

SISTEMAS DE CONTROL DE ACCESO PARA UNIDADES MILITARES

**EDGAR MAURICIO ORTIZ CHAVEZ
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

Las guarniciones Militares son los sitios destinados para acantonar uno o más batallones, su misión es alineada a la misión de las Fuerzas Militares, la cual se encuentra encaminada a defender la soberanía Nacional, la independencia e integridad territorial, esta se cumple mediante el desarrollo de diferentes operaciones Militares, teniendo en cuenta la importancia de su misión se hace necesario proteger sus instalaciones utilizando diferentes tipos de sistemas o dispositivos de alta tecnología, una técnica utilizada por el enemigo para obtener información acerca de las actividades que se están realizando en una guarnición Militar es por medio de la intrusión de personas las cuales ingresan a las unidades con el objetivo de extraer información o material, para contrarrestar esta intrusión, el mercado pone a disposición los sistemas de control de acceso, utilizados para controlar el ingreso o la salida a determinada instalación y a sus sitios más sensibles.

Palabras Clave: sistema, acceso, guarnición, biométrica, militar.

Introducción

Los sistemas de control de acceso son herramientas que han permitido a las organizaciones realizar un control de entrada a sus instalaciones, han mostrado excelentes resultados y permanentemente presentan avances tecnológicos, su utilización se hace estrictamente necesaria, el presente escrito busca analizar la importancia de instalar estos sistemas en una guarnición Militar.

Toda la información que se maneja al interior de una guarnición Militar es de uso exclusivo de las Fuerzas Militares, se clasifica como reservada, confidencial, secreta y Ultra secreta, sumamente importante para el manejo de la unidad Militar y el cumplimiento de la Misión institucional, por su parte el tipo material que maneja la Fuerza Pública es de uso privativo, puede estar catalogado como de armamento, intendencia y comunicaciones, el gobierno Nacional lo adquiere y lo suministra a las Fuerzas para su funcionamiento, por la importancia que reviste tanto la información como el material es necesario buscar los métodos o mecanismos más adecuados para su protección, es fundamental la planeación de recursos económicos que permitan proteger los activos tangible e intangibles mencionados.

Para tal efecto inicialmente es necesario conocer en que consiste un sistema de control de acceso por medio de una definición clara, las partes o dispositivos que lo componen y el papel que cumple cada uno dentro del funcionamiento del sistema, así mismo las ventajas que obtienen las organizaciones con la instalación de estos sistemas.

Una vez identificados los sistemas de control de acceso que existen y sus principales características, se debe verificar que es un cuartel Militar, sus principales actividades, los sitios más sensibles, identificar que sistemas de seguridad existen para complementarlos y las ventajas que puede llegar a obtener una guarnición Militar con la instalación, buena operación y mantenimiento de los sistemas de control de acceso.

Finalmente con toda la información recolectada acerca de los sistemas de control de acceso y el estudio de seguridad de la guarnición Militar, se puede llegar a establecer una recomendación de qué clase de sistema es el más adecuado a instalar, para minimizar el riesgo de intrusión a la guarnición y a los sectores más sensibles de esta.

SISTEMA DE CONTROL DE ACCESO PARA UNA GUARNICIÓN MILITAR

El sistema de control de acceso se conoce como el proceso de control de entrada y salida a determinado sitio o zona, estos pueden estar diseñados con diferentes tipos de tecnologías y dispositivos que permiten: En primera instancia restringir la entrada y salida a un sitio, en segundo lugar identificar el usuario que ingresa a un sitio y permitir o denegar su acceso según parámetros previamente establecidos, por último registra y audita los eventos de acceso por cada usuario y por puerta o sitio de ingreso.

Hay sistemas de control de acceso peatonal, control de acceso vehicular y para control de personal. Los de acceso peatonal se implementan para tener un control de todo el personal que ingresa y transita por un espacio público o privado de una organización, este tipo de sistema busca asegurar el paso de personas que cuentan con autorización para transitar por una zona y restringir el paso de las personas que no cuentan con autorización. (Ver figura 1).

