

**LA IMPORTANCIA DEL FACTOR HUMANO EN LOS PROCESOS DE
CONTROL DE ACCESO EN INSTALACIONES**

**JORGE HUMBERTO BEDOYA ARISTIZABAL
AUTOR**

**LUIS GABRIEL FERRER
ASESOR**

**UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE RELACIONES INTERNACIONALES ESTRATÉGIA Y
SEGURIDAD
DIRECCIÓN DE POST GRADOS
ESPECIALIZACIÓN ADMINISTRACIÓN DE LA SEGURIDAD
BOGOTÁ D.C.
2014**

Resumen

A través de la historia el ser humano ha sentido la necesidad de protegerse, de brindar seguridad a su entorno y de esta forma contrarrestar la presencia de enemigos, además defenderse del acecho de los animales salvajes, estas situaciones de amenaza lo lleva a demarcar los límites de su caserío, estos involucra las viviendas, es así como resguarda este perímetro con trampas y barreras sencillas compuestas por troncos de árboles o las imponentes murallas, dicha necesidad de protegerse ha establecido a lo largo de la historia el desarrollo de iniciativas de implementación de controles de acceso a los distintos tipos de instalaciones; en el ámbito de la seguridad, surgen modelos de protección para una simple edificación como vivienda, hasta la más sofisticada infraestructura industrial, defensa o cárceles, es por este motivo que surgen diversas normas o sistemas de gestión para validar los controles que implementan las organizaciones.

Palabras Clave: protegerse, seguridad, normas, dispositivos, implementación.

Introducción

El presente escrito permite explicar la importancia del factor humano en los procesos de control de acceso en instalaciones, el origen de los controles de acceso, sus objetivos básicos en la seguridad de instalaciones, la estructura que lo conforma, las ventajas que presentan de acuerdo al tipo utilizado en la protección de instalaciones, además en qué estado deben permanecer para su óptimo funcionamiento, establecer cómo mediante un programa de mantenimiento se garantiza su operación y efectividad para lo cual se ha instalado.

Conocer su trayectoria en el marco normativo en países, como España, la legislación Colombiana que lo regula, para ser implementado en la protección de los bienes de las organizaciones, también citar algunos sistemas de gestión como Alianza Empresarial para un comercio seguro BASC, la norma de la seguridad de la información ISO 27001 los cuales auditan la conformidad de estos controles y el cumplimiento de las funciones del hombre de seguridad.

Los controles de acceso son dispositivos que impiden o retrasan cualquier acto de intrusión que atente contra la seguridad, estos han permitido a diferentes organizaciones proteger su patrimonio en forma eficaz, es importante identificar cuáles son los más utilizados de acuerdo a las instalaciones en Colombia.

Es así como a partir del avance de la tecnología empleada en seguridad y de los dispositivos y los protocolos implementados en diferentes escenarios, se establece el perfil

y competencias con que debe contar la persona que realice las actividades de guarda de seguridad en el procesos de control de acceso de instalaciones, donde se puede llegar a establecer un plan de capacitación para fortalecer el servicio de seguridad.

LA IMPORTANCIA DEL FACTOR HUMANO EN LOS PROCESOS DE CONTROL DE ACCESO EN INSTALACIONES

Los controles de acceso surgen de la necesidad de protección, es así como en el año 8.530 AC es construida la primera ciudad amurallada con este fin, se colocaban soldados que vigilaban cada esquina y controlaban el cumplimiento y efectividad de las actividades de seguridad las cuales evitaban el paso del enemigo.

La protección del perímetro fue implementada en la antigüedad para evitar que las fronteras fueran penetradas por los enemigos considerados por estos como objetivos militares, se colocaban barreras para defenderse de los ataques producto de los conflictos con pueblos cercanos, en el transcurrir de los años, de acuerdo a la necesidad y características de las infraestructuras como empresas, industrias, centros carcelarios, aeropuertos estas protecciones son instaladas y adaptadas de acuerdo a diferentes normas para el control.

