# TENDENCIAS DE LA SEGURIDAD ELECTRONICA Y SU IMPACTO EN LA SEGURIDAD PRIVADA.

**Presentado por:**

**JORGE EDUARDO MOLINA CUELLO**

**Trabajo de grado como requisito para optar el título de:**

**Especialista en Administración de la Seguridad**

**Tutor:**

**Ing. FERNANDO ANTONIO MORENO FORERO**

**UNIVERSIDAD MILITAR NUEVA GRANADA**
**FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD**
**ESPECIALIZACIÓN EN ADMINISTRACIÓN DE LA SEGURIDAD**
**BOGOTA 2017**

**INDICE**

**Resumen**

Hoy día se observa desde una posición perceptiva para algunos, o tal vez de realidad para otros, que la tecnología avanza de tal manera, que de una u otra forma coloca en duda las capacidades del ser humano en el sector de la seguridad privada (labor de medios no de resultados) y de cualquier ocupación en general, acarreando como consecuencia la implementación de medios electrónicos para que las personas puedan desempeñar su trabajo. En el presente escrito se definen tendencias de la Seguridad Electrónica en el campo de la Seguridad Privada haciendo énfasis en la protección de los activos, incluyendo a las personas de la organización, además analizar en qué aspectos o hasta qué punto la Seguridad Electrónica pudiese ocupar espacios, ocupados hasta el momento por las personas, señalando las posibles limitaciones, posibilidades y relación entre ambas. El uso de la tecnología en el medio de la seguridad es más evidente, encontramos diferentes sistemas que nos alertan ante una amenaza pero detrás del sistema existirá alguien que lo supervise. La motivación para adentrarnos en el tema, es la de confiar de nuestras capacidades profesionales y complementar nuestro trabajo con el mundo tecnológico.

**Palabras clave:** Seguridad Electrónica, Seguridad Personal, Seguridad Privada, Tecnología, Medios tecnológicos.

**Abstract**

Nowadays, it is observed from a perceptive position for some, or perhaps reality for others, that technology advances in such a way that in one way or another the capacity of human being's in the private security sector are questioned (work of means and not of results) and of any occupation in general, resulting in the implementation of electronic means for people to carry out their work. This paper defines the trends of Electronic Security in the field of Private Security with emphasis on the protection of people and assets of the organization, as well as analyzing in which aspects or to what extent Electronic Security could occupy spaces defined with respect to the people, indicating the possible limitations, possibilities and relation between both. The use of technology in the medium of security is more evident, we find different systems that alert us to a

threat but behind the system, there will be someone to supervise. The motivation to delve into the subject is to trust our professional skills and complement our work with the technological world.

**Key words**: Electronic Security, Personal Security, Technology, Technological means.

## Introducción

Actualmente, la constante evolución de la tecnología ha generado cambios en la sociedad, lo que obliga a las empresas a tecnificar y/o posiblemente reemplazar al ser humano, con el propósito de disminuir los costos en la mano de obra, con la implementación de sistemas electrónicos. Sin embargo, en países desarrollados se evidencia los impactos que surgen de la implementación tecnológica como la reducción de miles de empleos, y que al mismo tiempo, nace la oportunidad de crear nuevos empleos.

Esto denota la importancia de la automatización a través de la tecnología según Restrepo:

"La automatización a través de la tecnología nos ha hecho la vida más fácil para el ser humano, sin embargo, no es tan evidente la amenaza que genera para muchos de nosotros y el mayor riesgo que tenemos de perder nuestro trabajo por culpa de integración en los sistemas electrónicos. Los aparatos electrónicos sólo requieren mantenimiento para trabajar, y no seguro de salud, seguro de vida, fondo para retiro, ni días de vacaciones o de enfermedad, además del riesgo que mitigan las empresas de tener un mal empleado". (2017)

Resulta incierto decir hasta qué punto, la Seguridad Privada con el empleo de personas podría ser reemplazada por la Seguridad electrónica, pero la idea tampoco es entrar en un estado de incertidumbre al saber que con la modernización probablemente se estaría a la merced de quedar desempleados, o la preparación para el cambio. Estos equipos requieren más que mantenimiento, supervisión, programación, configuración, parametrización, adicional las labores de seguridad van a requerir siempre actividades de valoración, de criterio, de buen juicio y sobre todo de toma de decisiones, que un equipo electrónico no lograra.

Si bien no se tiene certeza del impacto de la Seguridad electrónica (SE) con respecto a la Seguridad Privada (SP) con las personas que laboran en el sector, el mundo moderno evidencia un sin número de tecnologías que están a la vanguardia, como son los Sistemas Integrados Electrónicos, la Inteligencia Artificial, las máquinas para desarrollar distintas tareas, los robots, el software video-analítico que incorporan Circuito Cerrado de Televisión (CCTV), los drones, etc. Se puede apreciar que los sistemas electrónicos cumplen un papel importante en el sector de la Seguridad privada, por eso se habla de sistemas integrados productos de la solución e innovación de las estrategias de las empresas. Sin embargo, no es evidente aún el impacto que

tiene la Seguridad electrónica en las personas y en los procesos realizados tradicionalmente (con personas) por las organizaciones. La industria de la Seguridad para ser vigente en el tiempo debe considerar las tendencias de la Seguridad electrónica que se relaciona con la persona y que tiene un impacto en el desarrollo de la Seguridad Privada. Las soluciones integrales en los sistemas de Seguridad electrónica trasfieren tareas para la protección de bienes o activos, realizadas habitualmente por operadores humanos a un conjunto de elementos tecnológicos. Es por eso que se puede plantear la siguiente pregunta:

¿Cuál es la tendencia de la Seguridad Electrónica y su impacto a la Seguridad Privada?

El propósito de este escrito es analizar la evolución de los Sistemas integrados en Seguridad electrónica (SE) tendencias e impacto que se pueden presentar en la Seguridad Privada, exponiendo el desarrollo de la Seguridad electrónica en la actualidad, cuáles serán los posibles aspectos y procesos en los que la Seguridad electrónica podría impactar el desempeño del personal de seguridad privada. Además, determinar los límites y las posibilidades actuales de la seguridad electrónica en el sector de la Seguridad Privada y la identificación de herramientas que se pueden emplear para la aplicación de la Seguridad electrónica en el sector de la seguridad privada.