Figura 1. Dispositivos Control de Acceso Peatonal.



Fuente. www.t2app.com.

En el sistema de control de acceso vehicular (ver figura 2), se busca controlar la entrada y salida de los vehículos que pertenecen a la organización personal de la misma y los vehículos visitantes, para facilitar el manejo y la integración de los sistemas de control peatonal y vehicular estos se pueden integrar permitiendo que el conductor del vehículo ingrese a las instalaciones sin la necesidad de volver a registrarse o pasar por el sistema de control peatonal.

Figura2. Dispositivos Control de Acceso Vehicular.



Fuente. www.dointech.com.co/control-de-acceso-html.

Por último se tiene el control de personal, con el cual se verifica la hora de entrada y salida a las instalaciones o zonas de trabajo, este sistema también se le conoce como sistema de control de asistencia y por medio de él se puede llevar un control exacto de las horas en que el personal está dentro o fuera de las instalaciones de trabajo, para lo cual se utilizan dispositivos como teclados, biométricas o tarjetas. (Ver figura 3).

Figura3. Dispositivos Control de Personal.



Fuente. www.Google.com.co/imagenes.

Una organización que tenga bien instalado y controlado un sistema de control de acceso adquiere unas ventajas en materia de seguridad y en materia de productividad, como por ejemplo: Control del personal que entra y sale de las instalaciones evitando el ingreso de personas ajenas o no autorizadas a la organización, aumenta la seguridad al no permitir que ingrese personal ajeno a las instalaciones, se presenta un ahorro en costos de personal de vigilancia en la entrada y en las instalaciones, se puede obtener un registro real de la entrada y salida del personal medida utilizada para que los empleados sientan un control de entrada y salida a las zonas de producción, con lo anterior se mejora la productividad del personal, se permite restringir la apertura de puertas en vista a que se hace de forma automatizada y solo para personal autorizado a determinada área, con la instalación de sistemas de control de acceso se percibe un ambiente moderno en las organizaciones siendo visto por los clientes como un valor agregado, otra ventaja es el respaldo a otros sistemas de control de seguridad como circuito cerrado de televisión, así mismo se puede administrar y centralizar la información de asistencia del personal de la organización, sirve de base de datos o como soporte o prueba al departamento de nómina al momento de liquidar horas extras, impide que personal ajeno a determinado sitio ingrese sin ser autorizados en

determinadas horas, es posible verificar que cantidad de personal hay en el momento en determinado sitio o sector de la organización, permitiendo tener un control de acceso vehicular, se puede realizar una base de datos con los registros de proveedores y clientes de la organización, así como controlar el tiempo de permanencia de una persona o un vehículo dentro de la organización, los sistemas de control de acceso están en capacidad de evitar que haya suplantación de una persona por medio de su identificación, también es de ayuda para identificar los hábitos del personal de la organización para poder tomar medidas disuasivas oportunamente, con un sistema de control de acceso se puede programar autorización o desautorización del acceso relacionando usuarios fechas y horas.

Así mismo un sistema de control de acceso da sensación de seguridad y las personas que laboran o ingresan a una instalación que cuenta con este sistema se sienten seguras, para las organizaciones delincuenciales una instalación con sistema de control de acceso se convierte en un objetivo difícil o tal vez imposible al dificultarse o imposibilitarse su ingreso a la instalación, estos sistemas son además de fácil manejo y los costos de instalación y operación relacionados con todas las ventajas que brinda son bajos.

Hay varios sistemas de control de acceso, su funcionamiento depende de la configuración de los elementos y dispositivos que lo componen, pero básicamente el principio de funcionamiento es igual, consiste en un dispositivo que contiene un lector ya sea de tarjeta de proximidad, de huella, voz, iris, o de clave, en algunos casos se combinan estos tipos de lectores, la otra parte del sistema la compone un dispositivo conocido como controlador, su trabajo es autorizar o denegar el paso del personal, este controlador realiza la comunicación entre los lectores y el sistema de apertura previa comparación de una

información establecida en una base de datos o software contenida en un ordenador, al controlador también se le conoce como tarjeta controladora y tiene conectados todos los periféricos que realizan todo el proceso de control de acceso, trabaja como cerebro central del sistema, el último componente de los sistemas de control de acceso son los dispositivos de apertura, los cuales reciben del controlador la orden de abrir o no las puertas, molinetes, jaulas, torniquetes, pasillo automáticos o portillos. (Ver figura 4).