El concepto de controles de acceso en la seguridad de instalaciones es muy extenso, abarca un sinnúmero de campos de acción y entre algunos objetivos primordiales se destacan la seguridad de las personas, la protección de los bienes y de la información, esta protección de instalaciones está siendo implementada en todos los campos de la sociedad, que conlleva a un ambiente de seguridad.

La función principal del control de acceso es evitar que un individuo no autorizado ingrese a una instalación, es decir controla la entrada y salida, si no es detectado a tiempo y

el control es ineficaz, este periodo de tiempo de intrusión sería necesario para que se materialice un daño, un sistema de control de acceso involucra hardware y software, los cuales pueden presentar un componente tecnológico sencillos o dispositivos más complejos. (Ver figura 1).

Figura 1. Hardware y software Control de Acceso.



Fuente: formación Fraj 11 Michelin

Básicamente el control de acceso consiste en adaptar algún mecanismo electrónico y mecánico que identifique si un sujeto que quiere ingresar a un sitio o área está autorizada y por consiguiente le permite el correspondiente acceso o se lo niega (Ver fig. 2).

Figura 2. Dispositivos Control de Acceso.

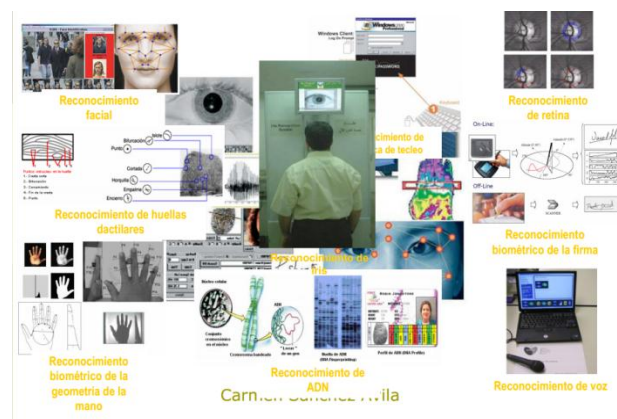


Fuente formación Fraj 11 Michelin

Los diferentes controles de acceso a instalaciones, se utilizan en área como ingreso a parqueaderos, bodegas, centros de cómputo, estos presentan ciertas ventajas ya que solo permite el ingreso de personas autorizadas, permitiendo registrados en las bases de datos, también retrasa en muchos casos las intenciones de ingreso no autorizadas siendo detectadas por la señal de alarma del sistema.

Según las características de los controles para instalar, se puede nombrar diversos dispositivos que son diseñados para identificar rasgos propios de una persona garantizando su efectividad ya que estos son únicos en cada uno como los biométricos(ver figura 3), los dispositivos pueden adaptasen a un lugar, edificio o áreas diversas dentro de instalaciones cuya función es la separación de accesos, los controles a instalaciones deberán ser capaz de identificar las personas que trata de entrar en las áreas restringidas de tránsito, verificando su autorización de ingreso, estos Permitirán asegurar que sólo el titular de una autorización de seguridad es autorizado en una zona de acceso restringido.

Figura 3. Dispositivos biométricos



Fuente: http://www.criptored.upm.es/descarga/TASSI2012_CarmenSanchez.pdf

Los sistemas de control de acceso se dividen en: sistemas de credencial o tarjetas magnética, que consiste en llaves mecánica, eléctrica, electrónica, magnética, mixta, tarjetas con un sistema de código de circuito eléctrico, con banda magnética, mecánica, con código magnético, electrónico, mixtas, emisores de radiofrecuencia, infrarrojos, ultrasonidos, sistemas de credencial de conocimiento y personal, teclado digital, cerradura de combinación, escritura, credencial personal, huella digital, voz, geometría de la mano, rasgos faciales, iris de ojos, entre otros.

En los sistemas de control de acceso se deben incluir también dispositivos que mantengan registros de las entradas y salidas del personal, es decir la correspondiente trazabilidad tanto en horario de trabajo como también fuera de dicho horario, el sistema más común que se conoce de doble tecnología es la tarjeta de seguridad, que puede ser de aproximación o banda que es acompañada de un número de identificación personal, que deberá ser introducido en el sistema que controla el ingreso por cada individuo utilizando un teclado numérico haciendo más efectivo el control.

