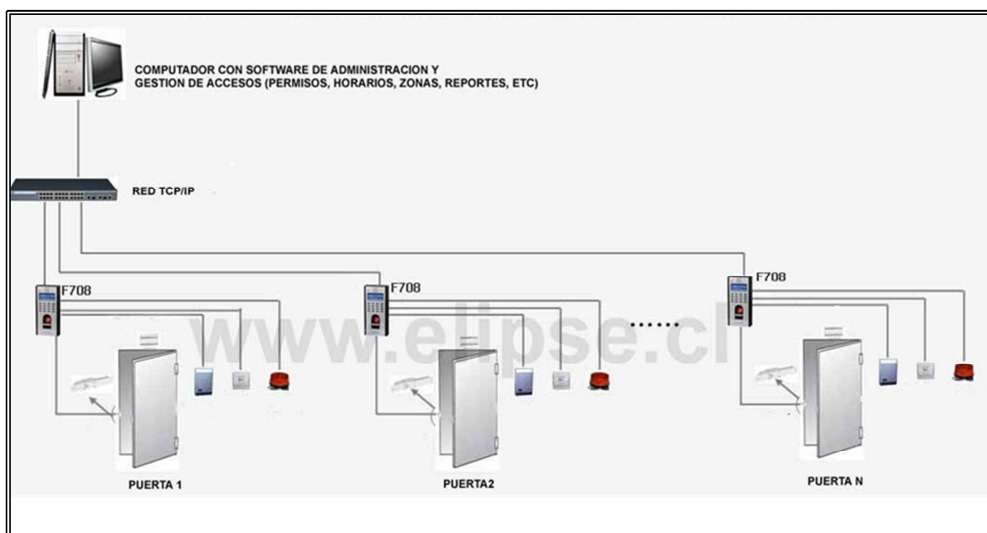


Ilustraciones de revista de negocios de seguridad. Buenos aires argentina.  
Director Claudio Marcelo Alfano Numero 64 oct/nov de 2011.

### **Control de Acceso con Software**

Maneja lectoras de cualquier tipo, proximidad, código, biométrico, etc, pero desde un computador con un software de administración de todas las puertas que reciben la orden de apertura lo hagan plena verificación de identidad de

la persona que va a entrar, facilitando dejar un registro de la persona que abrió la puerta.



Ilustraciones de revista de negocios de seguridad. Buenos aires argentina.  
Director Claudio Marcelo Alfano Numero 64 oct/nov de 2011.

Dentro de estos últimos existen dos sistemas uno que constantemente confronta su lectura con una base de datos en un computador, para hacer verificación de identidad y permitir accesos, lo que de ser muchos equipos haciendo la consulta de manera simultánea hace al sistema algo lento en su respuesta. Y otro sistema donde cada equipo tiene su propia base de datos y hace su verificación de manera independiente y solo reporta su movimiento al puesto de control que registra cada operación.<sup>3</sup>

Mencionaremos algunos tipos de credenciales que sirven para identificar y diferencias a cada usuario del sistema de control de acceso, así:

<sup>33</sup> Manual para el Director de seguridad, Manuel Sánchez Gómez Merelo, Madrid, España, ET Estudios Técnicos S.A.

Credencial Material: Llave mecánica, llave eléctrica, llave electrónica, llave magnética, llave mixta (mecánica electrónica, tarjeta con código o chip electrónico, tarjeta mecánica, tarjeta holográfica, tarjeta de código magnético, tarjeta de código capacitivo, tarjeta de código óptico, tarjeta de código electrónico, tarjeta mixta, emisor de radiofrecuencia, emisor de infrarrojos y emisor de ultrasonidos.

Credencial de conocimiento: teclado digital, cerradura de combinación y escritura.

Credencial Personal: Huella Dactilar, voz, geometría de la mano, rasgos faciales e iris del ojo. <sup>4</sup>

De otro lado el acceso de personas residentes o visitantes en vehículos hace que igualmente se deba implementar un control de acceso para estos. En este sistema de control se debe tener como parámetros a seguir:

Asociación de las matriculas o número de placas a la imagen del vehículo y la del conductor.

Asociación del vehículo con la base de datos de los vehículos autorizados por cada conductor.

Asociación con un código tarjeta, chip o control remoto de proximidad.

Comprobación de fecha, hora, en la que el vehículo y su conductor tienen acceso.

---

<sup>4</sup> Manual para el Director de seguridad, Manuel Sánchez Gómez Merelo, Madrid, España, ET Estudios Técnicos S.A.