Todos los anteriores dispositivos que componen el sistema deben estar conectados a fuentes de energía que permitan una alimentación constante del sistema, es decir se debe tener el sistema o fuente de alimentación principal y un sistema de alimentación de respaldo que puede ser una UPS o banco de baterías.

Figura 4. Esquema Sistema Control de Acceso.



Fuente del Autor.

Inicialmente los sistemas de control de acceso se basaron en las tarjetas o carnets (Ver figura 5), que contenían un chip para ser leído por el sensor del lector, entregando como resultado de la lectura autorización o denegación de ingreso, también se utilizaron

inicialmente dispositivos que contenían teclados numéricos (Ver figura 5), que se instalaban a la entrada de una puerta o sitio de ingreso en el cual se digitaba la clave o código de ingreso y la chapa electrónica recibía la orden de abrir en caso de estar correcta la clave o código.



Fuente. www.Google.com.co/imágenes.

Actualmente se han desarrollado sistemas de control de acceso con dispositivos modernos que se le conoce como biométricas esta tecnología basa su trabajo de investigación en el estudio de características sociales y biológicas propias de cada ser humano las cuales son comparadas por un ordenador mediante modelos matemáticos y estadísticos, existen dos tipos de biométricas una de ella es labiométrica biológica que comparan medidas fisiológicas o partes del cuerpo humano como la medida de las huellas dactilares, el iris, la retina, venas de las manos, la mano y el rostro, el otro tipo de biométricas son las que identifican aspectos sociales, se basan en la medición de acciones de la conducta del ser humano como el uso de un teclado, la firma de la persona y la voz, en algunos casos se pueden combinar los usos de las biométricas a este proceso se le conoce como biométrica multi-modal, siendo comúnmente utilizadas la de iris y huella dactilar,

huella dactilar y la firma, huella dactilar y digitación de clave entre otras, los sistemas biométricos más comunes y utilizados son los de huella digital, iris del ojo, características de la mano, características faciales y la voz.

Figura6. Técnicas biométricas.

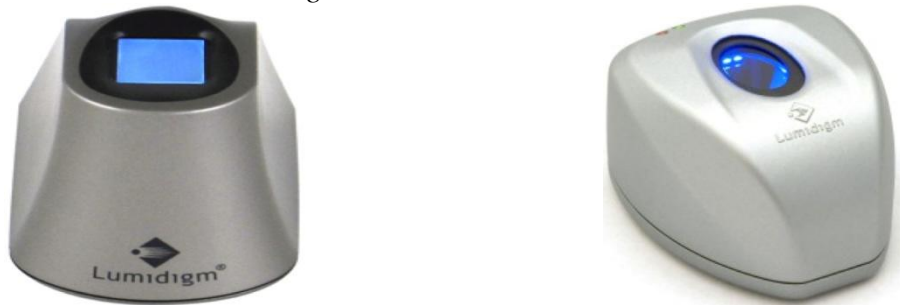


Fuente. www.Sistemasbiometricos.co/blog/técnicas-biométricas

Los sistemas biométricos de huella dactilar o huella digital se basan en el principio de que no existen dos personas con la misma huella, las huellas digitales cuentan con una característica especial llamada técnicamente minucia, esta minucia está compuesta por los arcos, ángulos, bucles y remolinos, siendo el factor a analizar por la biométrica para la identificación de una persona, la mayoría de las personas cuentan con un aproximado de 30 minucias en su huella y los investigadores en este tema afirman que nadie tiene más de 8 minucias iguales ni siquiera siendo gemelos idénticos, la huella se forma en el ser humano desde su desarrollo fetal y se mantiene inalterable por toda la vida, esta sirve como una prueba legal en un proceso judicial, existen varias técnicas para la identificación o análisis de la huella como la técnica manual, la técnica basada en imágenes y la técnica basada en texturas, pero la biométrica funciona utilizando técnicas basadas en las minucias de la huella, esta técnica es la más conocida y precisa que existe, la biométrica de huella digital o