El código utilizado deberá consistir en cuatro o más números, seleccionados en forma aleatoria, sin conocimiento o asociación lógica con la persona para evitar su fácil identificación, este deberá ser cambiado cuando exista cualquier duda sobre posible alteración, o riesgo de su conocimiento por personas que quieran afectar las instalaciones.

De acuerdo a la clasificación hecha en las instalaciones por áreas, se implementarán sistemas avanzados de control como el tipo “antipassback” el cual obliga a los usuarios a salir antes de poder entrar y viceversa, de esta forma se evita la inapropiada utilización de

los sistemas de tarjetas de aproximación para entrar más de una persona con un mismo dispositivo de acceso.

Con el fin de conservar en buen estado de funcionamiento los dispositivos, cada instalación, se somete a verificaciones y a un mantenimiento preventivo, por lo cual el responsable de administrar el sistemas establece con un técnico certificado un contrato o acuerdo de mantenimiento para formalizar contractualmente el servicio, donde incluirá al menos una visita anual, y la verificación completa de dicha instalación.

El número de visitas puede variar ya que puede presentarse averías por diferentes motivos ,el contrato de mantenimiento debe precisar, la frecuencia de visitas de verificación, la naturaleza de las operaciones realizadas, un plazo máximo de intervención por fallas con rapidez, lo anterior debe estar bien estipulada en el contrato.

Las verificaciones, es decir mantenimiento preventivo tienen por objetivo controlar el estado de funcionamiento de la instalación e informar al responsable en cada visita, este debe manifestar al técnico los problemas eventuales relacionados con su funcionamiento, por otra parte, el técnico instalador debe asegurar, en acuerdo con el cliente, que no se han realizado en la disposición de los locales, modificaciones que sean susceptibles de disminuir la eficacia de la instalación, además, cualquier modificación, obligatoriamente es objeto de una nueva verificación de conformidad y de una puesta al día de los registros de archivos de seguimiento técnico de operaciones a realizar.

Después un control visual de la instalación (que permita descubrir un daños en los cables, etc.), el técnico de mantenimiento verifica la eficacia de la instalación de los controles de acceso, los controles deben comportar, al menos, las siguientes operaciones, control de alimentación, verificación de las tensiones de baterías, cargadores, verificación del consumo de la instalación, operaciones de mantenimiento que se efectúan en las fuentes de alimentación secundaria, ensayos de verificación de los dispositivos, lectora, troncal, funcionamiento de los dispositivos de aviso y señalización de alarma, estos dispositivos funcionan en sus fuentes de alimentación secundaria (de forma autónoma en el caso de dispositivos autoalimentados).

Se debe realizar pruebas de transmisión y de recepción de las informaciones procedentes de la instalación de control de acceso, conectadas con la estación central de monitoreo o comunicaciones o destinatarios particulares, funcionamiento de la central de alarma, Verificación de temporizaciones de entrada y salida, Control de auto vigilancia de la instalación, análisis del histórico de mantenimiento correctivo estas intervenciones tienen por objeto restablecer el funcionamiento de la instalación tras una avería o un fallo, el administrador, en caso de avería o interrupción de la instalación de detección de intrusión, avisará inmediatamente a mantenimiento para su intervención y tomará las medidas de seguridad o vigilancia que se precisen durante el tiempo que sea necesario.

Los Registros de mantenimiento, constituyen un elemento de trazabilidad, es diligenciado al final de la intervención y se anexa a los archivos históricos de la instalación, debe indicar las operaciones efectuadas, las anomalías constatadas y la duración de cada visita de verificación o de mantenimiento correctivo.

La normativa aplicable para los controles de acceso de las instalaciones, las diferentes actividades y servicios de seguridad enfocada en este caso a los controles de acceso a instalaciones se debe prestar conforme a la Constitución Política Colombiana, lo dispuesto en la ley y ordenamiento jurídico, las personas involucradas en la seguridad de instalaciones tendrán actuaciones fundamentadas en los principios de integridad , protección y trato correcto a las personas.