# 1. La industria de la Seguridad Electrónica

## 1.1 Integración de la Seguridad Electrónica en la Seguridad Privada

### Normatividad.

Para incorporar los sistema de seguridad electrónica en la seguridad privada existen normas que reglamentan la aplicación de medios tecnológicos en áreas residenciales, empresas, establecimientos comerciales, financieros, e industriales. La función de la vigilancia privada es de medios, más no de resultados, los servicios de vigilancia son responsables, en el momento en el que este falle en la aplicación del protocolo de seguridad establecido y se incumplan con los acuerdos y compromisos adquiridos en el contrato de prestación de servicio.

Por consiguiente la superintendencia de vigilancia y seguridad privada ha emitido un protocolo para la regulación de la vigilancia electrónica con los objetivos de:

- Mejorar la calidad en la prestación de los servicios de vigilancia y seguridad privada, asegurando un adecuado nivel técnico y profesional.
- Establecer las condiciones mínimas de prestación del servicio de vigilancia electrónica.
- Brindar una adecuada protección a los usuarios de servicios de vigilancia y seguridad privada, a través de reglas claras en la prestación de los servicios, con personal calificado, procurando optimizar los recursos y la mejora en la prestación del servicio.

Por otro lado según el protocolo “se relaciona quienes son los responsables para la aplicación de la vigilancia electrónica, cuales son las condiciones generales para la prestación del servicio de seguridad y vigilancia privada – vigilancia electrónica, condiciones específicas para la prestación del servicio de vigilancia y seguridad privada – vigilancia electrónica teniendo en cuenta procedimientos de funcionamiento, otras condiciones para la prestación de servicios y recomendaciones”.

**Integración.**

A través del protocolo se refleja que la vigilancia electrónica depende de procesos interrelacionados que prestan apoyo a la seguridad privada, y que hasta el momento deben ser operados y controlados por personas idóneas en el campo de los sistemas electrónicos. En efecto se necesita personal más capacitado: La incorporación de la tecnología como quedó dicho, será una variante casi obligatoria para las empresas que quieran permanecer y ganar nuevos nichos de mercados. Pero para lograrlo deberán, a la par que desarrolla su departamento tecnológico, comenzar a capacitar a sus empleados en el uso y los beneficios de los equipos. La necesidad de perfeccionar el entrenamiento de los involucrados en este sector, no muy diferente a la requerida en muchos otros sectores económicos en Colombia y Latinoamérica, es clara. Hablamos aquí tanto de entrenamiento en habilidades operativas, como también de habilidades gerenciales para quienes conducen la organización. La Seguridad Electrónica ha influido para que las empresas de Seguridad Física amplíen sus límites y neutralicen algunas de las vulnerabilidades que aparecían en sus operaciones de salvaguarda, procurando una mejor calidad de vida tanto para el vigilante como para los que contratan estos servicios.

## 1.2 Labores en las que posiblemente es reemplazado el ser humano con ayuda de herramientas tecnológicas

Las herramientas tecnológicas complementan el trabajo de los operadores a todo nivel en Vigilancia Privada, tanto así, que ahora se pueden encontrar diferentes subsistemas que integran la Seguridad Electrónica y que facilitan la labor cotidiana para prestar un servicio eficiente, y además, con respaldo ante cualquier eventualidad. A continuación se relacionan algunos de los sistemas electrónicos de seguridad que están siendo aplicados actualmente:

**a. Protección perimetral (Barreras físicas).**

Un sistema de barreras es cualquier tipo de obstáculo siempre y cuando cause unos impactos directos en la velocidad, tiempo y herramientas necesarios para sortearlo. Las barreras pueden ser elementos naturales del sitio, elementos estructurales prefabricados; pueden ser pasivas o temporales (desplegables). Las barreras más rentables son aquellas que ya existen como parte del sitio, o que

están previstas como parte de un nuevo sitio o dl diseño de las instalaciones. Las barreras pueden proporcionar todas o algunas de las siguientes funciones:

- Demarcación de los límites legales delos locales.
- Entrada canalizada a través de una zona segura, al impedir la entrada por cualquier otro punto de los límites.
- Una zona para instalar detección de intrusos, sistemas de vigilancia, sistemas de iluminación y personal de vigilancia.
- Impedir a personas no autorizadas la entrada a la zona asegurada;
- Forzar al intruso a demostrar su intención de entrar a la propiedad.
- Retraso en el acceso, aumentando por tanto la posibilidad de detección y respuesta.
- Entre otras. (ASIS,2009, p. 39)

**b. Control de Acceso.**

Los programas de control de acceso son instituidos para permitir o denegar la entrada de personas, vehículos y paquetes a determinados lugares de las instalaciones; incrementa o reduce la rata o densidad de movimientos y protege a personas, materiales e información contra la remoción y observación no autorizada previniendo pérdidas de personas y materiales.

Un sistema de control de entrada permite el movimiento de personal autorizado y material dentro y fuera de las instalaciones, detectando y retardando el movimiento de personas y bienes no autorizado. Los elementos de control de entrada pueden ser encontrados en el límite o perímetro de una instalación, tales como entradas de vehículos, punto de entradas a los edificios o puertas de ingreso a una habitación u otras áreas especiales dentro de un edificio. (García, 2008)

**c. Monitoreo de Alarmas**

El objetivo de una estación de monitoreo es identificar los eventos detectados por el sistema de alarma instalado y tomar una acción pertinente. Esta acción puede ser: dar aviso a la policía de un robo detectado, a un técnico para la reparación del sistema o a un supervisor de guardia para corregir algún problema en la línea de

montaje de una fábrica, es decir, el monitoreo aumenta el nivel de seguridad y productividad de una propiedad protegida haciendo de enlace entre el propietario y las autoridades pertinentes o la comunicación a distancia entre las máquinas y los usuarios. (Gau Barrera, S.F)

**d. Sistema GPS**

G.P.S. (Global Position System) es un sistema de navegación global basado en 29 satélites, 24 activos y 5 de backup. Originalmente fue desarrollado sólo con fines militares y con el correr de los años se extendió su uso hacia aplicaciones civiles.