dactilar trabaja bajo el siguiente proceso cumpliendo con unos pasos esenciales para la autorización o denegación de la entrada a un sitio, el primer paso es captura de la imagen, los usuarios colocan su huella sobre un dispositivo (Ver figura7), posteriormente se efectúa la verificación del dato capturado, este se hace por medio del análisis de las minucias, el siguiente paso corresponde en poner los datos capturados en una plantilla de mapeo contenida dentro del software que posee el sistema, esta información se codifica como un código binario y por último se compara la información de los códigos que tiene almacenados internamente el sistema, si la comparación es correcta se autoriza ingresar a la zona o sector que se requiere.

Figura7. Lectores de Huella



Fuente. www.Lumidigm.com/es/products.

Los sistemas biométricos que trabajan con la identificación de patrones oculares (Ver figura 8), se basan en dos aspectos uno de ellos trabaja haciendo un escáner de la retina del ojo, estos sistemas biométricos toman como patrón de medida las venas en el fondo del ojo, esta medida se obtiene por medio de la proyección de una luz infrarroja en la pupila del ojo, el otro patrón ocular que se utiliza en sistemas biométricos es la identificación del iris del ojo estos sistemas son más utilizados que los de análisis de retina y funciona por medio de

cámaras con iluminación infrarroja, la cámara que captura la imagen es de alta resolución y cuenta con un zoom avanzado que le permita aproximarse lo suficiente al objetivo para enfocar el ojo a una distancia que no resulte incomoda al usuario, el usuario debe ubicarse en un campo que le permita a la cámara capturar la imagen, posteriormente a la captura de la imagen esta se procesa por medio de la localización de la zona de interés una vez localizada esta zona se extrae el patrón de comparación para convertirlo a coordenadas polares por medio de algoritmos matemáticos, posteriormente los resultados del algoritmo son convertidos a códigos por medio de la transformada de Haar (Principio matemático). Este código se compara con el código o plantilla almacenado previamente en la base de datos del sistema para autorizar o denegar el ingreso a determinado sitio.

Figura 8. Sistemas biométricos de patrones oculares



Fuente. www.Google.com.co/imagenes.

Algunas organizaciones prefieren utilizar la biométrica que utiliza el análisis de la geometría de la mano (Ver figura 9), este sistema funciona por medio de la toma de la muestra de la mano la cual debe ser puesta en un dispositivo que contiene unas guías para posicionar de una forma correcta la mano, el sistema toma imágenes o muestras de la mano una superior y otra lateral, en la toma de estas muestras lo que se observa son las características de anchura interdedo, dedos, medida de disimilaridad, distancia euclídea,

desviaciones y altura, líneas de la palma de la mano estas imágenes o muestras posteriormente se convierten en algoritmos matemáticos, el resultado de este algoritmo es comparado con lo que esta previamente archivado en la base de datos y el resultado de esta comparación es la autorización o denegación de la entrada a un sitio determinado de la organización.