En diferentes países se tiene presente reglamentaciones para poder realizar las actividades de controles de acceso bajo el marco legal, un ejemplo de ello es la Ley 23 del 30 de julio de 1992, que rige en España donde expresa que para garantizar la seguridad, solamente se podrán utilizar las medidas reglamentadas y los medios materiales y técnicos homologados, de manera que se garantice su eficacia y se evite que produzcan daños o molestias a terceros.

Además el Ministerio del Interior Español determina las características y finalidades de dichos medios técnicos, que podrán ser modificadas o anuladas cuando varíen las condiciones o circunstancias que determinaron su aprobación, se debe realizar un seguimiento a la instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad, una interacción con las autoridades, explotación de centrales para la recepción, verificación y transmisión de las señales de alarmas y su comunicación a las autoridades competentes.

En Colombia el Decreto 356 de 1994 por el cual se expide el estatuto de vigilancia y seguridad privada que autoriza a las empresas de vigilancia y seguridad privada desarrollar actividades de fabricación, importación, instalación, comercialización o arrendamiento de equipos para vigilancia y seguridad, y tener su correspondiente registro ante la Superintendencia de vigilancia, las empresas de seguridad privada son las autorizadas para distribuir, comercializar e instalar los diferentes dispositivos de seguridad donde está involucrados de los controles de acceso, los cuales están diseñados para proteger diferentes tipos instalaciones, también indica esta ley que el Gobierno Nacional reglamentará el ejercicio de estas actividades.

Los equipos que serán objeto de inspección, control y vigilancia por parte de la Superintendencia de Vigilancia y Seguridad Privada, equipos de detección, los cuales son todos aquellos materiales o equipos para descubrir la presencia de armas u otros elementos portados por las personas, equipos de visión o escucha remotos, son todos aquellos equipos y materiales que se emplean para observar o escuchar lo que sucede en lugares remotos, equipos de detección, identificación, interferencia y escucha de comunicaciones que son aquellos equipos que se emplean para descubrir, identificar, interferir y escuchar sistemas de comunicaciones, o para descubrir la presencia de estos mismos sistemas.

Equipos de seguridad bancaria. Son todos aquellos materiales o equipos que se emplean para proteger instalaciones, valores, dineros, joyas, documentos y demás elementos de custodia de las entidades bancarias o similares, equipos donde se incluyen controles de acceso.

Así mismo internacionalmente, existen diferentes normas como la ISO 27001, Sistema de Gestión de la seguridad de la información, de carácter internacional que abarca la protección de la información hace énfasis en los controles de acceso para ingresar a las áreas sensibles, es decir aquellas donde no todas las personas tienen la autorización para ingresar, de acuerdo a las actividades de cada una se debe programar un perfil, este derecho anula o restringe cuando ya no pertenece a la compañía, abarca también los derechos de acceso de todos los empleados, contratistas o usuarios hasta que termine su contrato laboral.

Entre más obstáculos se implementen es mayor la dificultad para el intruso, se deben utilizar perímetros de seguridad (barreras tales como paredes, puertas de acceso controladas con tarjeta o molinetes) para proteger las áreas que contienen información y servicios de procesamiento de información, las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado, se pueden citar ejemplos como áreas de carga, despacho acceso público y aeropuertos.

De igual forma entre los sistemas de Gestión de seguridad sobresale la Alianza empresarial para un comercio seguro BASC, el cual establece estándares con una serie de orientaciones a seguir relacionadas a los controles de acceso, estos unidos a la identificación que deben de cumplir todas las personas que vayan a ingresar a las instalaciones, lo cual genera filtros proporcionando seguridad en las organizaciones, hace énfasis que debe de existir un sistema de identificación de empleados con el propósito de controlar el acceso y su obligatoriedad de uso dentro de las instalaciones, los carnés son personal e intransferibles.