## **BENEFICIOS DE IMPLEMENTAR EL CONTROL DE ACCESO DE PERSONAS**

Son muchos los beneficios de adoptar un sistema de control de acceso de personas en una copropiedad, entre los que se destacan:

**Controlar el personal autorizado:** Con la implementación del sistema de control y gracias a tener actualizada una base de datos de todo el personal autorizado para ingresar como residente, trabajadores de unidades familiares, trabajadores de administración y visitantes esporádicos, se podrá tener mejor confiabilidad del personal que ingresa al conjunto, por cuanto el procedimiento de identificación y registro se hará de manera más inmediata y segura a que si se hiciera con el método tradicional de tener un hombre vigilante encargado del mismo.

**Mejor grado de confianza:** La implementación del sistema de control de acceso de manera permanente, hace que no se dependa de la memoria o capacidad de retentiva que se tenga por parte de un vigilante, que en cualquier momento puede enfermarse o ausentarse de su trabajo y que para ser reemplazado deberá ser entrenado otro vigilante con un tiempo de entrenamiento que no es inmediato., generando inconvenientes y riesgos de intrusión al conjunto.

**Registro de identidades de personas que ingresan o salen:** Facilita el proceso de ingreso y salida de personas haciéndolo mas ágil y seguro.

Evitar ingreso de personas no autorizadas. El personal de vigilancia puede ser engañado o por su cansancio o distracción puede cometer errores al permitir ingresos de personas ajenas a la copropiedad.

Clasificar y priorizar accesos a determinadas áreas. El control de áreas internas de la copropiedad se puede hacer de una manera más económica y efectiva evitando tener contratado recorredores, que no pueden estar en todas las áreas al mismo tiempo y pueden ser burlados por intrusos.

Registrar horario de entrada salida por áreas determinadas. El permanente control de la operación por parte del sistema hace que se generen reportes de movimientos internos a través de las puertas con controladoras de acceso, informando horas de ingreso y salida así como la identidad de las personas que entraron a ciertas áreas y sus horarios de permanencia o tránsito.

Eliminación de errores: La disminución de los registros manuales de datos hace que igualmente disminuyan los errores de digitación. También disminuye los elementos subjetivos y de complicidad por el personal de vigilancia.

Informar los intentos no autorizados de intrusión: Esta información es importante registrarla por cuanto dará evidencia sobre posibles hechos sospechosos al interior del conjunto y que pueden ayudar en caso de investigaciones generadas por la ocurrencia de siniestros.



## **QUE CONTROL DE ACCESO ES MAS SEGURO PARA EL SECTOR RESIDENCIAL**

No existe un control de acceso que sea 100% seguro, todos tienen algún grado de vulnerabilidad y pueden ser burlados, sin embargo; después de vistos los diferentes tipos de lectoras de acceso, podemos recomendar que se deberá buscar tener un conjunto de controles que dificulte la suplantación, la falsificación y/o la clonación, mediante la combinación no solo de una entrega de documento (tarjeta inteligente), sino adicional una clave de ingreso y un lector biométrico de huella, lo que permite establecer que la persona que ingresa es realmente la que dice ser es y no otra. Pero, esta combinación de tres llaves de ingreso, hace que el ingreso sea algo lento.

De todas maneras el implementar un control de acceso con bases de datos actualizadas de manera constante por parte de la misma copropiedad permite mejorar el nivel de seguridad de la misma, y si se combina con un vigilante fijo, se convierte en la mano derecha del mismo, por cuanto podrá dedicar su tiempo a verificación de otras áreas del conjunto que pueden estar monitoreadas por CCTV.

En aplicación al concepto de seguridad en profundidad, deberá tomarse los puntos de acceso de la copropiedad al exterior y los internos de acuerdo a las áreas que conducen cada uno, en esta forma asignar el tipo de controladora más apropiado.

En relación a los ingresos iniciales a la copropiedad es recomendable asignar un tipo de lectora que exija de entrada una tarjeta de proximidad y un código o pin lo que facilitaría el ingreso rápido de residentes en horas pico.

En ingresos a áreas críticas como las unidades familiares, las controladoras de acceso requerirán al transeúnte de la tarjeta de proximidad y de su huella que ha sido previamente avalada y registrada por el administrador, por lo tanto, cualquier persona que burle el ingreso al conjunto, no podrá acceder a estas áreas restringidas, si no fue visado por el guarda, como un visitante con huella.

De otra parte existen áreas comunes sociales, como salones, gimnasio, piscina, áreas de juego, en las que también se requerirá de instalación de controladoras con tarjeta de proximidad y huella, pero solo las huellas de los residentes, no la de visitantes, que deberán esperar a que un residente les invite y autorice su ingreso.

Con relación a sitios de mantenimiento como cuartos de máquinas, planta eléctrica, subcentrales eléctricas, terrazas o áreas de riesgo de accidente, tendrán accesos controlados no solo con la tarjeta de proximidad sino la huella de personal capacitado y avalado por la administración previamente. Ahora bien, el vigilante recorridor tendrá un acceso con una tarjeta “maestra” que le permitirá acceder a todos los niveles de la copropiedad, apoyando casos especiales como personas extrañas deambulando en áreas restringidas, etc.