Figura9. Sistemas biométricos de Análisis de la Geometría de la Mano

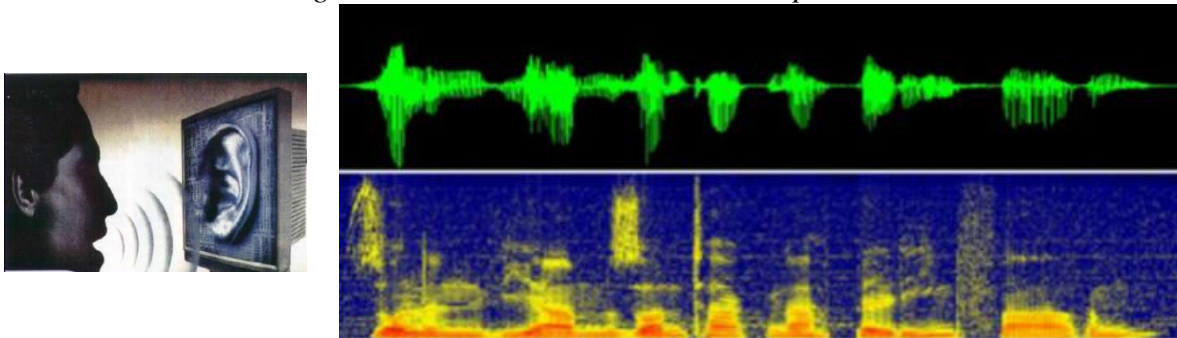


Fuente. [www. Google.com.co/imagenes](http://www.Google.com.co/imagenes).

Otro sistema biométrico utilizado en las organizaciones es de reconocimiento por voz este sistema es una combinación de sistemas biométricos físicos y de conducta, existen dos formas para hacer el reconocimiento por voz, una de modo limitado o dependiente del texto, funciona por medio de una pronunciación que hace el usuario de una frase o contraseña preestablecida en el sistema, la otra forma de reconocimiento es independiente donde la persona simplemente habla o repite la frase indicada por medio del dispositivo,

una muestra de la voz es tomada en forma de onda análoga, convertida posteriormente a información digital, la cual es comparada con la información previamente grabada en la base de datos del sistema y autoriza o deniega el acceso, los sistemas biométricos de identificación de voz identifican y analizan los tonos bajos y agudos, las vibraciones de la laringe, tonos nasales y de la garganta, también intervienen la anatomía de la tráquea, cuerdas vocales y las cavidades (Ver figura 10), la reunión e intervención de todos los elementos anteriores es lo que hace al sistema ser conocido como una combinación entre aspectos físicos y de conducta.

Figura 10. Sistemas de Reconocimiento por Voz



Fuente. [www. Rysostenibilidad.telefonica.com](http://www.Rysostenibilidad.telefonica.com)

Los anteriores sistemas son los más utilizados actualmente y de mayor eficiencia, otros sistemas de identificación por biométrica tienen el mismo principio de funcionamiento, captura de imagen o muestra, posteriormente se procesa esta muestra por medio de modelos matemáticos, pasa a ser un código binario, que se compara con lo que está almacenado en la base de datos del sistema, el resultado de esta comparación es la autorización o no de entrada al sitio que se solicita.

Todos los sistemas de control de accesos por biométrica tienen márgenes de error y algunas desventajas, se debe tener en cuenta características que pueden cambiar en los usuarios como por ejemplo la mano puede engordar, la huella se puede modificar a causa de una cicatriz o de la edad al igual que el iris del ojo puede ser alterado por una cirugía o el tono de la voz en algunos casos puede variar dependiendo del estado de ánimo de la persona, lo importante para el administrador del sistema es tener en cuenta todos estos aspectos, que comparados con las ventajas resultan insignificantes, también se debe concientizar al personal de la organización que los sistemas se instalan para la seguridad de todos, puesto que algunas se molestan y muestran incomodidad con la utilización de sistemas de control de acceso, hay varios precios y variedad de dispositivos en el mercado para escoger lo que mejor se ajuste a la necesidad de la organización se debe hacer un estudio profundo de todos los aspectos de seguridad de la organización como por ejemplo, cantidad de personas a ingresar, ubicación de las instalaciones, sitios o entradas que se deben restringir, los elementos tangible e intangibles que se quieren proteger y los sistemas de seguridad que ya existen para poder combinarlos o complementarlos de forma adecuada.

Los sistemas de control de acceso representan un gran aporte dentro de la seguridad de las organizaciones con ellos se pueda identificar quien ingresa y que sale de las instalaciones o de un sector determinado, las guarniciones militares son sitios sensibles en los cuales se tiene información y material de uso privativo de las Fuerzas Militares.

