

Año 1 | Edición 10 | Abril 2011

# ESTRATEGAS

La revista del empresario de la seguridad

ESPECIAL  
**Plan estratégico**  
de **SEGURIDAD** de **CIUDAD SALITRE**  
Modelo Innovador de Seguridad Comunitaria

ESTRATEGIA CORPORATIVA

**Cloud Computing**

LA INFORMACIÓN DE SU EMPRESA;  
SEGURA Y UBICUA.

MUNDO SEGURO

**Hábitos del Polígono**

QUE LO HACEN VULNERABLE  
EN LA CALLE.

Parte II

EN LA PRÁCTICA

**SIMULACRO**  
de Intrusión y Defensa

Parte I

[www.estrategas.org](http://www.estrategas.org)



2145-924X



El pasado 12 de abril conmemoramos el 50 aniversario del primer hombre que salió de la atmósfera de la tierra. Fue en 1962 cuando el astronauta soviético Yuri Gagarin con tan solo 27 años de edad viajó en su capsula esférica nombrada Vostok 1 y juntos traspasaron la atmósfera terrestre. Durante 108 minutos Gagarin estuvo en la órbita de la tierra, a una velocidad de 28.200 km/h siendo capaz de llegar a una altura de 327 kilómetros para posteriormente perder altitud y empezar a descender.

# Sun Tzu

战略家

No repitas los medios para conseguir la victoria,  
más bien responde a la forma desde lo inagotable.

Del Capítulo 6, Lo Lleno y Lo Vacío

La Organización ve la victoria, pero no logra ver la forma  
en que aquella se consigue.  
Los Ejecutivos entienden las características de la victoria,  
pero no el modo en que pueda producirse.  
El Estratega, libre de todo prejuicio, responde incansablemente  
a cada situación.



# ESTRATEGAS<sup>®</sup>

La revista del empresario de la seguridad

CARRERA 53 N° 103B - 42 Of. 405

NUESTROS NUEVOS NÚMEROS TELEFÓNICOS  
PBX (571) 742 75 69 - 257 54 41

WWW.ESTRATEGAS.ORG

## Gerente General

María Victoria Méndez G.  
gerencia@estrategas.org

## Director

Alexander Becerra V.  
editorial@estrategas.org

## Consejo Editorial

María Victoria Méndez G.  
Alexander Becerra Vargas  
Óscar Murcia Bravo  
TCIM (R) Guillermo Lara Páez

## Redacción

Óscar Javier López.  
redacción@estrategas.org

## Pre - Producción, Diseño y Diagramación

César Bejarano  
diseno@estrategas.org

## Impresión

Corcas Editores Ltda.

## Ventas Publicidad

Alexander Amado  
comercial@estrategas.com

## Servicio al cliente - Suscripciones

suscripciones@estrategas.org



EDITORIAL  
MOGA<sup>®</sup>

Los artículos de esta publicación,  
no reflejan necesariamente el pensamiento de la REVISTA.

Las opiniones expresadas en los artículos  
son estrictamente responsabilidad del autor.

Los escritos de los colaboradores sólo  
comprometen a quienes firman.

El Consejo Editorial se reserva el derecho de publicar  
los artículos que estime conveniente.

Prohibida la reproducción total o parcial sin autorización expresa  
y escrita de Revista ESTRATEGAS.

Revista ESTRATEGAS es una marca registrada de EDITORIAL MOGA SAS.



1 n O S

Diseño y prestación de servicios en la prevención de riesgos profesionales y en la promoción de la salud ocupacional.  
Prestación del servicio de cobertura económica y asistencia en las lesiones generadas por exposición a riesgos profesionales.

[www.arpcolpatria.com](http://www.arpcolpatria.com)



ARP Colpatria tiene todo lo que usted necesita para atenderlos y prevenirlos. Para mayor información comuníquese con su Asesor de Seguros o a nuestra Línea de Atención al Cliente: 018000 512620, en Bogotá al 423 5757

# Contenido

Al día con la Supervigilancia



10

Inteligencia Corporativa



12

Técnicas de pensamiento y análisis de situaciones. Parte IV

Estrategia Corporativa



16

Cloud Computing,  
La información de su  
empresa, segura y ubicua

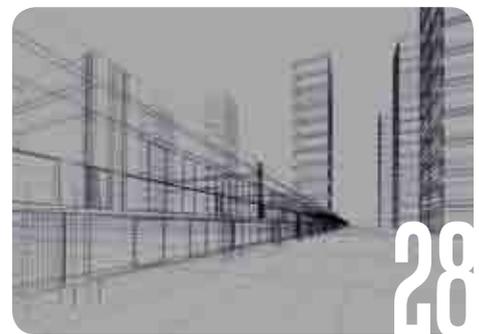
En la práctica



24

Simulacro de intrusión y  
defensa. Parte I

En la práctica



28

Control de acceso

Especial



20

Plan estratégico de  
seguridad de asosalitre

Mundo seguro



32

Hábitos del polígono que lo hacen  
vulnerable en la calle. Parte II

Actualidad Gremial



38

III Congreso virtual  
latinoamericano de seguridad:  
múltiples factores, un solo objetivo



**SONY**  
make.believe



# SERIE IR

## CÁMARAS DE SEGURIDAD HD SONY, CON ILUMINADORES INFRARROJOS Y "VIEW DR"

- Excelente calidad de Imagen HD, soporta H.264 a 30 CPS
- Captura claramente objetos en la oscuridad hasta 15m de distancia
- Únicas con capacidad de análisis inteligente de las imágenes dentro de la cámara
- Capacidad de PoE



SNC-CH260

**IPELA**

Para más información visítenos en  
[www.sonypro-latin.com](http://www.sonypro-latin.com)



## "La sinergia entre los gremios, el camino para el crecimiento de la Industria de la Seguridad en Colombia"

**L**a convivencia entre los seres humanos es fundamental para el desarrollo social del individuo; el trabajo en equipo, el debate de las ideas y el acuerdo sobre objetivos comunes, es la unidad primordial de toda sociedad moderna, lo que se traduce en comportamientos que cada uno de nosotros aplicamos a los roles sociales de nuestro diario vivir.

El desarrollo profesional y laboral es uno de los aspectos más relevantes como seres humanos, por lo cual se convierte en uno de los mejores escenarios para la aplicación de métodos y actividades que permitan desarrollar al máximo estas capacidades, ya que son potencializadas al crearlas y trabajarlas en un grupo de individuos que buscan un mismo objetivo.

El sector de la Seguridad y Vigilancia Privada es una industria en constante crecimiento y desarrollo, encontrar y generar espacios de interacción participativa es fundamental para apalancar el sector a un futuro donde haya una sinergia con los actuales y constantes cambios de los mercados mundiales y la globalización de las economías.

Fomentar y participar activamente en agrupaciones como comités, agremiaciones, mesas de trabajo y cualquier otra figura que permita la definición de objetivos comunes para el sector, donde se desarrollen estrategias empresariales con la inclusión de los nuevos mecanismos y destinos de la economía, generará un crecimiento aún mayor, más participativo y con el resultado de mejores negocios y beneficios para la Seguridad y Vigilancia Privada en todos sus aspectos.

Desde la Revista Estrategas invitamos a todos los empresarios del sector de la Vigilancia y Seguridad Privada, a que sigan participando activamente en la defensa de sus intereses comunes, disfrutando de su construcción conjunta, se integren a los grupos de trabajo, se demuestren así mismos que tienen la capacidad y tenacidad, para darle su toque personal a la creación de proyectos en común. Que se diferencien por su capacidad de gestión y su talento para hacer de éste, el mejor gremio del país, gracias a su numerosa participación democrática, los programas que son consensuados por todos, sus oportunidades culturales, deportivas y recreativas, y su responsabilidad social empresarial.

En la unidad y el respeto mutuo entre las diferentes asociaciones que integran el ámbito de la Vigilancia y Seguridad Privada, está la llave maestra para un porvenir colmado de éxitos, beneficios y utilidades.



# Estrategas en esta Edición

Tenemos el honor de publicar los artículos de cuatro importantes estudiosos de la seguridad integral; ellos son:



**Germán Duarte Vargas**

Con la cuarta entrega del artículo Técnicas de pensamiento para Estrategas – El análisis de situaciones, continuamos cumpliendo con nuestro propósito de entregar a nuestros lectores herramientas efectivas de Inteligencia Corporativa. Así mismo, continuamos agradeciendo y enaltecendo la valiosa gestión que realiza el Mayor (r) Germán Duarte Vargas, compartiendo sus conocimientos a todos los que hacen parte del sector de la Seguridad y Vigilancia Privada. El Mayor Germán Duarte es Gerente de Aseproteco y Colseg.com; miembro de Asociaciones como SAS, el Colegio de Profesionales de Seguridad Integral de Colombia y Adesec.