El personal de seguridad de la compañía o la persona responsable tienen que controlar en forma adecuada la entrega y devolución de los carnés de identificación de empleados, visitantes y proveedores, documentar los procedimientos, está contemplado que los visitantes tienen que presentar una identificación con foto al momento de ingresar a la instalación exhibiendo en lugar visible su identificación o sticker adhesivo y de lo posible ser acompañados dentro de las instalaciones por un responsable.

De acuerdo a las características de las instalaciones a proteger y los equipos utilizados son implementados los protocolos, es decir, cuál es más eficaz ya que los ambientes, edificaciones y organizaciones son diferentes, no es igual las condiciones de una empresa a las de una cárcel de máxima seguridad, donde los dispositivos y los controles cambian de acuerdo a las personas que interactúan en estas dos instalaciones.

Los diferentes tipos de control de acceso utilizados en instalaciones con tecnología avanzada exigen a las personas en el oficio de la seguridad mayores niveles de competencias, requieren todos ellos de la aplicación de métodos que en forma integral permitan hacer frente a los diferentes retos que se presentan en el día a día en esta actividad, es de recalcar que uno de los factores claves del éxito de la labor del hombre de seguridad es la excelencia, donde las actividades van más allá del desarrollo normal de sus funciones logrando buenos resultados.

La calidad humana de las personas que desarrollan la labor de seguridad, su desarrollo personal, autoestima, visión personal y profesionalismo está orientado a entender el rol dentro del escenario empresarial donde se presta el servicio de seguridad, que incluye el

qué, el cómo, el por qué y el para qué, de la misión de seguridad, el hombre de seguridad debe ser proactivo, que significa estar antes de que sucedan los acontecimientos, identificar herramientas que le permita contrarrestar situaciones que puedan afectar la seguridad de las instalaciones a las cuales se le ha encomendado basado en el análisis de riesgos.

Un Protocolo es el conjunto de pasos u orientaciones destinados a estandarizar una acción o comportamiento de las personas frente a una situación específica, la historia hace referencia al primer protocolo conocido el de Hammurabi, rey de Babilonia que dictó una serie de normas sociales que se tenía que cumplir paso a paso, de igual forma se referencian que los Romanos en cada conquista guerrera tenían también una serie de instrucciones para alcanzar victorias en el campo de batalla.

Las características de los controles de acceso cambian, instalaciones petroleras, aeropuertos, bancos, cuartos de cómputo son consideradas de gran importancia y los dispositivos utilizados, deben cumplir con ciertas necesidades, las normas aplicadas y el personal con su formación hacen que funcionen con efectividad.

En Colombia son diversos los controles de acceso implementados en las organizaciones, desde lo más sencillo y elemental como la verificación de un listado por parte de un guarda de seguridad, como la implementación de elementos sofisticados ya sean biométricos, lectoras de tarjetas de proximidad, unidas a sistemas de monitoreo, detector de metales, molinetes, estos equipos depende de grandes presupuestos de las organizaciones.

El guarda de seguridad es la persona encargada de proteger la integridad física de las personas y los bienes materiales de las instalaciones donde prestan el servicio, este profesional de la seguridad debe ser capaz de tomar decisiones de acuerdo a las funciones, contar con la capacidad para persuadir a aquellos que generen problemas, manejar un autocontrol ligado a la serenidad para afrontar situaciones de riesgo, estar siempre concentrado y demostrar proactividad hacia la seguridad.

Su profesión lo hace ser analítico, observador, que lo conduzca a identificar y formular problemas que afecten el entorno donde presta el servicio de protección a su vez debe tener en cuenta los protocolos definidos para ser implementados en cada situación, los cuales siempre deben de estar ligados a la normativa vigente.

Para que un guarda de seguridad pueda desempeñar su función debe de cumplir como requisito cuatro niveles de capacitación en una empresa avalada por la Superintendencia de Vigilancia y Seguridad Privada, en esta capacitación es preparado en diferentes actividades contemplando aspectos laborales donde sobresale el conocimiento y uso de las armas de dotación, relaciones humanas ya que un hombre de seguridad debe entrar en contacto todos los días con diferentes personas.