La seguridad conceptualmente se ha extendido; no solo es un asunto de robo de vehículos. Podemos actualmente, controlar y monitorear flotas, proteger mejor las mercancías en tránsito, los servicios prestados, incluso la integridad del personal que interviene diariamente. Las empresas hoy buscan minimizar los incidentes, no solo por el cuidado de sus bienes y su gente, sino también buscan atender mejor a sus clientes y respaldar sus marcas.

La tecnología de Monitoreo GPS permite todo esto. A través de su combinación con Internet, se puede tener una visualización en tiempo real de flotas completas desde su propia computadora conectada a Internet y confirmar todo tipo de avisos, alarmas y reportes. (Fuente: www.trend-tek.com )

**e. Control vehicular**

AVL (por sus siglas en inglés), o Localización Vehicular Automatizada, es el sistema más utilizado para el monitoreo y localización de vehículos, personas u objetos y se utilizan dos tecnologías distintas en un mismo equipo: GPS y GSM/GPRS. La tecnología GPS utiliza la triangulación de señales de por lo menos cuatro de los veintisiete satélites geoestacionarios alrededor del planeta, pudiendo recolectar los datos de la ubicación exacta donde se encuentra el vehículo, pudiendo también obtener datos de su velocidad, altitud, sentido de dirección, fecha y hora, etc. Esta información capturada por el GPS es enviada por medio de una operadora celular (SIM CARD) utilizando la tecnología GSM/GPRS a un software de rastreo. Éste, por lo general, posee la cartografía

local o mundial, según el caso, para poder visualizar el vehículo en el mapa. Acompañando el avance de la tecnología, en la actualidad los equipos AVL cuentan con muchas funciones adicionales, que permiten a la estación de monitoreo o dueño del vehículo poder obtener un control total de su flota. Algunos ejemplos:

• Permite identificar qué conductor está conduciendo en cada momento.
• Sensor de temperatura, para mantener una cadena de frío.
• Captura de imagen.
• Sensor de combustible.
• Sensores de puertas y pulsadores de pánico.
• Escucha cabina.
• Emitir un aviso sonoro ante exceso de velocidad.
• Permite accionar el bloqueo de motor a distancia.
(Fuente http://www.rnds.com.ar/articulos/109/RNDS_096-98W.pdf)

**f. Protección de activos.**

El contexto de la protección de activos – cuando se aplica a un sistema de gestión de la protección física de activos (PAMS, por sus siglas en ingles)- considera los riesgos asociados con los sucesos intencionados, involuntarios y/o los causados de manera natural. La protección de activos incorpora las funciones de seguridad y funciones relacionadas de la organización (por ejemplo, la gestión del riesgo, de la seguridad financiera, el aseguramiento de la calidad, la conformidad, etc.) a un sistema de gestión exhaustivo y proactivo.

La protección de activos está directamente ligada con la misión de la organización de proteger sus activos tangibles e intangibles eliminando o reduciendo la exposición a las causas y consecuencias de los riesgos. El sistema de gestión de la organización debería:

- Asegurarse del liderazgo y el compromiso de la alta dirección con la política de la protección física de activos.

- Establecer un programa exhaustivo de gestión del riesgo que identifique, analice y evalué los riesgos de los activos tangibles e intangibles.
- Caracterizar los activos, el diseño y la implementación de un sistema de protección físico que cumpla los objetivos con respecto a los recursos disponibles.
- Integrar personas, procedimientos, tecnologías y equipamientos para cumplir los objetivos.
- Hacer el seguimiento, medir y revisar continuamente el desempeño del sistema de gestión. (ASIS, 2009, p.15)

**g. Sistemas de video – Videovigilancia**

En esta era de seguridad integrada, los sistemas técnicos y físicos se combinan para permitir la evaluación informada de situaciones que se producen en ubicaciones remotas. La videovigilancia es una herramienta de evaluación que puede ayudar en la gestión de las funciones de seguridad. Los sistemas de videovigilancia pretenden ser una herramienta de evaluación o de documentación visual. Las cámaras de videovigilancia se instalan por una o más razones principales:

- Vigilancia en directo
- Reconstrucción después de un suceso.
- Disuasión
- Evaluación de cualquier alarma activada para determinar la causa e iniciar la respuesta apropiada. (ASIS, 2009, p.45)

**h. Detección y extinción de incendios.**

La lucha contra los incendios, tanto en su faceta de prevención (medidas adoptadas para que no se produzca un incendio) como de protección se pueden llevar a cabo de dos formas: **activa y pasiva**.

- La **protección activa** incluye aquellas actuaciones que implican una acción directa en la utilización de instalaciones y medios para la protección y lucha contra los incendios. Por ejemplo: La evacuación, la utilización de extintores, sistemas fijos, etc.

- La **protección pasiva** incluye aquellos métodos que deben su eficacia a estar permanentemente presentes pero sin implicar ninguna acción directa sobre el fuego. Estos elementos pasivos no actúan directamente sobre el fuego pero pueden compartimentar su desarrollo (muro), impedir la caída del edificio (recubrimiento de estructuras metálicas) o permitir la evacuación o extinción por eliminación de humos. Este tipo de protección es quizás la faceta más importante en la lucha contra el fuego si bien es también la más olvidada por las dificultades de aplicación que conlleva y por los condicionantes que introduce en el diseño.
  (Fuente http://www.rnds.com.ar/articulos/014/RNDS_056W.pdf)
- **Plan de evacuación**

  Es el conjunto de acciones y procedimientos óptimos que establecen una distancia ideal entre la fuente del riesgo y la comunidad amenazada, mediante el desplazamiento de la comunidad a través de rutas seguras en tiempo mínimo a un sitio seguro o punto de encuentro.
  Las evacuaciones se realizan en caso de: Incendio, Amenaza Terrorista, Inundación, Deslizamiento o Sismo, Terremoto y Huracán. (Fuente http://www.rnds.com.ar/articulos/034/RNDS_162W.pdf)

**i. Medios de Comunicación.**

Antes de adentrarnos en los sistemas de transmisión de datos en redes repasaremos el concepto básico de comunicación a través de sus componentes:

• Emisor y receptor identificados
• Medio de comunicación (cara a cara, telefónicamente, mensaje escrito, etc.)
• Protocolo de comunicación (idioma, codificación de símbolos gráficos, lenguaje gestual, etc.)