**Inspector Ernesto Carrera**

En esta edición publicamos la segunda entrega del artículo Hábitos del Polígono que lo hacen vulnerable en la Calle, su autor es el Inspector Ernesto Carrera, Instructor fundador de la Escuela de Protección Personal, ubicada en Caracas – Venezuela. Ha sido instructor en instituciones policiales y militares venezolanas en combate sin armas, armas blancas y de fuego, además de formación en protección a personalidades, operaciones en áreas confinadas y manejo evasivo, entre otras. De igual manera, es asesor en materia de protección a altos ejecutivos y dicta instrucción a personal de seguridad, trabajadores y altos ejecutivos en empresas nacionales y transnacionales.



**Víctor Hugo Paredes Guerrero**

Para la edición N° 10 de Estrategas traemos el artículo Simulacro de Intrusión y Defensa, del Investigador de Seguridad Privada Víctor Hugo Paredes, quien cuenta con 10 años de amplia experiencia y trayectoria en temas de Seguridad e Investigaciones, asesoría, análisis y ejecución de Estudios de Seguridad Física y Electrónica a Instalaciones y capacitación en amplias áreas de la seguridad privada. Administrador de Empresas de la Universidad Cooperativa de Colombia, con Diplomados en Inteligencia Estratégica y Alta Gerencia en Seguridad Privada; Afiliado a ASIS (American Society for Industrial Security).

## 9<sup>o</sup> Curso Básico para Expertos Poligrafistas

Curso de 400 Horas  
Académicas y Prácticas

Este curso proporciona entrenamiento para Expertos Poligrafistas bajo estándares internacionalmente aprobados ya que todos nuestros cursos siguen los requerimientos de la American Polygraph Association (APA). Dirigido a profesionales vinculados en el área de investigación, interesados en la evaluación criminal o evaluación de selección o reclutamiento de personal.

Valor de la Inversión:  
\$11,000,000.00 Pesos  
o US\$ 6,000.00  
más IVA (16%)

INFORMACIÓN e INSCRIPCIONES:  
AUDIOCINE COMERCIAL LTDA  
POLIGRAFOS LAFAYETTE COLOMBIA:  
PBX: (571) 281 77 11 Ext. 102  
Móvil: (57) 311 853 61 51  
Email: oaranguren@audiocine.com

Fecha de inicio:  
MAYO 16 AL 22 DE JULIO DE 2011



**AUDIOCINE COMERCIAL LTDA.**  
Expertos en Marcas Mundiales



**HORARIO: Lunes a Viernes de 8:00 a.m. a 5 p.m.**

# Al día con la Supervigilancia

Redacción | Fotografía: SuperVigilancia

## SuperVigilancia ratifica compromiso con la Seguridad Ciudadana de la capital

Bogotá D.C., 13 de abril de 2011.

**L**as ventajas y beneficios de contratar los servicios de vigilancia privada con una empresa legal, así como los riesgos a los que se expone la ciudadanía cuando confía la seguridad de su hogar o negocio a empresas que no cuentan con licencia de funcionamiento, fueron los principales puntos tratados por la Delegada para la Operación de la SuperVigilancia, Tatiana González Cerón, en su intervención durante el encuentro por la Propiedad Horizontal, realizado este miércoles 13 de abril en la Cámara de Comercio de Bogotá (CCB), sede chapinero.

En el evento, al que también asistió la Delegada para el Control, Marcela Castro Macías y que fue organizado por la Alcaldía Mayor de Bogotá a través del IDEPAC, la Delegada explicó las diferencias entre conserjería, vigilantes y porteros; respondió inquietudes de la ciudadanía relacionadas con sanciones y multas; e instó a los asistentes para que en el Sitio Web de la Entidad [www.supervigilancia.gov.co](http://www.supervigilancia.gov.co), en el ítem Sector de la Vigilancia y Seguridad Privada, del menú principal, verifiquen si la empresa a contratar cuenta con la licencia de funcionamiento vigente.

La actividad abarcó otras temáticas como la seguridad capital a cargo de la CCB, las buenas prácticas de vecindad con niños y adolescentes, orientada por la Secretaría de Integración Social, y las campañas de transformación de parques en lugares para la sana recreación, dirigida por el programa Amor por Bogotá de la Alcaldía Mayor.



La participación de la SuperVigilancia en este evento ratifica el compromiso de la Entidad como miembro activo del Pacto por la Convivencia y Seguridad Ciudadana, cuyo objetivo es implementar un plan de acción conjunto con la Secretaría Distrital de Gobierno, Policía Nacional, gremios y empresas del sector de la Vigilancia y Seguridad Privada para combatir la ilegalidad y la delincuencia, identificando los factores de riesgo que afectan la convivencia de los capitalinos.





## Alta participación de vigilados en foro sobre Derecho al Turno y agilización de trámites

Bogotá D.C., abril 15 de 2011.

Con una dinámica participación por parte del sector, se llevó a cabo este viernes 15 de abril el Foro Virtual de la SuperVigilancia sobre Derecho al Turno y disminución de tiempos en trámites, actividad que cumplió su objetivo de informar y actualizar a los vigilados sobre esta nueva medida que comenzará a hacerse efectiva en el mes de mayo.

En el Foro Virtual, liderado por la Superintendente Delegada para la Operación, Tatiana González, cerca de un centenar de representantes del sector de la vigilancia y la seguridad privada, dieron a conocer inquietudes sobre temas relacionados con tiempos de expedición de documentos, cumplimiento de requisitos y verificación de los mismos.

El proceso de continuar con la disminución de los tiempos para la expedición de actos administrativos y permisos de estado, hace parte de la campaña “Derecho al Turno”, la cual está enmarcada en la política de fortalecimiento, transparencia y mejoramiento de la gestión institucional de la SuperVigilancia.



Superintendente Delegada para la Operación, Dra. Tatiana González

La disminución en tiempos de respuesta se verá, por ejemplo, en la expedición y/o renovación de licencias de funcionamiento que pasará de 30 a 10 días hábiles, y en trámites relacionados con vehículos blindados, conceptos de armas y vistos buenos de importación, que ahora se diligenciarán en un máximo de 5 días hábiles.

Para que esto sea efectivo, es necesario que se cumplan al pie de la letra, las reglas de juego, especificadas en la Circular Externa No. 004 de 2011 de la SuperVigilancia, que se encuentra en el link de normatividad – circulares externas.



# SuperVigilancia

Superintendencia de Vigilancia y Seguridad Privada

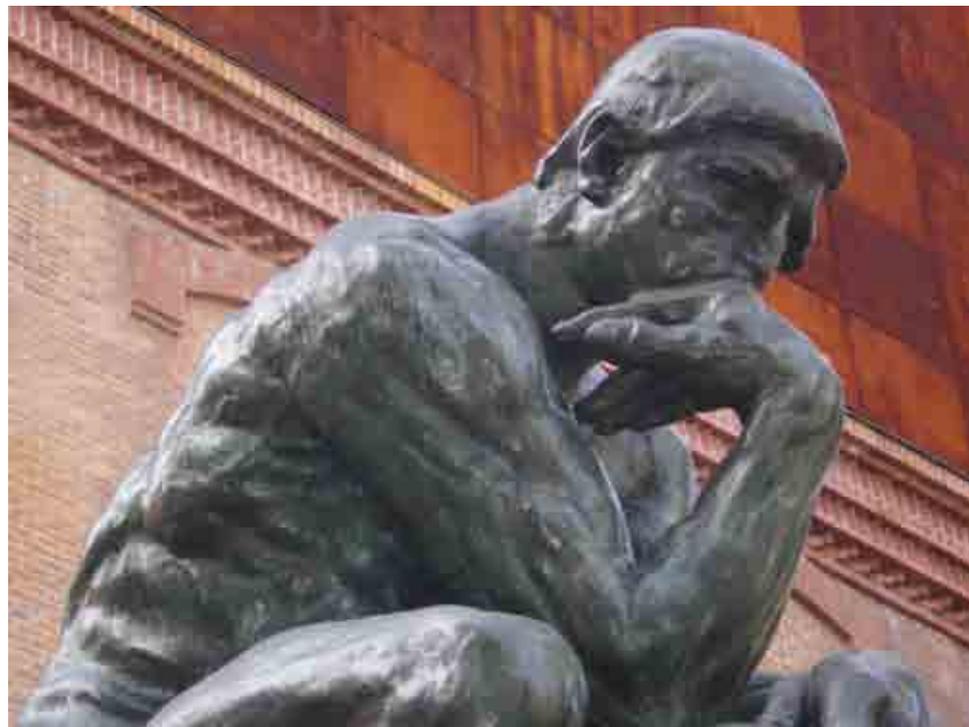


# Técnicas de pensamiento y análisis de situaciones

## Parte IV

Por: My © Germán Duarte Vargas

Luego de analizar el desarrollo del pensamiento y sus técnicas, al igual que la PNI y sus aplicaciones, presentamos a continuación la cuarta entrega de este invaluable artículo que ha construido un nuevo punto de vista sobre las técnicas del conocimiento en el mundo científico moderno.