Se conoce como cuartel militar al sitio donde se encuentran acantonados uno o más batallones ya sea del Ejército Nacional, Armada Nacional o Fuerza Aérea Colombiana, el nombre del cuartel militar puede cambiar por batallón, unidad, guarnición, Base Naval o

Base Aérea dependiendo de la Fuerza a la que pertenezca, pero el funcionamiento básicamente es igual, la entrada principal al cuartel es la guardia bajo el control del comandante de guardia quienes nombrado por un periodo de 24 horas para controlar y supervisar todo el personal y material que ingresa y sale de las instalaciones del cuartel y para resguardar la seguridad del mismo, para apoyar la labor del comandante de guardia se nombran 2 suboficiales uno para permanecer en el recinto de la guardia y otro que permanece constantemente verificando los puestos de guardia ubicados alrededor de todo el cuartel y en los lugares más sensibles de la unidad militar, mencionados puestos son custodiados por soldados llamados centinelas y son relevados máximo cada 3 horas, en la guardia o entrada de la unidad se hace el registro, requisas y verificación de las personas o vehículos que ingresan, para salir de la unidad militar también se verifica la identidad de quien sale, sea persona o vehículo, en caso de que salga material se verifica la autorización para salir.

Un cuartel militar dentro de sus instalaciones tiene alojamientos utilizados para el descanso de los soldados de la unidad militar, casinos de oficiales y suboficiales, casas fiscales de oficiales y suboficiales en las cuales vive el personal casado que trabaja en la guarnición con su respectiva familia, el dispensario médico sitio para prestar los servicios médicos al personal militar y a sus familias, oficinas en las cuales funciona la parte administrativa de la unidad, depósitos o almacenes de armamento, intendencia y comunicaciones para concentrar el material reservado, centro de operaciones y comunicaciones, pistas y áreas de instrucción y entrenamiento, la sala de reflexión o de detenidos, sección de transportes para el funcionamiento del parque automotor de la unidad, tiendas y en algunos casos micro mercados, capilla o iglesia, hay cuarteles con condiciones

especiales que dentro de sus instalaciones cuentan con centros de reclusión militar, utilizados como centros carcelarios para personal militar con algún tipo de problema jurídico, talleres o laboratorio de mantenimiento de comunicaciones, área de polígonos y helipuertos entre otras.

Todos los sitios mencionados son sensibles y merecen tener la seguridad y atención necesaria para evitar que personal ajeno a estas áreas o sectores deambulen por ellos, en las oficinas que funciona la parte administrativa, centros de operaciones o comunicaciones se maneja toda la información de inteligencia, operacional y administrativa de una unidad militar la cual es clasificada como reservada y restringida, su pérdida o desviación causaría fallas en las operaciones que se adelantan, si esta información cae en manos del enemigo posiblemente las compañías y pelotones que ejecutan diferentes tipos de operaciones en la jurisdicción del batallón tengan algún tipo de descalabro.

Los depósitos o almacenes de material restringido, son de vital importancia puesto que es el recinto para albergar los elementos de intendencia, comunicaciones o armamento, el material que de allí se pierdan o se roben va directamente al enemigo, para ser utilizados en contra de los mismos miembros de las Fuerza Pública, la población civil y sus bienes.

Las unidades Militares que cuentan con centros de reclusión militar, deben enfocar su esfuerzo principal hacia la seguridad de este sitio, el personal que allí se encuentra privado de la libertad está inmerso en investigaciones y son de vital importancia para esclarecer hechos o procesos judiciales, así mismo hay personal que ya está condenado por algún tipo de delito o conducta, si este personal se fuga de su sitio de reclusión, el personal encargado

de los detenidos y de la seguridad del cuartel militar en ese momento, inmediatamente le adelantaran una investigación disciplinaria y penal por permitir la fuga de este personal.