Desde el nacimiento de las computadoras, se conectaban dos o más equipos para poder pasar información de unos a otros con el fin de informar, compartir información para ampliar la capacidad de almacenamiento y/o no repetir innecesariamente los mismos datos. Una constante búsqueda de optimización de

este sistema de envío y acceso a la información fue el origen de las redes de datos, así como su constante evolución.
(Fuente http://www.rnds.com.ar/articulos/protocolos de comunicación)

**j. Medios de Transmisión**

Ante la vulnerabilidad de las líneas telefónicas terrestres, las empresas de monitoreo y los propios usuarios comenzaron a preguntarse cómo evitar la pérdida del vínculo de comunicación. Como causa de ello nacieron los back-up para celulares; hoy las alternativas que ofrece la tecnología plantean nuevos desafíos: qué canal es el más seguro, económico y transparente para la transmisión de los eventos generados por un panel de alarmas. (Fuente http://www.rnds.com.ar/articulos/030/RNDS_074W.pdf)

**k. Medios de Iluminación.**

La iluminación de seguridad permite al personal de seguridad mantener la capacidad de evaluación visual de los activos durante las horas de oscuridad. La iluminación de seguridad proporciona los elementos de disuasión y detección. Como objetivos de la iluminación de seguridad indicados por ASIS International en su libro "Sistemas de gestión de la seguridad; protección física de los activos", a continuación hace referencia a algunos de estos:

- Debería haber un alto contraste de brillo entre el intruso y el fondo.
- Deberían iluminarse los límites y sus proximidades.
- Deberían iluminarse las superficies y estructuras.
- Los niveles de iluminación deberían cumplir los requisitos legales, reglamentarios y normativos.
- La iluminación debería ser integrada con los sistemas de vigilancia.
- La reproducción de color debería respaldar la operación de los sistemas de videovigilancia.
- Entre otros.

**Convergencia de la Seguridad**

La convergencia de la seguridad es un proceso gestionado que aplica los principios de la gestión del riesgo de seguridad a la convergencia Protección Física de Activos (PAP por sus siglas en inglés) individuales y a su integración en los sistemas de seguridad empresariales y en los procesos de gestión del riesgo empresarial de la organización. Esto crea un único proceso integrado gestionado, ajustado para cumplir los requisitos generales de seguridad de la organización, que sirve para proporcionar una mayor protección frente a los riesgos de seguridad de la organización. (ASIS, 2009, p.33)

El concepto de integración de sistemas se planteó desde el nacimiento de la seguridad electrónica. Se hace posible hoy gracias a la presencia de grandes corporaciones, capaces de implementar los medios para manejar, desde un mismo control, los diferentes rubros que integran la seguridad. Distintos especialistas analizan y explican de qué se trata la integración y cuáles son las posibilidades de implementarla. La integración de sistemas logra reducir los costos de administración por mantener sistemas independientes, eliminando cargas redundantes no deseadas. De esta manera se obtiene un mejor control con un nivel de centralización mayor.
(Fuente http://www.rnds.com.ar/articulos/022/RNDS_058W.pdf)

**Los drones como herramienta de aplicación de la Seguridad electrónica.**

"Como es por muchos conocidos los vehículos aéreos remotamente tripulados RPAS, son comúnmente conocidos como drones. Estos han tenido un desarrollo industrial importante durante la última década, de tal forma que hoy en día son un importante foco de estudio para diferentes entidades como universidades, estados, consultores e inversionistas. El concepto de RPAS se ha derivado de la industria aeronáutica, combinado con los avances tecnológicos, como la miniaturización de la electrónica y la versatilidad aérea; por lo que gracias a ello se han empezado a explotar los drones en diversas aplicaciones. El desarrollo drone no es ajeno a Colombia, de hecho ya existen varias compañías en el país con representación directa de los grandes productores de RPAS del mundo, además hay compañías dedicadas a desarrollar este tipo de aeronaves remotamente tripuladas como "Made in Colombia" y múltiples empresas que ofrecen servicios básicos o altamente especializados con RPAS, de tal forma que se han creado

asociaciones que agrupan dichas compañías desde diversos intereses y se esfuerzan por el reconocimiento nacional como gremio y nuevo sector productivo, promoviendo la organización y las buenas prácticas, buscando atraer inversión". (Parra, 2017)

Teniendo en cuenta las crecientes necesidades de implementar seguridad por medio de video en situaciones como desastres naturales, misiones de rescate, contraterrorismo o de carácter militar, Hikvision creó el Drone UAV-MX 4080A Falcon Series por ejemplo. El funcionamiento de este equipo se realiza por medio de un control de señal que administra la dirección del vehículo aéreo en hasta 2km de distancia. Además, transmite el video HD a una estación en tierra que puede instalarse a hasta 10km de distancia, lo que significa que puede volar en longitudes no mayores a 10.000 metros alrededor de la estación tierra. A su vez, la estación transmite a través de 4G o cable la información de video a la central de monitoreo del cliente. Por su parte, la estación en tierra de estos equipos permite la revisión en tiempo real y visualización de los datos de vuelo, la transmisión de imágenes en microondas digital y es conectable a la red vía 4G, Wi-Fi o interface de red.

El Drone puede alcanzar una velocidad máxima en vuelo de 80km/h. Además, fue diseñado con el objetivo de evitar que seres humanos hagan reconocimientos de áreas inseguras, peligrosas o que pongan en riesgo su integridad física.

Finalmente, el UAV MX4080A es capaz de brindar valor agregado a sistemas de seguridad en aplicaciones cercanas a áreas marítimas o cuerpos de agua en los que se dificulta instalar equipos de vigilancia.