## 2. La búsqueda deliberada de alternativas.

**L**a búsqueda deliberada de alternativas es una parte muy importante de la capacidad de pensar, porque contrarresta otra tendencia natural de la mente que es la de ir hacia la certidumbre, la seguridad y la arrogancia. Al ser ésta una maquinaria que construye y usa esquemas, desea reconocer e identificar la certidumbre lo más pronto posible, para dejar de pensar y pasar a la acción. Con frecuencia la carencia de decisiones se debe a la aparente inexistencia de alternativas. (1)(1)

1 (7) DE BONO EDWARD, Aprender a pensar. Editorial Plaza y Janes. Barcelona, 1987



Pero si hay varias elecciones, es imposible pasar a la acción, porque es difícil ir en varias direcciones a la vez, y menos en caminos opuestos. Primero hay que definir cuál es el camino, y para definirlo ya es necesario tener en cuenta todas las disyuntivas generadas.

Para producir alternativas debemos abandonar la dirección lineal del pensamiento lógico y forzar la consideración de posibilidades diferentes, así estén aparentemente reñidas con las rigurosas consideraciones del razonamiento científico. Debemos entonces salirnos del esquema y romperlo. Los mecanismos para este cambio han sido tradicionalmente “EL ERROR”, “EL ACCIDENTE” y “EL HUMOR”. En algunos casos utilizaremos estos recursos tradicionales, pero nos proponemos utilizar un método más apto y confiable que estos para cambiar el esquema. (2)

Para esto pueden seguirse diferentes técnicas como las de:

*LA PALABRA “PO”:* Viene de Poesía, Posibilidades, Hipótesis, Suposiciones, todas estas válidas para provocar el rompimiento de los esquemas y generar alternativas.

*LA FUGA:* Reside en identificar el rumbo principal del pensamiento lógico, qué es lo razonable en la consideración del problema, y luego escapar de él dirigiéndonos en otra dirección deliberadamente.

*LA ASOCIACIÓN:* En este caso asociamos en forma absolutamente aleatoria cualquier palabra, frase o concepto, con el problema convirtiendo en solución posible la asociación.

## 2. El APE y sus aplicaciones.

### El A.P.E.

Otra herramienta muy útil en el proceso de pensar es el APE. El nombre está formado por las iniciales de ALTERNATIVAS, POSIBILIDADES y ELECCIONES. El APE se emplea cuando se desea buscar disyuntivas en un punto específico y consiste en proponer explicaciones alternativas a una situación, sin ocuparnos de su improbabilidad aparente. No se debe buscar solo lo que parece probable, ya que esto puede ser una trampa. En la generación de opciones, cuando se hace un APE, debemos ser cuidadosos de no proponer solamente las que se encuentren dentro del mismo enfoque general, sino que provengan de enfoques completamente diferentes. (3)

**“Es frecuente que la dificultad para tomar decisiones provenga de la imposibilidad de producir alternativas suficientes”**

## 3. La información y el pensamiento.

Cuando nosotros disponemos de información, podemos disponer de poco o mucho conocimiento, pero frecuentemente carecemos de ella. De manera que al analizar un

Las más avanzadas soluciones de integración de seguridad electrónica y eficiencia operacional que su negocio necesita ...



Una empresa de Tyco International

Representante de fábrica de los sistemas de detección de incendio



 Obtenga diagnóstico inicial y entrega de informe de estado general del sistema

 Actualice la programación de panel central y realice mantenimiento a sus rutinas

EAS - CCTV - Access Control - Fire - Automation - Integration



Optimice el funcionamiento de su sistema a través de nuestro programa de mantenimiento preventivo

Ventas, mantenimiento y soporte

01 8000 91 98 55

co.servicioalcliente@tycoint.com

Servicio en Bogotá 57 1 655 36 00 ext 1116

www.adt.com.co

problema, frecuentemente tendremos que suplir CARENANCIA DE INFORMACIÓN, CON PENSAMIENTO. Entre más conocimiento tengamos, más posibilidades tendremos de analizar y de tomar decisiones acertadas, pero al carecer de ella, debemos desarrollar una mayor destreza reflexiva.

### 3. 1. Operatividad.

A esta consideración debemos sumar el hecho de que generalmente estamos resolviendo problemas y situaciones que se desarrollarán EN EL FUTURO. El futuro es el lugar de la acción, y así dispongamos de toda la información sobre el pasado, no tendremos nada sobre el futuro más que nuestra capacidad de pensar y de imaginar dicho porvenir. De Bono define como OPERATIVIDAD la capacidad necesaria para actuar. Esta facultad provendrá de la sumatoria que resulte de la información que se posea más la capacidad de pensamiento o capacidad reflexiva, que nos posibilita la toma de decisiones y el pasar a la acción. (5)

### 4. La C.T.F.

Corresponde a la Consideración de Todos los Factores, y es una herramienta más para orientar la atención, como el PNI y la APE. Consiste en considerar todos los factores que es preciso valorar en una situación dada. Puede parecerse o compararse esta técnica con una lista de verificación de las que utiliza un piloto de avión para preparar el vuelo y despegar la nave, con la diferencia de que al elaborar la lista de una CTF, no tienen que estar los factores enumerados en ningún orden, sino simplemente considerados. (6)

### 5. La C. y S.

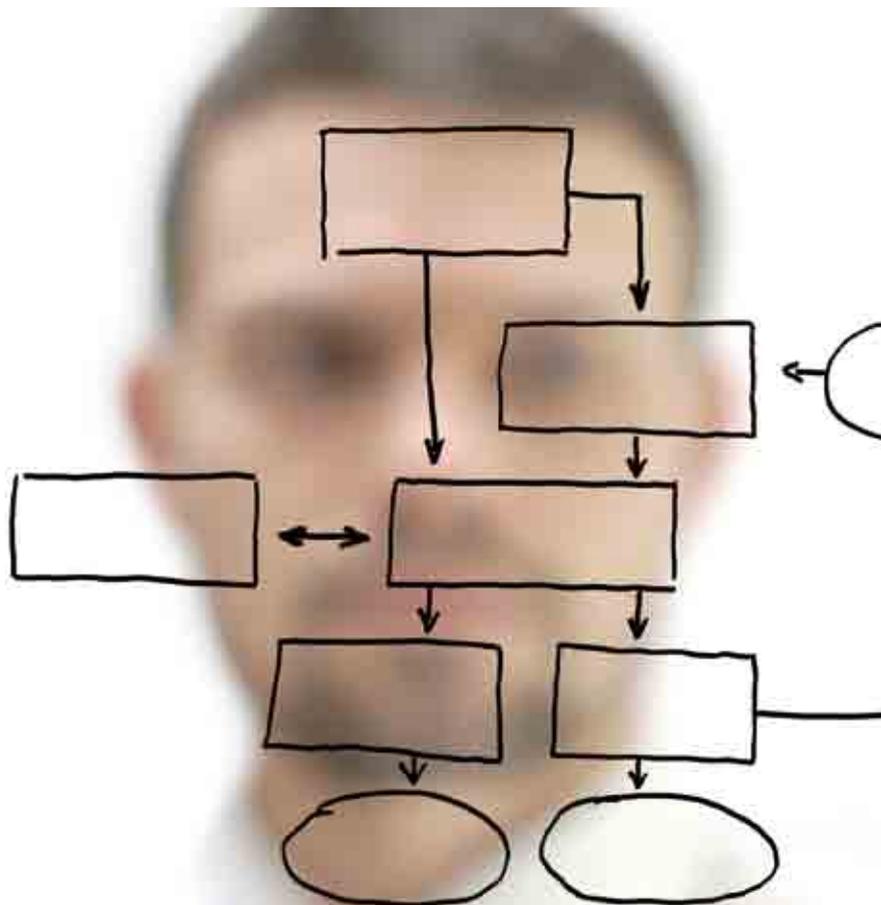
La C. y S. es una técnica para considerar de manera deliberada las consecuencias de una acción o decisión en profundidad cronológica hacia el futuro. La técnica tiene por objeto forzar la consideración de resultados a posteriori, contrarrestando en esta forma la tendencia que se tiene de tomar decisiones para resolver situaciones en forma transitoria, atendiendo la inmediatez de las mismas sin ocuparnos de lo que pase en el futuro, ignorándolo y desconociendo consecuencias inconvenientes o incluso catastróficas. (7)