Todos los procesos que se adelantan dentro de un cuartel militar son de carácter reservado y con la pérdida de información o material se puede ver comprometida la seguridad, la integridad y la vida de las personas que viven en él, así como la de las personas que se encuentran en las diferentes áreas de operaciones pertenecientes a la unidad, por esto se hace necesario reforzar los sistemas de control de acceso y salida de los cuarteles militares por medio de dispositivos tecnológicos que permitan tener un mayor control de estos procesos, actualmente en la mayoría de los cuarteles militares solamente se tiene un carnet como identificación del funcionario pero este puede ser falsificado o utilizado por otra persona, así mismo para la entrada a los dispensarios médicos solo basta con presentar el carnet de servicios médicos y en ocasiones no se verifica adecuadamente la identidad de quien lo porta, hay otros cuarteles en los cuales se cuenta con el fichero de identificación con chip de acceso en su interior pero por falta de mantenimiento se bloquea el lector o el torniquete de acceso.

Para mejorar los sistemas de control de acceso a las unidades militares se puede implementar un fichero o carnet de identificación con su respectivo chip, a la entrada el carnet debe ser cotejado por un soldado que verifique la identidad de quien lo porta, este sistema debe tener su respectivo mantenimiento para que funcione adecuadamente, ya al interior del cuartel se pueden instalar sistemas biométricos en las entradas de oficinas, depósitos y sitios sensibles, con esto se garantiza que solo puedan entrar a estos sitios personal autorizado.

Otra solución es instalar sistema biométrico en la entrada de la unidad para la identificación de las personas, cuando llegue personal que no esté registrado dentro de la base de datos de la unidad se procede a verificar a fondo quien es y a que sitio del cuartel se dirige.

En la entrada vehicular también se debe tener el fichero que permita identificar el vehículo y su procedencia, con lo anterior se controla que vehículos no autorizados estén en la instalación militar, con la instalación de los sistemas mencionados se controla la entrada o salida de personal, orgánico de la unidad y de ingreso permanentemente como proveedores o contratistas, se disminuye el riesgo de pérdida, fuga de información y material, sirve como herramienta de control a los comandantes de las unidades militares y servicios de régimen interno, también se puede verificar quien está dentro o fuera del cuartel, su hora de ingreso o salida

En las instalaciones que funciona el Ministerio de Defensa Nacional, Comando General de las Fuerzas Militares y Comandos de Fuerza actualmente hay instalado un sistema de control de acceso peatonal y vehicular que consiste en el uso de tarjetas que contienen un chip, el cual al ser leído activa un torniquete permitiendo el acceso, previamente a colocar la tarjeta sobre el lector esta es verificada por un soldado que valida la identidad de quien porta el carnet, por medio de la presentación de la cedula de ciudadanía o cedula militar, así mismo en la entrada a las oficinas más sensibles hay instaladas biométricas de huella para el ingreso a estos sectores, esta combinación de sistemas ha mostrado resultados positivos, ha disminuido la intrusión de personal ajeno a

las instalaciones y dentro de las estadísticas no se tiene referencia de haberse presentado atentados desde su puesta en funcionamiento.

Por las ventajas y resultados que los sistemas de control de acceso ofrecen, es recomendable instalarlos en la entrada de los cuarteles militares, con la combinación de estos sistemas y un control oportuno por parte del comandante de guardia y sus subordinados se disminuye el riesgo de intrusión de personal no autorizado, así como la fuga y pérdida de material e información, por las condiciones de la mayoría de las unidades militares y por los resultados observados en algunos sitios que se encuentran instalados, lo más adecuado a instalar es un sistema de carnet con chip que al ser leído active la entrada por un torniquete o jaula, este sistema puede ser combinado con la instalación de biométricas a la entrada de los sitios más sensibles.

Otro sistema que puede ser instalado en los cuarteles militares es un sistema de identificación biométrica la cual puede ser de huella o iris, en vista a que son las de mejores resultados, más fáciles de instalar, mantener y utilizar, previo a la instalación de cualquiera de los sistemas mencionados se hace necesario inicialmente hacer un estudio para observar aspectos de seguridad como la cantidad de personal que entra y sale del cuartel, los sistemas existentes, los costos, horas en las cuales más ingresa personal y otros aspectos a tener en cuenta según las actividades que se realicen en ese cuartel y el tamaño de este.