De no contarse con el vigilante permanente, el sólo control de acceso puede complementarse con el uso de puertas de acceso tipo exclusiva, es decir que se requiere del paso de dos puertas para ingresar y nunca las dos puertas estarán abiertas de manera simultánea. Cuando en la copropiedad se presente esta última situación descrita se recomienda para las visitas dejar un video citofono externo, para ayudar a identificar desde cada unidad familiar quien va a ingresar y permitir su acceso. Este ultimo sistema de

control de acceso ayudara a bajar los costos de vigilancia fija con hombres, lo cual habíamos enunciado al comienzo del presente documento.

## CONCLUSIONES

Conocida la importancia de las controladoras de acceso en el sector residencial de Colombia podemos encontrar que ayudan a controlar de manera eficiente el flujo de personal externo e interno de cualquier copropiedad residencial

Disminuyen el riesgo de intrusión, al servir de apoyo a la vigilancia donde los vigilantes son rotados frecuentemente, a donde el vigilante no alcance a memorizar ni retener a los residentes que habitan una copropiedad.

Por la situación de alto riesgo que presenta nuestra sociedad, estos controles de acceso deben complementarse con el uso de sistemas de puertas tipo exclusiva, que permiten apertura de dos puertas no de manera simultánea, sino como filtro la una de la otra, así evitar posibles aprovechamientos de intrusión en el momento de ingreso de una persona o vehículo. Los controles de acceso ayudan a disminuir los costos por pérdidas de bienes y servicios que se producen frecuentemente en Colombia, ayudando a mejorar los niveles de seguridad de toda la copropiedad al minimizar el riesgo de intrusión.

El presupuesto y el nivel de seguridad requerido son los factores determinantes para establecer el tipo de opción de sistema de control de acceso que va desde los mas económicos basados en la identificación por tarjeta y claves, hasta los mas sofisticados basados en sistemas biométricos.

## BIBLIOGRAFIA

1. Physical Security: Articles on architectural considerations, access control, perimeter protection, Intrusion detection and alarms, and lock and key control. Asi, reprint series. Arlinton: ASIS, 1992.
2. Electronic Security Systems, autor: Robert Pearson, Editorial Buterworth Heineman, Noviembre 29 de 2006.
3. Titulo Fundamentals of Information Systems Security, autor:David Kim, Michael G. Solomon, Editorial Jones y Bartleth Learning, Noviembre 7 de 2010.
4. Gerencia de la seguridad preventiva, autor: Vallejo Rosero Silvio, Santafé de Bogotá, 1998.
5. [http://www.securitysa.com//digital/2009\\_ach/files/2009\\_access\\_control\\_handbook.pdf](http://www.securitysa.com//digital/2009_ach/files/2009_access_control_handbook.pdf)
6. Titulo: Manual de vigilancia Para Empresas industriales, comerciales y de servicios.Autor\_ Martínez Eduardo, Casado Estrada Jose A., México Trillas, 1985.
7. Titulo: Manual de Proteccion Empresarial, portuaria y Maritima. CigarruisteacT. Rpdrido<f. Buenos Aires: Argentina, Grafica Sur. Seguidadydefensa.com.
8. [www.microcontroladores.pic.com](http://www.microcontroladores.pic.com)

9. [www.rnd.com.ar](http://www.rnd.com.ar), Ing. Luis Consentino consultor independiente.  
[consentino@fibertel.com.ar](mailto:consentino@fibertel.com.ar). Modelo EASI. Protección en profundidad.
10. Título: Manual para el Director de seguridad, Manuel Sánchez Gómez Merelo, Madrid, España, ET Estudios Técnicos S.A.
11. Revista de Negocios de Seguridad. Buenos Aires Argentina. Director Claudio Marcelo Alfano Numero 64 oct/nov de 2011.
12. Artículo: [Seguridad informática. Control de acceso](#) Disponible en: "www.mygnet.com" Consultado: 23 de enero de 2012.
13. Rodríguez Berzosa, Luís. [Control de accesos: De la era mainframe a las PKI](#). Disponible en: "www.mygnet.com". [www,iec.csic.es](http://www.iec.csic.es)



ERROR: syntaxerror  
OFFENDING COMMAND: --nostringval--

STACK:

/Title  
( )  
/Subject  
(D:20130717080959-05'00')  
/ModDate  
( )  
/Keywords  
(PDFCreator Version 0.9.5)  
/Creator  
(D:20130717080959-05'00')  
/CreationDate  
(User)  
/Author  
-mark-