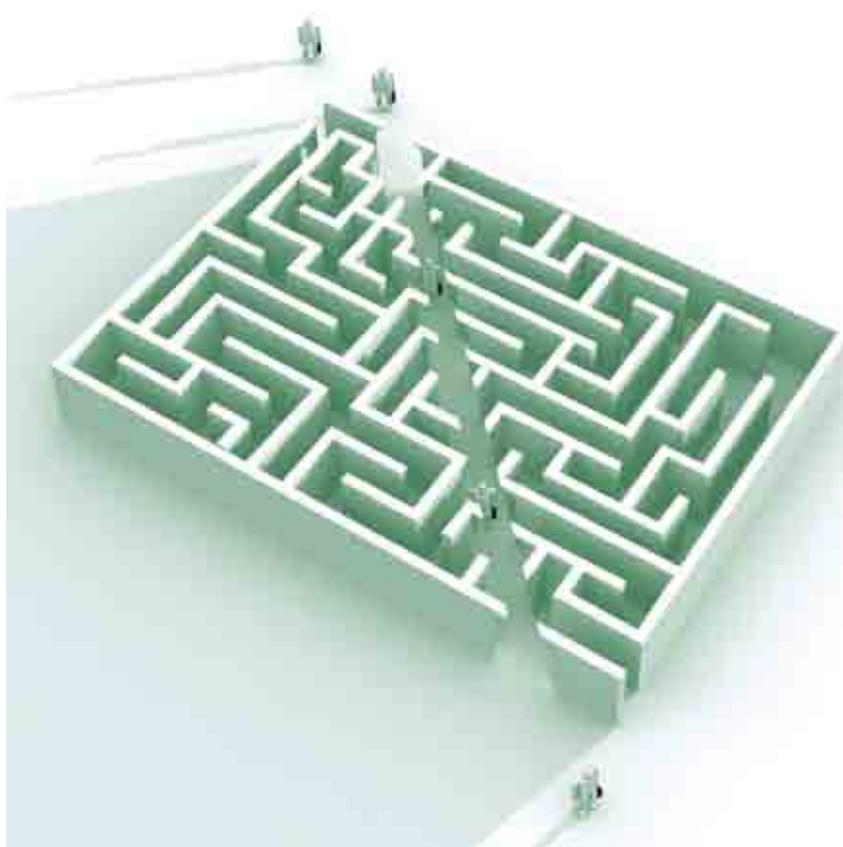
Se sugieren cuatro etapas:

- Consecuencias inmediatas, vistas a un plazo de 1 año.
- Consecuencias vistas a corto plazo: de 1 a 5 años
- Consecuencias vistas a mediano plazo: de 5 a 20 años
- Consecuencias vistas a largo plazo: de más de 20 años

### 6. La obtención de más información.

Siempre es necesaria más información. Para ello debemos ACUDIR A FUENTES, en donde esté el conocimiento, y podamos obtenerla por inspección directa. Debemos también acudir a PREGUNTAS, cuando la información la posee otra persona. Para ello podemos acudir a Preguntas Directas (PD) cuya respuesta suele ser un sí o un no, o a Preguntas Tentativas (PT) con las cuáles estamos echando el anzuelo a ver qué recogemos.





Otra forma de obtener más información sobre un tema son los EXPERIMENTOS, los cuales pueden definirse como preguntas que se hacen a nuestro entorno para conocer su comportamiento.

## 7. Los seis sombreros para pensar.

Una de las mejores técnicas propuestas por Edward de Bono en la estimulación y producción de ideas, es la de los “Seis sombreros para pensar”. Esta técnica consiste en el principio de “ACTUAR COMO SI...” Nosotros podemos asumir papeles en forma deliberada, que implican una forma específica de ver las cosas. Al estar dentro del papel asumido, estaremos pensando como si fuéramos la persona que representamos, o como si viviéramos realmente el papel que aparentamos. Se han estandarizado entonces seis sombreros, cada uno de un color diferente, que tienen cada uno un papel específico. Veamos: (8)

**3. 1. EL BLANCO:** Hechos y cifras. Solamente se exponen hechos de manera neutral y objetiva. No se interpreta.

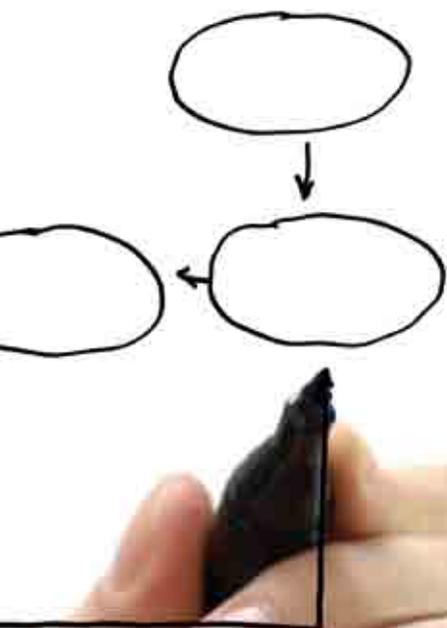
**3. 2. EL ROJO:** Son las Emociones y los Sentimientos. Es lo opuesto a la información neutral y objetiva: los Presentimientos, intuiciones, impresiones que no necesitan justificación. No es necesario dar razones ni fundamentos.

**3. 3. EL NEGRO:** Lo que tiene de malo. Lo lógico - negativo. Porqué no funcionará, Juicio crítico, el punto de vista pesimista.

**3. 4. EL AMARILLO:** Especulativo - positivo. El pensamiento positivo, optimismo, concentración en el beneficio, pensamiento constructivo, hacer que las cosas ocurran, que se realicen.

**3. 5. EL VERDE:** Pensamiento creativo, nuevas ideas nuevos conceptos, y nuevas percepciones. La creación deliberada de nuevas ideas. Generación de Más y más alternativas. Cambio. Nuevo planteamiento de problemas.

**3. 6. EL AZUL:** Control y organización del pensamiento, instrucciones para pensar. Control sobre los otros sombreros.



Queremos conocer sus comentarios a este artículo y otros publicados en esta edición, escríbanos a [editorial@estrategas.org](mailto:editorial@estrategas.org)

# Cloud Computing La información de su empresa, segura y ubicua

Por: Oscar Javier López



**L**as aplicaciones comerciales actuales se trasladan a la “Nube”. Está ocurriendo más rápido que nunca: el paso de los modelos de software tradicionales a Internet ha adquirido un mayor impulso en los últimos 10 años. Fijando la vista hacia el presente, vivimos la década de “*Cloud Computing*” que promete nuevas maneras de interactuar desde cualquier parte del mundo a través de nuestros dispositivos móviles.

El “*Cloud Computing*” o computación en la nube es toda una revolución para los consumidores de tecnología y especialmente en el ámbito empresarial, en donde este concepto se ha popularizado tanto que cada día surgen nuevas formas para aprovecharlo.

## La vida antes de Cloud Computing.

Las aplicaciones comerciales tradicionales han sido siempre demasiado complicadas y caras. La cantidad y la variedad necesaria de hardware y software para ejecutarlas son abrumadoras, por lo que se necesita todo un equipo de expertos para que las pueda instalar, configurar, probar, ejecutar, asegurar y actualizar. Gracias a Cloud Computing se olvidarán esas dificultades porque no se tendrá que gestionar el hardware ni el software, que es de responsabilidad directa de un proveedor experimentado.

Las aplicaciones basadas en la “Nube”, pueden implementarse y ejecutarse en cuestión de días o semanas y cuestan menos. Con dicha aplicación, sólo se tiene que abrir un explorador, registrarse, personalizarla y empezar a usarla.

## Definición de la “Nube”.

El Cloud Computing o Computación en la Nube, nace de los términos: Cloud y Computing.

*Cloud* o *Nube* es el símbolo que se usa generalmente para representar la Internet, mientras que *Computing* o *Computación* reúne los conceptos de informática, lógica de coordinación y almacenamiento de información.