Finalmente es de recordar que la tecnología es una herramienta fundamental a utilizar por las organizaciones, pero ningún sistema funciona solo, todos deben ser correctamente administrados y verificados por el hombre, para obtener excelentes resultados, a igual

conclusión se llegó en la catedra de seguridad electrónicaal observar y analizar diferentes sistemas de control de acceso existentes.

Conclusiones

Al colocar sobre la balanza los recursos a invertir en seguridad en un sistema adecuado de control de acceso y las graves consecuencias que pueda traer para la Institución Militar la materialización del riesgo de pérdida, fuga o robo de información y material ampliamente esta se inclina para el lado de la inversión.

La información y material reservado manejado en las guarniciones militares son elementos que tiene relación directa con la seguridad Nacional de allí su cuidado y preservación, los sistemas de control de acceso bien administrados son herramientas que permiten obtener excelentes resultados y reducir los riesgos mencionados.

La fuga o robo de información y material puede causar la pérdida de vidas humanas, razón por la cual la inversión de recursos en la instalación de sistemas y dispositivos que permitan tener control sobre los activos tangible e intangible no se debe considerar como un gasto, por tal razón todas las unidades militares de Colombia deberían contar con un sistema para controlar el acceso a sus instalaciones, este sistema complementado con la oportuna acción de los servicios de la unidad militar permiten prevenir que personas no autorizadas ingresen a sitios restringidos.

Bibliografía

TECNOLOGÍA XUE. (ND). *Control de acceso*. Recuperado de:
www.xue.com.co/soluciones/control-de-acceso

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

DOINTECH. (2012). *Sistemas de control de acceso*. Recuperado de:
www.dointech.com.co/control-de-acceso-html

INDITAR. (2002). *Soluciones de control de acceso y presencia*. Recuperado de:
www.inditar.com/control-accesos/sistemas-de-control-de-acceso-php

SYON SOLUCIONES & IDENTIFICACIÓN. (ND). *Control de accesos*. Recuperado de:
www.syon.es/soluciones/control-de-accesos/

SYON SOLUCIONES & IDENTIFICACIÓN. (ND). *Control de presencia y accesos*.
Recuperado de: www.syon.es/productos/control-de-presencia-y-accesos/

PROSEGMAN S.A DE CV. (2014). *Sistemas de control de acceso*. Recuperado de:

<http://www.prosegman.com/productos/List/listing/sistemas-de-control-de-acceso-93/1>

ALSE MEXICANA S.A DE C.V. (ND). *Sistemas de control de acceso*. Recuperado de:

www.alsemexicana.com/control-de-acceso/control-de-acceso.html

INTEGRALARM. (ND). *Como funciona un control de acceso*. Recuperado de:

www.integralarm.com.mx/index.php7como-funciona-acceso

INSTITUTO NACIONAL DE TECNOLOGÍAS EDUCATIVAS Y FORMACIÓN DEL PROFESORADO. (ND). *Sistemas biométricos de seguridad*. Recuperado de: de.rekursostic.educacion.es/observatorio/we/es/cajón-de-sastre/1045-sistemas-y-biometricos-de-seguridad

CUADERNO RED DE CÁTEDRAS TELEFÓNICA. (2011). *Cátedra telefónica de la Universidad de las Palmas de Gran Canaria, sistemas biométricos*. Recuperado de: http://www.rcysostenibilidad.telefonica.com/blogs/documentoscatedras/files/2012/07/Catedra_telefonica_Sistemas_Biometricos.pdf

LOPEZ, N., & TORO, J. (2012). *Técnicas de biometría basadas en patrones faciales del ser humano*. Universidad Tecnológica de Pereira, Pereira, Colombia.

BIOMETRÍA. (2006). *Reconocimiento facial*. Recuperado de.

www.biometria.gov.ar/metodos-biometricos/facial.aspx

T2APP. (1996-2013). *Terminales de control presencia, control de acceso y control producción*. Recuperado de. www.t2app.com

SISBIOCOL. (2014). *Técnicas biométricas*. Recuperado de.

<http://sistemasbiometricos.co/blog/tecnicas-biometricas>

LUMIDING. (2001-2014). *Productos*. Recuperado de.

<http://www.lumidigm.com/es/products/>