**Los Robots instrumentos para uso de la Seguridad Electrónica.**

Alrededor de la última década hemos considerado el impulso que las tecnologías, calculando cual será el alcance y/o la eliminación de la participación humana en los empleos donde tradicionalmente se desempeña la población. Pero como puede afectar el desarrollo de la ciencia la posibilidad de que los guardias de seguridad humanos puedan ser reemplazados?:

En un estudio separado por el Dr. Carl Frey de la Universidad de Oxford, se predijo que la automatización del trabajo resultante del uso de robots representaría hasta el 47 por ciento de los empleos existentes en Estados Unidos en "alto riesgo". En un ejemplo mucho más espeluznante, Kokoro de Japón, ha introducido los robots humanoides que

cree pueden substituir a recepcionistas humanos en oficinas. Mejor aún, ¿ha visto el interior de una moderna planta de fabricación recientemente? Aunque todavía imaginamos un lugar donde los trabajadores humanos trabajan en las líneas de montaje, la mayoría de las veces eso está lejos de la verdad. De hecho, la mayoría de las líneas de montaje están ahora mecanizadas al 100%; Incluso la mayoría de los coches se hacen con menos de 24 horas de trabajo humano. Aunque los guardias de seguridad no son uno de los ejemplos dados arriba, no pasará mucho tiempo antes de que veamos los primeros guardias de seguridad robóticos, pero esperemos..., eso ya está sucediendo. ¿Es posible que los robots puedan ayudar a resolver problemas como la falta de capacitación, la rotación alta y los bajos salarios? Aquí hay tres ejemplos de tecnologías que podrían reemplazar un día a los guardias de seguridad humanos (Sparkman, 2015*).*

**Bob** es el primer guardia de seguridad robótico del Reino Unido. Bob patrulla la sede de G4S en Gloucestershire, y forma parte de un proyecto piloto de 12,2 millones de dólares para la Universidad de Birmingham. El objetivo del proyecto de la universidad es colocar robots en oficinas en todo el mundo. La historia de Bob hace referencia en Gran Bretaña donde hoy día a todos los policías se conocen comúnmente como“Bobbies”.
Originalmente, sin embargo, se les conocía como 'Peelers' en referencia a un tal Sir Robert Peel (1788 - 1850). Su legado permanece mientras los 'Bobbies' británicos patrullen las calles y mantengan a la población a salvo de los malhechores; y ayuden a los turistas perdidos a encontrar el camino de regreso a la comodidad de sus hoteles.

La Vigilant **Mobile Camera Platform (MCP)** es otro ejemplo de un guardia de seguridad robótico móvil. El Vigilant MCP fue desarrollado por la Dra. Louise Gunderson y el Dr. Jim Gunderson de Gamma 2 Robotics.
Según el sitio web de la compañía, su robot cumple tres necesidades de alto nivel que una compañía de guardias de seguridad tendría para tal robot. Esos requisitos son asequibilidad, autonomía y fiabilidad.
El último de nuestra lista de posibles contendientes para reemplazar a los guardias de seguridad humanos es Junior. **Junior** es un pequeño robot que está siendo desarrollado por Roambotics, Inc. Junior está actualmente en desarrollo y orientado hacia el mercado de la seguridad en el hogar, pero también veo su uso en aplicaciones comerciales.

Al igual que Bob, Junior podrá aprender a adaptarse a su entorno utilizando sus sensores de a bordo y cartografiar el entorno en el que funciona. Según el CEO y fundador de Roambotics, Scott Mentor, "... nuestro software utiliza el aprendizaje automático para ser más inteligente ahora".

## 2. Tendencias en los Sistemas de Seguridad Electrónica

En las empresas e instituciones la Seguridad Electrónica se basa en el uso de tecnologías de última generación, lo que incluye sistemas CCTV, controles de acceso, sistemas de intrusión, control de activos y centros de control de alarmas, etc. En este terreno no hay que olvidar la protección contra incendios. Su finalidad es prevenir las pérdidas y daños producidos por el fuego, impidiendo que éste se propague y ponga en peligro la vida de las personas y bienes. Aquí las TIC permiten la protección activa, la protección pasiva, la señalización y el alumbrado de emergencia o la megafonía de emergencia y evacuación.

La importancia de la videovigilancia es evidente. Millones de cámaras de televisión y vídeo están instaladas por todo el planeta en empresas, tiendas, calles, aeropuertos, parques, centros comerciales, instalaciones de alta seguridad, urbanizaciones, etc. La mayoría de las cámaras utilizadas son de alta definición y se conectan con las redes existentes vía protocolos IP. Incluyen muchas opciones para comparar objetos de forma automática por su tamaño, color o velocidad de movimiento, para programarlas a fin de que desencadenen acciones en función de las imágenes (movimiento, humo o fuego, personas caídas en el suelo, comportamientos anómalos, etc.), para coordinar varias cámaras y hacer un seguimiento de todos los movimientos de una persona dentro de un edificio o un área pública, etc. (Roca, 2015)

### 2.1 La evolución de los sistemas de Seguridad Electrónica y su tendencia.

Abraham Maslow posiciona la seguridad como una de las necesidades básicas del hombre, dentro de una teoría sobre la motivación humana (en inglés, A Theory of Human Motivation) de 1943, Necesidades de seguridad y protección. Estas surgen cuando las necesidades fisiológicas se mantienen compensadas. Son las necesidades de sentirse seguro y protegido; incluso desarrollar ciertos límites de orden. Dentro de ellas se encuentran: Seguridad física y de salud. Seguridad de empleo, de ingresos y recursos.

Seguridad moral, familiar y de propiedad privada. Para ello las sociedades, al transcurrir el tiempo, han encontrado la necesidad de procesar y transformar la Seguridad Personal por medios tecnológicos, con el fin de prestar un mejor servicio. En este orden es necesario responder a este interrogante ¿Que es la Seguridad electrónica?

Según José Miguel Roca: es la aplicación de las Tecnologías de la Información y la Comunicación (TIC) a las actuaciones de seguridad física (2015). De igual forma un sistema de seguridad electrónica será la interconexión de recursos, redes y dispositivos (Medios técnicos activos) cuyo objetivo es precautelar la integridad de las personas y su entorno previniéndolas de peligros y presiones externas (Cevallos, 2011). También se obtienen diferentes tipos de sistemas electrónicos aplicables en la actualidad por las organizaciones, desde un CCTV, hasta sistemas de identificación de reconocimiento de rostro que puedan detectar una posible intrusión. La transformación y el desarrollo de los medios tecnológicos están en constante lucha en el mercado por repuntar en la era digital y alcanzar su máxima cúspide para que el usuario final "consumidor", quien confirmara a satisfacción si los productos a utilizar en la protección de sus activos o patrimonio. Las principales funciones de un Sistema de Seguridad Electrónica son: la detección de intrusos en el interior y exterior, el control de accesos y tráfico (personas, paquetes, correspondencia, vehículos, etc.), la vigilancia óptica mediante fotografía o CCTV, la intercomunicación por megafonía y protección de las comunicaciones.