Es así como el Cloud Computing consiste en mover la informática del simple computador personal o centro de datos convencional hacia Internet. (1)

### Características esenciales del Cloud Computing.

El modelo Cloud Computing está compuesto por cinco características esenciales(2):

- *Auto-servicio por demanda:* Los servicios pueden ser solicitados por el usuario o cliente a través de Internet directamente. El usuario paga únicamente por el tiempo de uso del servicio.
- *Acceso ubicuo a la red:* Los servicios están desplegados en la nube y son accesibles desde cualquier medio con acceso a la red (Internet, Intranet o Extranet).
- *Fondo común de recursos:* Los servicios se encuentran en la Nube para ser usados por múltiples usuarios bajo un modelo multi-arrendatario en diferentes lugares del mundo. Esto genera una independencia de la ubicación de los recursos aprovechando la naturaleza del Internet, Intranet o Extranet.
- *Rápida elasticidad:* La cantidad o calidad de los servicios ofrecidos en la Nube puede aumentar o disminuir rápidamente dependiendo de las necesidades cambiantes de los usuarios.
- *Servicio medido:* Cada recurso que consume el usuario y que es facturable debe ser medido, no sólo para fines de tarificación sino también de control. Este servicio puede ser vendido al mismo usuario o cliente dentro de su contexto y/o ambiente.

### ¿Cloud Computing es seguro?

La seguridad es el aspecto que más les preocupa a las compañías al momento de pensar en Cloud Computing. Sin embargo en la nube la información está más segura que cuando se encuentra en su centro de cómputo, o en sus propios equipos, pero quien presta el servicio tiene que cumplir con una serie de requerimientos que incluyen las mejores políticas y contratos a nivel legal.

1 MESA SECTORIAL CLOUD COMPUTING, "Cloud Computing, una perspectiva para Colombia", 2010.  
2 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, "Cloud Computing Technology", 2009.

La recomendación para los usuarios es que se le pida al proveedor certificados que cumplan con estándares internacionales de seguridad. En Colombia por ejemplo, el ISO 270001 y el SAS70 son los más grandes y los más complejos de cumplir. Si un proveedor cumple con esas normas garantiza que tiene el más alto nivel de seguridad. Y a esto se suman dos aspectos claves, por un lado las limitaciones de uso, lo que quiere decir que quien provee el servicio debe certificar que la información de la compañía ni siquiera puede ser vista por quien maneja la nube, sino sólo por el usuario.

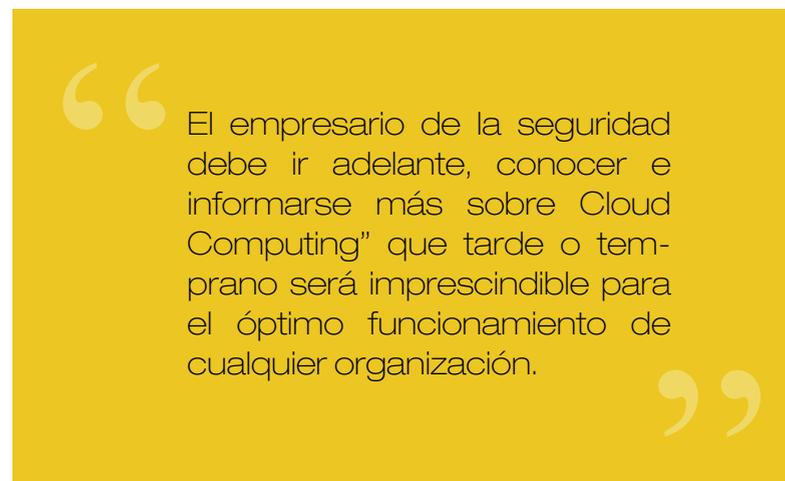
Por otra parte, la empresa debe cerciorarse de que en cualquier momento, y cuando se retire del servicio, le van a dar toda la información disponible. (3)

### Ventajas y desventajas del Cloud Computing

Entre las ventajas en el uso de la nube, tenemos los siguientes aspectos:

- Integración probada de servicios Web. Por su naturaleza, la tecnología de Cloud Computing se puede integrar con mucha mayor facilidad y rapidez con el resto de sus aplicaciones empresariales (tanto software tradicional como Cloud Computing basado en infraestructuras), ya sean desarrolladas de manera interna o externa.
- Prestación de servicios de talla mundial. Las infraestructuras de Cloud Computing proporcionan mayor capacidad de adaptación, recuperación de desastres completa y reducción al mínimo de los tiempos de inactividad.
- No necesita instalar ningún tipo de hardware o software: siempre y cuando sea una infraestructura 100% de Cloud Computing. La belleza de la tecnología de Cloud Computing es su simplicidad y el hecho de que requiera mucha menor inversión para empezar a trabajar.
- Implementación más rápida y con menos riesgos: Podrá empezar a trabajar muy rápidamente gracias a una infraestructura de Cloud Computing. No tendrá que volver a esperar meses o años

3 DIARIO EL ESPECTADOR, "Claves para saber si su servicio está en la nube" 14 de marzo de 2011.



e invertir millones de dólares antes de que un usuario inicie sesión en su nueva solución.

- Gran capacidad de personalización: Algunos profesionales de las Tecnologías de Información creen equivocadamente que es muy difícil o casi imposible personalizar la tecnología de Cloud Computing, por lo que no es la elección adecuada para las empresas más complejas. Sin embargo dicha infraestructura no sólo proporciona útiles funciones de personalización y configuración de aplicaciones, sino que también las conserva incluso después de las actualizaciones. Y aún mejor, la tecnología de Cloud Computing es ideal para el desarrollo de metodologías que estén en consonancia con las crecientes necesidades de cualquier organización.

De otra parte, las desventajas más destacadas en el uso de Cloud Computing, son las siguientes:

- *Fuera de Servicio*: En ocasiones, puede que debido a una catástrofe natural o error humano, el servicio que ofrece la nube se interrumpa, con las malas repercusiones para los clientes.
- *Guardar datos privados, fotos, videos, o información mucho más privada en estos servicios*: Actualmente parece que esta acción es inofensiva, pero, ¿realmente se puede estar de acuerdo y tranquilo cuando cualquier persona deja datos a terceros? ¿Hasta dónde se pierden los derechos a la privacidad?



- *Descontrol* del manejo, almacenamiento y uso de esta información.
- *Relatividad del servicio*: Dependiendo de qué tecnología use ese servicio, un dispositivo u otro podrá acceder o no a usarlo.
- *Dependencia*: Mayor dependencia de proveedores de internet y de la velocidad de ADSL, cable, fibra óptica u otras tecnologías.
- *Inseguridad*: Posibilidad de que delincuentes cibernéticos vulneren la seguridad del servicio y roben los datos privados de las personas, sin solicitar ninguna clase de permiso.

En pocas palabras, Internet desde sus inicios ha sido un gran acierto, que está mejorando con el paso de los años y sin duda ha hecho la vida más fácil. Pero, ¿realmente se está llegando a vivir lo que podría ser el “Gran Hermano” en la Red? ¿Son todo alabanzas a servicios 2.0 que nos hacen la vida más fácil? La respuesta usted la decide.





### Y para las empresas de seguridad, una infraestructura de Cloud Computing, ¿representa algún valor?

Las infraestructuras de Cloud Computing se han granjeado una gran fama entre los directores de sistemas de información de algunas de las empresas más grandes del mundo. Estos previsores ejecutivos tecnológicos (aunque muy preocupados por la seguridad) han confirmado el valor de la tecnología de la Nube.

Dicha tecnología libera a las empresas del software tradicional y de sus costos ocultos, de los altos porcentajes de fallos, de los riesgos inaceptables y de las implementaciones prolongadas. Todo ello, a la vez que ofrece una plataforma completa y flexible, que se ajusta a las necesidades de las empresas de todos los tamaños, desde las más grandes multinacionales a PYMES de todo el mundo.

Además se reduce al mínimo el riesgo que implica el desarrollo e implantación de aplicaciones. Después de todo, la tecnología debe resolver sus problemas comerciales y no crearle más. Gracias a la tecnología de Cloud Computing se podrán resolver problemas estratégicos en lugar de preocuparse por requisitos de infraestructuras, mantenimiento y actualizaciones.

La infraestructura de Cloud Computing también promete ahorros significativos en costos administrativos: más del 50 por ciento, en comparación con el software cliente/servidor.



“ El Cloud Computing consiste en mover la informática del simple computador personal o centro de datos convencional hacia Internet. ”

Aunque en Colombia el ingreso de esta plataforma es lento a nivel corporativo, el empresario de la seguridad debe ir adelante, conocer e informarse más sobre este tema que tarde o temprano será imprescindible para el óptimo funcionamiento de cualquier organización

### Algunos ejemplos de Cloud Computing

Varias son las grandes empresas que se han dedicado a ofrecer estos servicios, promoviendo el fácil acceso a nuestra información, los bajos costos, la escalabilidad y muchas características que nos hace pensar en la comodidad que nos brindan, entre ellas podemos mencionar:

- Google Apps: brinda el servicio de aplicaciones para empresas como Gmail, Google Talk, Google Calendar y Google Docs, etc.
- Amazon Web Services: los servicios que ofrece son el Amazon EC2, Amazon S3, SimpleDB, Amazon SQS.
- Azure de Microsoft: ofrece servicios de sistema operativo, hosting, sistemas para desarrollo.
- Rackspace: una famosa empresa de hosting, está detrás de Mosso una compañía que ofrece un paquete básico de hosting y a partir de éste se escala según se necesite (y sin migrar de servidores).