Esta capacitación es de estricto cumplimiento al decreto 356 del 11 de febrero de 1994 emitido por la Supervigilancia y en el cual estipula una intensidad mínima de 200 horas dividida en cuatro niveles que conlleva a una prestación de servicios con calidad. Esta permite desarrollar destrezas y habilidades tanto físicas como intelectuales para poder aplicar en la protección de las personas y de los diferentes bienes que se le encomienda, es

así como va más allá de una simple vigilancia es un profesional del manejo de armas, el primer respondiente ante un conato de incendio por su formación en el manejo de extintores, controlando los diferentes dispositivos electrónicos empleados en la seguridad.

El guarda de seguridad es la base fundamental de un esquema de seguridad de cualquier instalación, en conjunto con los dispositivos implementados logra la tranquilidad a los clientes, ellos son evaluados desde el proceso de selección, incorporación presentando y superando pruebas, valoraciones psicológicas, físicas y psicotécnicas.

Así mismo el personal de seguridad es evaluado periódicamente de acuerdo al cumplimiento en el servicio por el cliente, los cuales se reúnen con su jefe inmediato analizando actitudes, comportamientos proactivos, cumplimiento de funciones o consignas de cada puesto, habilidades en el manejo de los dispositivos y re direccionando en aquellos puntos a mejorar.

No hay duda que el factor humano es la base fundamental en el proceso de seguridad de cualquier instalación presenta una serie de características, un parqueadero, centro de reclusión, hospitales, aeropuertos que requieren la implementación de diferentes tipos de controles. (Ver figura 4).

Figura 4. Dispositivos Control de Acceso Vehicular.



Fuente. <http://controldeparqueadero.blogspot.com>.

El control de acceso a las instalaciones de un parqueadero, consta de diferentes dispositivos como lectoras de aproximación, talanqueras, CCTV, en muchos casos se realizan verificación por parte de guías caninos y con la presencia del hombre de seguridad que está atento en el cumplimiento de las labores propias de seguridad. (Ver figura 5).

Figura No.5 Controles de acceso en instalaciones Carcelarias



Fuente. http://www.accesor.com/esp/art2_query.php?sec=10

Los controles de acceso a los centros penitenciarios se caracterizan por realizarse una completa identificación de las personas al ingreso y a la salida, con sistemas dactilar (Figura 4) para contrarrestar posible suplantación, de igual forma requisas minuciosas para evitar el ingreso de armas, narcóticos, medios de comunicación como celulares, radios que conllevan a riesgos dentro de las instalaciones. (Ver figura 6).

Figura No.6 Control de acceso aeropuerto



Fuente. http://www.rinconeducativo.org/rayo_de_acceso.html

Unas de las instalaciones que tienen implementados una serie de dispositivos de control de acceso con presencia de personal de seguridad, autoridades, dispositivos de detectores de metales, scanner son los aeropuertos ya que los controles se realizan para evitar tráfico de contrabando, acciones terroristas entre otras situaciones que pudieran presentarse.

Como propuesta de capacitación del personal de seguridad para fortalecer la integración de los dispositivos de control de acceso y las disposiciones establecidas se debe tener en cuenta los diferentes sistemas de gestión de control en seguridad como BASC, ISO 28000, pues son las normas técnicas internacionales fundamentales para generar en el personal de seguridad una actitud de profesionalismo integral y crear una cultura prevencionista y dar la aplicación de procedimientos establecidos con toda la proactividad del hombre de seguridad.

Generar, mediante las acciones de formación y capacitación, el desarrollo de competencias comunes y comportamentales en los empleados, con el objeto de incrementar

la efectividad en sus prácticas laborales, realizar procesos que propicien sentido de pertenencia y compromiso con la organización.

El programa de capacitación planteado contempla las siguientes temáticas: Sistema de gestión en control y seguridad, Procedimiento para el control de acceso adecuado, de empleados, contratistas y visitantes.

Conclusiones

El factor humano es importante en los procesos de control de acceso a instalaciones, es el resultado del trabajo profesional que interrelaciona la capacitación, disciplina y compromiso de las personas e instituciones que prestan este servicio.