En este momento la innovación y la automatización en la vida cotidiana es una necesidad para las personas y empresas, porque la amenaza no da espera, quien se encuentra incesante en la preparación de distintas técnicas y tácticas para llevar a cabo el delito, sin importar las consecuencias; en el presente muchos denotan, argumentan inclusive, que el adversario va a la vanguardia de los sistemas de seguridad, vulnerando, por necesidad las instituciones, alcanzando de esta manera su objetivo, donde ni siquiera las entidades estatales, pueden prevenir o actuar de una manera eficiente para prevenirlo. Al mismo tiempo se observa que las grandes organizaciones procuran invertir en seguridad, y es así, que el señor David Chong dispone bajo esta perspectiva: 'la contratación de servicios de seguridad, como cualquier otro ejercicio presupuestal, enfrenta la decisión de cuánto gastar y de qué manera. Y aquí es precisamente donde, bajo una premisa de "hacer más con menos", surge ese tentador espejismo de "lo más barato"

en lugar de “lo más adecuado”, si no se tiene claro lo que se quiere o lo que en realidad se necesita’ (2010). En realidad la integración de los sistemas en el sector público y privado se hacen necesarios para combatir la criminalidad, puesto que atacar desde un solo lado las amenazas sería casi imposible.

## 2.2 Tendencias de impacto en seguridad y videovigilancia para 2017

Tendencias tecnológicas que impactarán en el sector de la seguridad y videovigilancia en 2017, de acuerdo al análisis presentado por la señora Lizzette Pérez, así:

**1.** Seguridad como Servicio: Se espera que los clientes dejen de pensar en la videovigilancia como una colección de hardware y software conectado a una red. En su lugar, se empezará a visualizar como un servicio: remoto y profesional, con almacenamiento y monitoreo de videogestionado desde el lugar donde se encuentre el operador.

Esto no sólo constituye una reducción de costos sino que también significa una mejora en el nivel de servicio del sistema, permitirá una mejor administración de los dispositivos y fortalecerá los procesos de seguridad cibernética.

**2.** Soluciones Integradas**:** La industria de la seguridad continuará con la tendencia de ofrecer soluciones específicas para problemas concretos, en lugar de ofrecer un hardware / software único. Al final, los clientes no buscan comprar una cámara, o un sistema de gestión de video; lo que realmente quieren es proteger su patrimonio, los clientes, el personal y, en general, lograr una mayor seguridad, por ejemplo, la reducción del robo en tiendas o hacer un detallado seguimiento de las potenciales amenazas en un aeropuerto.

La convergencia de hardware y software, así como las herramientas de pre y post instalación conllevan al desarrollo de soluciones de extremo a extremo que podrán abordar diferentes situaciones. Esto implicará el diseño de cámaras de alto rendimiento, controles de almacenamiento y acceso, cuidadosamente integrados con las herramientas de administración y análisis de video.

**3.** Uso extenso de los analíticos**:** Mientras la calidad en el video resulta una característica básica de las cámaras de seguridad de hoy en día, en última instancia, la información que se genera debe ser analizada.

Los recientes avances de la tecnología, como la imagen térmica y la mejora de las capacidades para las condiciones de poca luz han sido pasos importantes para el sector. Pero al final, generan más datos que necesitan ser revisados. Por ello, la industria de la seguridad ha trabajado en la innovación para el software de análisis de video, que puede utilizarse en tiempo real para ayudar a los profesionales a tomar decisiones informadas. Se espera para el próximo año (2018) que estas nuevas funcionalidades, incluyendo el reconocimiento facial, análisis forense y protección perimetral, se combinen aún más para brindar un uso más optimizado de los analíticos en tiempo real.

**4.** Aprendizaje Profundo (Deep Learning): Con todos estos datos recolectados, las tecnologías de aprendizaje profundo comienzan a tomar relevancia. Estas usan software de reconocimiento de patrones para 'aprender' sobre diferentes tipos de comportamientos a través de las múltiples cámaras de seguridad instaladas en todo el mundo.

Las técnicas que incorporan la inteligencia artificial tendrán un uso más amplio dentro de la industria de la seguridad. Aunque todos los clientes son diferentes, los entornos y ubicaciones en los que se basan tienden a estar en las mismas categorías generales, con personas que exhiben los mismos comportamientos.

**5.** Más allá del video: La videovigilancia no sólo implica la seguridad de personas, lugares u objetos. También ahora incluye el control de acceso físico, comunicación bidireccional y la gestión de situaciones de emergencia, en paralelo, y que se pueda manejar desde una distancia considerable.

Para ampliar aún más el concepto de integración, 2017 debería ser el año en que las cámaras de seguridad se coordinen también con puertas inteligentes, intercomunicadores y altavoces, a nivel local y remoto. Eso significa soluciones integrales que se pueden controlar en tiempo real, permitiendo que los clientes vean, oigan y hablen con la gente de forma cercana dentro de sus instalaciones.

## 3. Relación de la seguridad electrónica y la seguridad privada.

La mejor forma para que las organizaciones y los humanos se sostengan en el mercado laboral es la capacidad de **adaptarse,** los cambios tecnológicos obligan a las personas a

adquirir nuevas habilidades que contribuyan al desarrollo de las empresas. Empresas, sistemas políticos, educación; estos son solo algunos ejemplos de sistemas que están enormemente obsoletos. Todos fallamos en transmitir el mensaje correcto a aquellos que se esfuerzan por conservar sus empleos y reducir la volatilidad en sus vidas. Al prevenir los cambios tecnológicos y de innovación para que lentamente se integren en nuestras sociedades, solo estamos retrasando el impacto que estos tendrán. Combatirlos puede salvar algunos empleos hoy, pero causará más daño en el futuro (Fonseca, 2017).

Por otro lado la SE y su vinculación en la SP, presenta en el mundo de hoy, una sinergia que se percibe en un choque de quien supera a quien; pero la realidad nos indica que los cambios se están dando y que se debe optar por aprender de las nuevas tecnologías, ajustarse a la Ciencia con el beneficio que trae para las organizaciones y las personas. La Seguridad moderna requiere de los dos campos para que sea efectiva, al momento de responder ante la amenaza. No se puede aislar la SE de la SP y viceversa porque al final una necesita de la otra.