Queremos conocer sus comentarios a este artículo y otros publicados en esta edición, escribanos a [editorial@estrategas.org](mailto:editorial@estrategas.org)



# Plan estratégico de seguridad de Asosalitre

## Modelo innovador de seguridad comunitaria

Por: Óscar Javier López | Fotografía: Estrategas



Herminia Herrera, Gerente y Rubén Darío Clavijo, Coordinador de Seguridad de ASOSALITRE

**A**SOSALITRE es la organización comunitaria de carácter civil sin ánimo de lucro, modelo de Bogotá y un ejemplo a seguir en el ámbito latinoamericano. Con más de 18 años de existencia, tiene una historia de trabajo por el servicio y el bien común de los habitantes de Ciudad Salitre Occidental, a través de programas de capacitación, integración y sensibilización para sus afiliados. La Asociación también ha realizado una gestión administrativa para permitir a la comunidad, recibir atención en el cuidado del sector, sirviendo de vocera ante los entes e instituciones públicas y privadas responsables del cuidado del patrimonio común salitreño.

En la actualidad ASOSALITRE la conforman 35 conjuntos residenciales afiliados de Ciudad Salitre Occidental, incluyendo un reconocido Centro Comercial del sector, los cuales nombran sus delegados para que en una Asamblea General tengan el derecho a elegir la junta directiva de la Asociación que por el periodo de un año, diseña las directrices de gestión y trabajo comunitario.

Dentro de los diferentes programas que maneja la Asociación por intermedio de sus 12 vicepresidencias entre los que están Arte y Cultura, Ambiente, Deportes, Bienestar Social, Juvenil, Comunicaciones, entre otras, sobresale el de Seguridad, el cual, a través de un concienzudo trabajo de más de dos años ha dado origen al **PESA**: Plan Estratégico de ASOSALITRE; como un modelo alternativo, innovador e integral en la vigilancia y protección externa de una comunidad organizada.

### Ciudad Salitre Occidental, "Ciudad dentro de una Gran Ciudad"

Para entender mejor dicho plan, es necesario conocer el entorno sobre el cual se desarrollará su ejecución. Ciudad Salitre Occidental tiene un total de 64 conjuntos residenciales; una institución educativa, el Colegio Agustiniño Salitre; una zona empresarial con aproximadamente 10 torres de oficinas; más de 600 locales comerciales; una zona hotelera de cinco firmas reconocidas y un espacio turístico en donde sobresale Maloka. Además de un considerable número de canchas deportivas, parques de bolsillo, plazoletas entre otros espacios comunales.

## Franjas Ciudad Salitre Occidental

Franja	Cantidad
Residencial	62 Conjuntos Residenciales
Empresarial	10 Torres Empresariales
Comercial	480 Establecimientos Comerciales
Hotelera	3 Hoteles
Turística	1 (Maloka)
Educativa	1 (Agustiniano C.S.)
Distrital	1 (Terminal de Transportes)

En ciudad Salitre estadísticamente se calcula una población flotante diaria de 10.000 personas mínimo, (sin contar el movimiento de la Terminal de Transportes en épocas de temporada).

### La Estructura de Seguridad de ASOSALITRE y sus Cinco Pilares:

La estructura de seguridad de ASOSALITRE nació como un trabajo estratégico para ser ejecutado a largo plazo, gracias a unas bases sólidas y cohesionadas dentro de la comunidad para su buen funcionamiento. Es por ello que se crearon cinco pilares fundamentales sobre los cuales se articularán todos los programas encaminados a fortalecer la seguridad de los salitreños.

Los pilares son los siguientes:

- **PILAR N° 1: “Vincular efectivamente a los sectores de la franja comercial, empresarial, turística y educativa con la seguridad residencial”.**

Durante el proceso de construcción de este programa se encontró que el tema de la seguridad no estaba siendo incluyente con el comercio, las empresas, los colegios, los hoteles, entre otros sectores.

- **PILAR N° 2: “analizar y diagnosticar la problemática de seguridad en el área externa a través de un mapa de riesgos, generando acciones de prevención y reacción para mitigarlas”.**

El levantamiento de esta información base servirá de guía en la operatividad de todas las acciones encaminadas a fortalecer la seguridad del sector.

- **PILAR N° 3: “Fortalecer una cultura ciudadana de participación activa y unidad entre los residentes, empresarios, trabajadores, comerciantes, policía y compañías de seguridad privada”**

Buscando así que la comunidad residente y flotante asuma también responsabilidades al prevenir, detectar, denunciar y actuar solidariamente en contra de la delincuencia.

- **PILAR N° 4: “Fortalecer los mecanismos de control, prevención y reacción en el sector”**

Potencializando los esquemas de patrullaje y apoyo tecnológico tanto de comunicaciones como de monitoreo para la vigilancia externa en la zona.

- **PILAR N° 5: “Estructurar un modelo integral de seguridad auto-sostenible, una sinergia entre las empresas de vigilancia y la ASOCIACIÓN, que genere recursos para reinvertir en el área externa del sector.”**

Es importante resaltar que los recursos obtenidos para reinvertir en el área externa del sector, no son monetarios sino servicios que la empresa de vigilancia se compromete a implementar, como un motoriza-

do más para ASOSALITRE, cámaras de vigilancia, otros dispositivos electrónicos de seguridad, entre otros recursos.

### Construcción Democrática de la Estructura de Seguridad de ASOSALITRE

La Asamblea General Ordinaria de Delegados de ASOSALITRE celebrada en abril de 2009 ordenó estructurar un proyecto de seguridad comunitario sostenible para implementarse en el sector y posteriormente en el 2010, avaló, bajo la estructura del Programa de Seguridad de la Asociación, los cuatro primeros pilares anteriormente descritos y solicitó explorar alternativas de alianzas para desarrollar el quinto pilar, las cuales se presentarían en una reunión extraordinaria antes de finalizar la vigencia. Es así como el pasado 6 de febrero de 2011, se realizó dicha asamblea en donde se presentaron tres propuestas con el objetivo de implementar el modelo de seguridad salitreño.

### La Búsqueda de un Modelo Integral de Seguridad.

Es interesante analizar las propuestas que se presentaron en la Asamblea Extraordinaria de Delegados, con sus ventajas y desventajas, para demostrar el trabajo disciplinado, estudiado y consensado que realizó ASOSALITRE en la búsqueda de su modelo de seguridad.

La primera propuesta era el “*Servicio Comunitario de Vigilancia y Seguridad Privada (SCVSP)*”, consistente en un sólo cuerpo de seguridad interna y externa, de carácter propio, autofinanciado y con



Una de las Zonas Residenciales

re inversión en la seguridad externa del sector. Tenía ventajas como las siguientes: Autonomía del servicio por parte de ASOSALITRE, reinversión total de excedentes y flexibilidad de las tarifas. Por el contrario las desventajas eran: Alta carga operacional, falta de experiencia de la Asociación en el manejo total de la seguridad, una potencial pérdida del objeto social de ASOSALITRE que dejaría de ser una organización sin ánimo de lucro y el riesgo de la influencia de intereses particulares en el proyecto al existir alto flujo de dinero.

La segunda proposición hacía referencia en *“La inclusión en el proyecto de las tres empresas de seguridad que lideran la vigilancia y seguridad privada de Ciudad Salitre Occidental”*, con los siguientes puntos a favor: Experiencia y conocimiento del sector por parte de dichas empresas y que los riesgos legales estaban en cabeza de las compañías. En contra tenía: Diversos intereses entre las compañías, escaso compromiso con la seguridad externa y dificultad para armonizar la operación del día a día.

Finalmente se presentó la tercera propuesta que hacía referencia a la *“Alianza estratégica de la Asociación con una única compañía de vigilancia y seguridad privada”*, con los siguientes beneficios: Músculo financiero de la compañía de vigilancia, alineación conceptual con el modelo de ASOSALITRE, experiencia de seguridad con la franja empresarial y comercial, reinversión de las ganancias en servicios apoyando los otros 4 pilares, experiencia en modelos de atención externa, una sede local en el sector y una tarifa competitiva y ajustada a la ley. Entre las desventajas se encontraban: Dificultad para lograr acuerdos internos entre las partes, reinversión condicionada al ritmo de contratación, presión del mercado en el cobro del servicio y los requerimientos individuales por contratación.