Con la implementación de Sistemas de Gestión en seguridad, los cuales se enfocan a normas o estándares, seguimiento y control de los protocolos y mantenimiento de los dispositivos empleados en la protección de instalaciones donde las organizaciones pueden garantizar el seguimiento y cumplimiento de los dispositivos para su protección.

El enfoque de capacitación de las empresas a su personal que cumple funciones de seguridad, se aplica conforme a las normas y protocolos lo cual permite neutralizar acciones que afectan su seguridad, lo cual se ve reflejado en reducción de pérdidas de su patrimonio, imagen y en muchos casos su permanencia en el tiempo.

Bibliografía

Instituto Colombiano de Normas Técnicas y Certificación. (2006-03-22). *Norma Técnica Colombiana NTC-ISO 27001*. Recuperado de:

<http://www.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf>.

Autoridad Nacional para la protección de la información clasificada N/S/03(2012). *Seguridad física (Edición 2.0)*. Recuperado de:

http://www.cni.es/comun/recursos/descargas/NS-03_Seguridad_Fisica.pdf.

Alianza Empresarial para un Comercio Seguro (2004). *Resumen Norma Estándares BASC*. Recuperado de: <http://www.wbasco.org/espanol/documentos/viejos/resumen-norma-estandares.pdf>.

Alianza Empresarial para un Comercio Seguro. (ND). *Guía para establecer la seguridad en el perímetro como primera línea de defensa y protección de la organización*. Recuperado de: <http://www.coexnort.com/documentos/seguridadperimetrica.pdf>.

P. Protección de riesgos. (ND). *Manual del guardia de seguridad*. Recuperado de:

www.proteccionderiesgos.com.ar/pdf/manual-guardia

Capacitación Procampo. (ND). *Formación de guardias de seguridad privada*. Recuperado:
http://www.procampo.cl/gestor/archivos/formacion_de_guardias_de_seguridad.pdf.

Organización Michelin (2009). *Formación Frafi 11 para técnicos en seguridad patrimonial*.

Seguridad Percol LTDA. (2011). *Control de acceso*. Recuperado de:
www.seguridadpercol.com/controles%20de%20acceso.html

Cano, J.J. (2009). *La seguridad física y electrónica*. Recuperado de:
http://www.infosecurityvip.com/newsletter/vista_dic09.html

García, A. (2009). *Estudio de mercado de la seguridad electrónica en Colombia*.
Recuperado de: <http://segelec.blogspot.com/>

O Baque, M. Moya. (ND). *Evaluación de riesgos físicos en una agencia de distribución de acuerdo al sistema BASC*. Recuperado de:
<http://www.dspace.espol.edu.ec/bitstream/123456789/2391/1/4731.pdf>

SUPERVIGILANCIA. (ND). *Protocolo de operación servicio en entidades financieras*.
Recuperado de: www.supervigilancia.gov.co/?idcategoria=56219

Ley 23 de 1992 30 de julio España. *Protección ciudadana*. Recuperado de:

<http://www.interior.gob.es/web/servicios-al-ciudadano/normativa/leyes-ordinarias/ley-23-1992-de-30-de-julio>

SUPERVIGILANCIA. Decreto 356. (1994). *Estatuto de Seguridad*. Recuperado de:

<http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=1341>

Dointech. (ND) *Control de acceso vehicular*. Recuperado de:

<http://www.dointech.com.co/control-acceso-vehicular.html>

Dolthink. (2012). Sistema Control Accesos en Aeropuertos: *ABC Sistema*

Necesidad de control de acceso avanzado en aeropuertos. Recuperado de:

<http://www.dolthink.com/abc-sistema-control-accesos-aeropuertos.html>

Secretaria de Capacitación y Formación Profesional Ecuador. (2012). *Perfil de competencia laboral Guardia de vigilancia y seguridad privada modalidad fija (2 Edición)*.

Recuperado de:

<http://www.secretariacapacitacion.gob.ec/wp-content/uploads/2013/07/Perfil-guardia-de-seguridad-y-seguridad-privada-modalidad-fija.pdf>.