Mary Lynn García indica que un Physical Protection System (PPS) integra personas, procedimientos, y equipo para la protección de bienes o instalaciones contra el robo, sabotaje u otros ataques humanos mal intencionados. Integrar procedimientos es el fundamento para que las organizaciones aseguren sus bienes más preciados, incorporando sistemas electrónicos que anticipen el ataque y el alcance del objetivo de un adversario, pero esto se logra con la participación y la respuesta que el humano pueda proveer en el instante. En este orden de ideas la Seguridad Personal (Como uno de los principios de la seguridad humana se denomina: Centrado en las personas**.** Manifiesta la seguridad humana donde las personas son el centro del análisis y, consecuentemente, se consideran las condiciones que amenazan la sobrevivencia, medios de vida y dignidad de las personas, por el Instituto Interamericano de Derechos Humanos, 2010) en conjunto con la vigilancia privada juegan un papel importante en la capacitación y/o profesionalización de los trabajadores a la hora de evaluar los resultados con el manejo del equipo de seguridad: “toda vez que el conocimiento del oficio con entendimiento del negocio nos lleva a contribuir de forma eficiente en lo objetivos trazados por la organización” (Rodríguez, 2008). Precedentemente a las menciones realizadas por Mary Lynn García y Diofanador Rodríguez, se puede corroborar que los componentes para un

programa de seguridad deben cumplir con medidas específicas de protección, que direccionado bajo las empresas, gobiernos y otras instituciones varían considerablemente de acuerdo a la naturaleza de la organización, las personas y lo que perciben los propietarios como más valorable o crítico. Por otra parte Cunningham y Taylor (1985), refieren que todas las organizaciones, en los programas de seguridad tienen esencialmente tres componentes claves: seguridad física, seguridad en la información y personal de seguridad. Este último componente tiene la función de respuesta que consiste en las acciones tomadas por la fuerza de respuesta para evitar el éxito del adversario. La interrupción es definida como el número de personal de Seguridad que llega al lugar comprometido para detener el progreso del adversario. Esto incluye: la comunicación a la fuerza de respuesta de información apropiada acerca de las acciones del adversario y el despliegue de la fuerza de seguridad (García, 2008).

### 3.1 Impacto que se presenta en la Seguridad Privada

Todo aquel que crea que por incorporar Seguridad Electrónica en un componente de la Seguridad Física tendrá que reducir el personal, está equivocado. La Seguridad Física necesita cada vez más a la Seguridad Electrónica y la SE requiere cada vez más de la respuesta humana. (Foro económico mundial, 2000). En concordancia con la mención anterior permite evidenciar que hay una relación entre el hombre y los sistemas que brindan seguridad, siendo oportuna la necesidad, de que uno depende del otro para cumplir con efectividad en el servicio, cabe aclarar que las empresas que solo se dedican a prestar servicios de vigilantes (guardas), están quedando excluidas porque el mundo actual exige estar alineado con el desarrollo y tendencias de la Seguridad electrónica dentro del marco de la globalización. En la sociedad el término de personal de seguridad es sinónimo de vigilante, guarda o incluso escoltas, pero la realidad es otra, actualmente en Colombia la cifra de vigilantes supera el pie de fuerza de la Policía Nacional y casi que alcanza al Ejercito Nacional, de acuerdo al estudio realizado por la Revista dinero en 2015, manifiesta que: el sector de vigilancia y seguridad es uno de los mayores soportes en materia laboral del país.

A corte de marzo de 2015, un total de 216.151 personas conforman el personal operativo del sector de vigilancia y seguridad privada en Colombia**,** de acuerdo con datos de la Superintendencia de Vigilancia y Seguridad Privada (Supervigilancia).

Esta cifra es cercana a la de los componentes de la fuerza pública nacional. Según un informe del Ministerio de Defensa divulgado en 2014, la Policía Nacional contaba con 176.557 uniformados y el Ejército con 246.325 efectivos. Quiere decir que día a día las empresas que prestan este servicio se ven obligadas a ofrecer un servicio más completo, inclusive un servicio integral incorporando subsistemas de seguridad (Sistema de video – vigilancia, Control de acceso, Protección perimetral, Protección de activos, entre otros); de tal forma que en esta época los clientes exigen el mínimo de errores en la prevención de delitos.

El ser humano por naturaleza cree que todo lo puede manejar y controlar a su alcance, incluso la familia, el trabajo, y tal vez su destino; pero en la Seguridad no se puede dar ese lujo, porque es un asunto que no depende totalmente de sus habilidades, sino que además requiere de sistemas electrónicos, para soportarse en todas las actividades, inclusive en la prevención del riesgo. Hay una realidad cierta, mientras el hombre procura evitar por sí solo, el riesgo (en algunos casos), los sistemas y la seguridad electrónica avanzan, la competencia tecnológica en la actualidad desborda casi, los límites del pensamiento humano.

## Conclusiones

Las Tendencias de la Seguridad Electrónica y su Impacto en la Seguridad privada; en la actualidad, dependen de factores que van mucho más allá de la regulación y la normatividad del Estado, de ahí que el avance tecnológico a trazado una amplitud entre lo que se debe y/o puede controlar y que 'no', por motivos legales; en cierto modo hay una gran brecha para las Entidades reguladoras en el uso de la Seguridad Electrónica (dispositivos electrónicos), y también en la clase de información (software) como parte del funcionamiento de estos medios tecnológicos.

Finalmente se puede concluir lo siguiente:

**PRIMERO:** El diseño para un sistema de protección física (PPS) integra personas, procedimientos, y equipo para la protección de bienes o instalaciones contra el robo, sabotaje u otros ataques humanos mal intencionados. Integrar procedimientos es el fundamento para que las organizaciones aseguren sus bienes más preciados, incorporando sistemas electrónicos que anticipen el ataque y el alcance del objetivo de un adversario, pero esto se logra con la participación y la respuesta que el humano pueda proveer en el instante (García, 2008). La transformación y el desarrollo de los medios tecnológicos están en constante lucha en el mercado por repuntar en la era digital y alcanzar su máxima cúspide para que el usuario final "consumidor", quien confirmara a satisfacción si los productos a utilizar en la protección de sus activos o patrimonio.