Zona Empresarial y Hotelera

Después de analizar cuidadosamente las anteriores propuestas, finalmente la Asamblea Extraordinaria de Delegados en una votación de 45 a favor y 1 en contra, aprobó el modelo contenido en la tercera propuesta, que contempla la alianza estratégica de ASOSALITRE con una empresa de vigilancia y seguridad privada para la implementación del quinto pilar del Plan Estratégico de Seguridad, (PESA).

### Virtudes de Poseer una Sola Compañía de Vigilancia y Seguridad Privada en Ciudad Salitre Occidental.

Es necesario aclarar que la Asociación recomienda a una reconocida multinacional de vigilancia privada, como la única empresa que se adecúa al modelo diseñado para la ejecución del Plan Estratégico de Seguridad. Principalmente en materia de reinvertir parte de las utilidades obtenidas en servicios para reforzar la seguridad perimetral de la zona, apoyando los otros cuatro pilares en la estructura del modelo salitreño, gracias a su experiencia en programas de vigilancia en comunidades organizadas. Sin embargo, cada conjunto residencial tiene la autonomía de acoger o no esta propuesta y decidir libremente sobre la compañía que realice la vigilancia de sus viviendas.

Sobre este tema es importante señalar que una de las principales dificultades encontradas en la elaboración del proyecto, es que debido a la variedad de compañías de vigilancia que cuidan los conjuntos residenciales del sector, la coordinación entre ellas es complicada.

Continuación



Zona Educativa

Fotografía: Asosalitre

Aún así se espera que con la cohesión de los 60 conjuntos residenciales de Ciudad Salitre Occidental, la coordinación entre los guardas de los edificios, la participación de la comunidad, la Asociación y la sinergia con la Policía Nacional a través de una *red de comunicaciones interna*, se genere una sincronía efectiva en la vigilancia, blindando definitivamente la parte interna y perimetral de la zona, ante cualquier intento de delito. Es de resaltar que este esquema de comunicación se adecúa perfectamente con la Policía Nacional y su “*Plan Nacional de Vigilancia Comunitaria por Cuadrantes*”, una articulación proactiva de protección y reacción frente al crimen en el sector residencial, la franja comercial, empresarial, hotelera y turística de los salitreños.

### Proyecto a Largo Plazo.

El Plan Estratégico de Seguridad de ASOSALITRE se encuentra en su etapa de socialización y su implementación puede tardar uno o dos años más; cuando esté en pleno funcionamiento será un ejemplo a seguir no sólo a nivel local y nacional, sino internacional, en donde las organizaciones comunitarias están destinadas a convertirse en el bastión social y participativo de la democracia moderna. La seguridad es un trabajo conjunto, en donde los diferentes actores involucrados, comunidad, sector empresarial, educativo, hotelero y las autoridades policiales, deben unirse en torno a la consecución de objetivos comunes.

La mejor carta de presentación son los resultados que se van a obtener a largo plazo, un trabajo silencioso que espera ver sus frutos gracias al apoyo de la comunidad salitreña. El tiempo de ejecución del PESA, depende de los recursos, de la reacción y el



Zona Comercial



Zona Turística

trabajo de la comunidad y la meta es que dentro de 4 ó 5 años esté consolidado el modelo de seguridad salitreño.

### Conclusión.

El esquema de seguridad incluido en el Plan de Seguridad de ASOSALITRE, tiene una estrategia de carácter disuasivo, para que el delincuente lo piense dos veces antes de actuar en Ciudad Salitre Occidental, una comunidad organizada en donde es difícil salir bien librado de cualquier accionar delincuencia. El Plan no busca reemplazar la función policial de las autoridades constitucionalmente competentes, sino trabajar conjuntamente con ellas.

ASOSALITRE definitivamente cuenta con un modelo único de seguridad, fundamentado en cinco pilares y que fortalecerá la vigilancia externa de los conjuntos residenciales de Ciudad Salitre Occidental, a través de la alianza estratégica con una compañía de vigilancia privada, un modelo aprobado por los representantes de la comunidad.

Bienvenido el PESA y ojalá existan más comunidades organizadas en Colombia que imiten este modelo innovador de seguridad comunitaria contribuyendo en la disminución de los índices de inseguridad en nuestro país.

Queremos conocer sus comentarios a este artículo y otros publicados en esta edición, escribanos a [editorial@estrategas.org](mailto:editorial@estrategas.org)

# Simulacro de intrusión y defensa

## Parte I

Material académico adaptado por  
Victor H. Paredes Investigador de Seguridad ®

**U**na organización de seguridad sin ejercicios de seguridad, es como una producción teatral sin ensayo general.

No importa cuán talentosos sean los actores o cuánto tiempo pasan separadamente estudiando sus líneas. Sin varios ensayos bajo el ojo crítico del productor y sin todos los protagonistas practicando juntos bajo condiciones que simulen la esperada presentación en vivo incluyendo, por ejemplo, las condiciones de luz y sonido, la noche de estreno probablemente sería un fracaso.

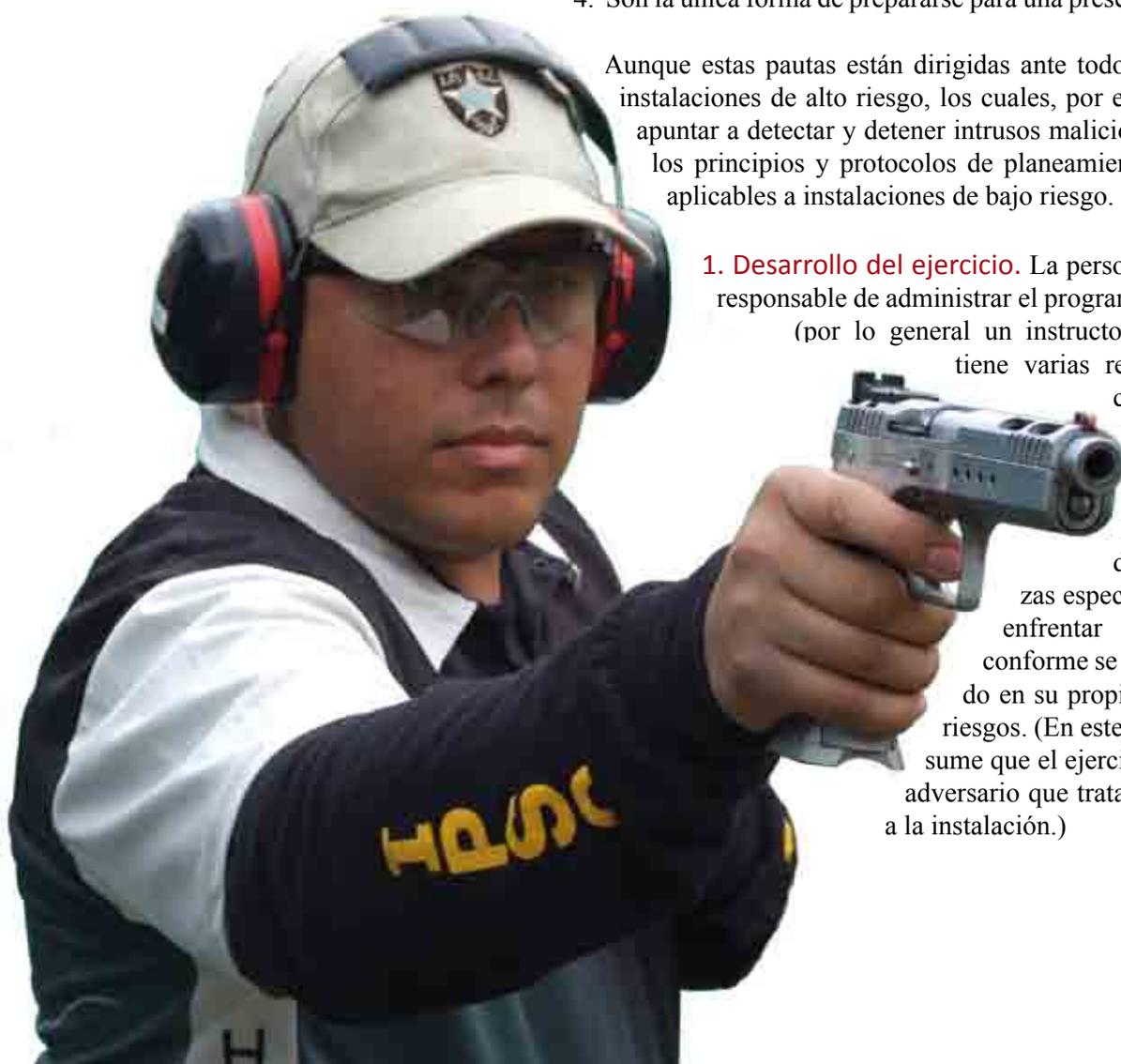
**“Un ejercicio es el ensayo general de la seguridad.”**

Los ejercicios de seguridad:

1. Aclaran ¿Quién hace qué?
2. Revelan las debilidades y necesidades de equipo.
3. Validan la efectividad de la respuesta y mejoran la coordinación entre seguridad, fuerzas policiales, y otras entidades de apoyo de emergencia.
4. Son la única forma de prepararse para una presentación en vivo.