**SEGUNDO:** En la actualidad las empresas de diferente naturaleza exploran el mercado, encontrando así la mejor solución integral de seguridad electrónica en el proveedor que ofrece todos los servicios de instalación, mantenimiento, garantía y la utilidad a futuro a que muy probablemente se someterán los sistemas. Dentro de los subsistemas sigue liderando el CCTV como una solución para la minimización del riesgo, con centros de comando y control como soporte del monitoreo de imágenes.

**TERCERO:** El ser humano como prestador de servicios en seguridad y vigilancia privada requiere de actualizaciones constantes, no solo la seguridad en general, sino además, en los sistemas integrados de seguridad electrónica, razón por la cual las organizaciones

precisan reducir los costos en la mano de obra, originando como consecuencia la necesidad en las personas que laboran en el medio de profesionalizarse y capacitarse.
La capacidad de adaptarse a un proceso cronológico que va de la mano con la tecnología y que tiene como eje central al ser humano, indica una relación cíclica en donde las personas se deben esforzar para no quedar aisladas de la realidad que vivimos.

**CUARTO:** Los cambios políticos y la transformación de la Normatividad en Seguridad Privada, son considerados para la implementación de los sistemas de seguridad electrónica, como apoyo y complemento de la Seguridad privada en el cumplimiento de sus funciones con el fin de satisfacer al cliente en la prestación de servicios de seguridad. En realidad existen vacíos en la reglamentación en el uso e implementación de los sistemas de seguridad electrónica, causados por el avance tecnológico y por la dilación de jurisprudencia necesaria para regular y supervigilar los sistemas. Los sistemas y la seguridad electrónica avanzan, la competencia tecnológica en la actualidad desborda casi, los límites del pensamiento humano.

**QUINTO:** Alrededor de la última década hemos considerado el impulso que las tecnologías, calculando cual será el alcance y/o la eliminación de la participación humana en los empleos donde tradicionalmente se desempeña la población. Por esta razón se encuentran algunas de las herramientas tecnológicas (Drones y Robots), que quizás, en el futuro o en el mundo moderno desplacen de forma paulatina la participación del ser humano en las diferentes modalidades para la prestación de servicios en seguridad privada. “La integración de sistemas logra reducir los costos de administración por mantener sistemas independientes, eliminando cargas redundantes no deseadas. De esta manera se obtiene un mejor control con un nivel de centralización mayor”. (Revista Negocios de Seguridad, S.F)

**Referencias**


ALAS, Asociación Latinoamericana de Seguridad, (2017). Consultado en: http://alas-la.org/

ASIS International, (2017). Advising security worldwide. Consultado en: https://www.asisonline.org/Pages/default.aspx

Ben Johnson, (S.F). Sir Robert Peel. Historic UK. The History and Heritage Accommodation Guide. Consultado en: http://www.historic-uk.com/HistoryUK/HistoryofEngland/Sir-Robert-Peel/

By Courtney Sparkman, (March 3, 2015).Will technology eliminate human security?. SSMMAGAZINE, Recuperado de: http://www.securitysolutionsmagazine.biz/2015/03/03/will-technology-eliminate-human-security/

C. F. Reisz, (S.F) Miembros del grupo y fuentes varias. Código de Practica. Manual de procedimientos de instalaciones. Dispositivos utilizados para alarmas con o sin monitoreo. Grupo Seguridad Electrónica Falsas Alarmas

Cardona, P, y Tapias C. (Mayo 2015). Seguridad privada: sector ganado. Seguridad. *Revista dinero.* Recuperado de: http://www.dinero.com/edicion-impresa/negocios/articulo/balance-positivo-del-sector-seguridad-privada colombia-2015/211924

Diofanor Rodríguez, CPP, (2008). Fundamentos de la Seguridad integral Seguridad y defensa.com

El hombre y la seguridad electrónica - Informe central, (S.F). Seguridad Física. Recuperado en: http://www.rnds.com.ar/articulos/037/RNDS_084W.pdf

Gabriel Francisco Cevallos (2011). Sistemas de Seguridad electrónicos. Consultado en: https://sites.google.com/site/seguridadelectronicagcm/capitulo-1

García-Allen, (2015). Pirámide de Maslow: la jerarquía de las necesidades humanas. Analizando uno de los artefactos teóricos más famosos: la jerarquía de necesidades. Consultado en: https://psicologiaymente.net/psicologia/piramide-de-maslow

José Miguel Roca (2015). ¿Qué es la seguridad electrónica?. Consultado en: http://www.informeticplus.com/que-es-la-seguridad-electronica

NFPA, National Fire Protection Association, (2017). Códigos y estándares. Publicaciones. Consultado en: http://www.nfpa.org/

Physical Security. Design Manual for VA Facilities, *July 2007.Department of Veterans Affairs Washington, DC 20420.*

Protocolo de Vigilancia electronica.pdf**,** (S.F). Superintendencia de Vigilancia y Seguridad Privada**.** Recuperado de: http://www.supervigilancia.gov.co/index.php?idcategoria=57358

Restrepo Manuel (2017). Automatización, su mayor competencia en el trabajo. Revista Dinero. Consultado en: http://www.dinero.com/opinion/columnistas/articulo/automatizacion--su-mayor-competencia-en-el-trabajo-por-manuel-restrepo/243287

Revista de Negocios de Seguridad – Argentina, (2002). Conceptos en Sistemas de Seguridad Electrónica. Consultado en: http://www.rnds.com.ar/

Security 101- Key Goals for a Physical Protection System Publication, (July 2006). *Homeland Defense Journal*. Recuperado de: www.homelanddefensejournal.com

Technical Support 1, Technical Support 2, Publication, (July 2006). *Homeland Defense Journal.* Recuperado de: www.homelanddefensejournal.com

Technology 3 – Hazards, Publication (July 2006). *Homeland Defense Journal.* Recuperado de: www.homelanddefensejournal.com.

The Design and Evaluation of Physical Protection Systems, Mary Lynn Garcia, CPP. Second Edition (2008). Butterworth-Heinemann is an imprint of Elsevier.

Ventas de seguridad, (S.F). Seguridad electrónica en Latinoamérica. Consultado en: http://www.ventasdeseguridad.com/

Vila, S**.** (Julio 2017). El Año en que los Robots Superarán al Ser Humano. Edisonews. Recuperado de: https://www.edisonews.com/la-fecha-la-los-robots-nos-sustituiran/