Aunque estas pautas están dirigidas ante todo a ejercicios en instalaciones de alto riesgo, los cuales, por ejemplo, podrían apuntar a detectar y detener intrusos maliciosos, muchos de los principios y protocolos de planeamiento también son aplicables a instalaciones de bajo riesgo.

- 1. Desarrollo del ejercicio.** La persona de seguridad responsable de administrar el programa de ejercicios, (por lo general un instructor de seguridad) tiene varias responsabilidades clave. Primero es decidir cuál será el tema del ejercicio. Debe estar basado en las amenazas específicas que podrá enfrentar la organización conforme se haya determinado en su propia evaluación de riesgos. (En este artículo, se presume que el ejercicio es contra un adversario que trata de introducirse a la instalación.)



Además de diseñarlos, el instructor de seguridad debe establecer un programa anual de ejercicios y asegurar que está integrado con otros programas de seguridad y de la instalación. Los programas de ejercicios deben tomar en cuenta las horas de trabajo de los empleados y otros factores operacionales. Por ejemplo, la alta gerencia probablemente no vería favorablemente a guardias de seguridad corriendo por los pasadizos durante el día de llevar su hijo al trabajo.

El instructor también es responsable de completar y mantener los informes de los ejercicios y otros archivos relacionados. Se puede usar estos documentos después para aprender y verificar que los ejercicios fueron efectuados.

El instructor de seguridad tendrá, por supuesto, que haber pasado por el proceso de entrenar a la fuerza de seguridad en cualquiera de los procedimientos que van a ser sometidos a prueba. No tiene sentido que la fuerza de seguridad realice ejercicios hasta que estén adecuadamente entrenados en los conjuntos de procedimientos y habilidades que se aplicarán.

**2. Participantes en el ensayo.** Además de entrenar a los empleados en los procedimientos que serán puestos a prueba, el instructor de seguridad debe designar y preparar al personal en los diversos papeles que se deben hacer durante el entrenamiento. Los ejercicios y mini-ejercicios pueden implicar sólo al instructor y a un guardia de seguridad o pueden involucrar a un turno completo. Sin embargo, los ejercicios totalmente desarrollados, y especialmente los de fuerza contra fuerza, requieren una escala más amplia de asignaciones. Los participantes podrían incluir los siguientes roles:



“ Una organización de seguridad sin ejercicios de seguridad, es como una producción teatral sin ensayo general ”

*Controlador principal.* Esta persona debe poseer un conocimiento completo de la situación y de las operaciones de respuesta de seguridad. Él o ella deben tener libertad para recorrer el área del ejercicio para brindar una supervisión apropiada. Esta función puede ser cumplida por el instructor de seguridad.

*Evaluador.* Los evaluadores son aquellos individuos entrenados en seguridad que se ubican estratégicamente para observar y documentar el desempeño de oficiales específicos de respuesta. Esta función debe ser desempeñada por una persona conocedora del puesto de seguridad al que es asignada. Si el ejercicio va a ser digno de consideración, los evaluadores deben saber qué observar y cómo evaluar lo que ven.

*Controlador.* Las personas que cumplen estas funciones son responsables de controlar o facilitar algún aspecto de las acciones de un oficial de seguridad o de la amenaza simulada. A la hora fijada, un controlador introduce estímulos artificiales o eventos ideados para evitar riesgos de seguridad o para agregar realismo a la situación (por ejemplo, un controlador puede estar encargado de abrir una puerta de seguridad después de la penetración simulada del adversario).

*Adversarios.* La persona o personas que cumplen esta función deben estar apropiadamente entrenadas y equipadas con las respectivas capacidades físicas y tácticas para ocuparse de los participantes en el ejercicio de seguridad.

*Fuerza de servicio.* Este es el personal de seguridad no incluido en el ejercicio que realiza sus funciones normales de seguridad sin interferir en el entrenamiento.

*Participantes de seguridad.* Estas personas son los miembros de la fuerza de seguridad que están de servicio en la estación central de monitoreo de alarmas, y aquellos guardas que responden a la amenaza simulada.

**3. Objetivos.** El primer paso para planear y coordinar un ejercicio es determinar el objetivo del mismo. El propósito podrá ser la comprobación del rendimiento o la validación de una nueva estrategia de respuesta.

**4. Criterios de evaluación.** El siguiente paso es establecer los criterios de evaluación. Los ejercicios sin criterios claros de evaluación a menudo producen una pérdida de tiempo para los participantes, un ejercicio inútil, si se desea. Al comienzo, pueden disfrutar la emoción y el abandono de sus rutinas diarias. Pero si no saben por qué están haciendo lo que realizan, o si no reciben una retroalimentación adecuada y alguna medición de su desempeño como individuo y como equipo, eventualmente pueden tomar a mal la pérdida de tiempo. Peor aún, pueden perder la confianza en su capacidad para responder a una amenaza real.

Los participantes de seguridad necesitan saber con respecto a qué están siendo evaluados. Los ejercicios diseñados para evaluar la respuesta de seguridad a una amenaza o ataque supuesto contra la instalación o determinados blancos deben incluir Elementos Claves de Evaluación (ECE).

Algunos criterios se refieren al tamaño y funcionamiento de la fuerza. Por ejemplo, el ejercicio debe prepararse para determinar si seguridad tiene un número adecuado de guardias para hacer frente a las amenazas probables o las de los peores casos posibles. También debe analizar si los guardias de seguridad normalmente están ubicados de tal manera que puedan responder e interceptar una amenaza con el suficiente tiempo.

Otro ECE sería si los guardias de seguridad que se ven frente a una amenaza disponen de una protección física adecuada (como una barrera o un recinto protegido) para enfrentar y controlar la amenaza de forma segura. Además, se debe preparar el ejercicio para determinar si los guardias de seguridad poseen las armas apropiadas u otro equipo de protección personal para tratar una amenaza con eficacia.

**5. Características de la amenaza.** El adversario simulado contra el que se ejercita el equipo debe basarse en amenazas verosímiles identificadas en el análisis de riesgos. Si la amenaza del peor caso involucra un grupo de activistas universitarios por los derechos de los animales con cocteles molotov, la organización no debería realizar ejercicios contra escuadras suicidas simuladas de Al Qaeda.

A continuación, el instructor debe considerar las características de los adversarios. Por ejemplo, ¿Cuáles son las probables armas preferidas? Con el tiempo, las armas y tácticas de una potencial amenaza pueden variar incluso para el mismo adversario. Por ejemplo, los eco terroristas solían contentarse con propaganda rociada con pintura sobre las paredes de los laboratorios, pero cuando las compañías aprendieron a hacer frente a eso, estos grupos terminaron efectuando incendios intencionales y atentados con bombas.

Seguridad debe examinar muy de cerca las características de la amenaza para asegurarse que están representadas con realismo en los ensayos y ejercicios. Al considerar el programa total de ejerci-

cios se debe practicar con toda la variedad de características del adversario. Cada situación debe identificar claramente los elementos que están siendo evaluados y las características de los adversarios que están siendo usados en ese ejercicio.

**6. Elementos de planificación.** El instructor necesita tener en cuenta otros aspectos al planear el ejercicio. Por ejemplo, puede necesitarse equipo especial para la actividad. Esto podrá incluir armas simuladas, equipo para penetrar puertas, y bombas artificiales (marcadas claramente como auxiliares didácticos que pertenecen al departamento de seguridad).

El instructor también debe conseguir apoyo de comunicaciones para los participantes en el ejercicio. Si fuera posible, por ejemplo, los participantes deben estar preparados para usar una radiofrecuencia diferente a la de los guardias que están de servicio.

Otra preocupación es que el personal apropiado reciba una notificación previa de que se va a realizar un ejercicio. Esto es esencial para asegurar que el personal de planta no confunda el ejercicio con un ataque real.

**7. Escenario.** Para cada situación, el instructor de seguridad debe identificar el tipo básico de estrategia del adversario, como el intento de burlar furtivamente un sistema de seguridad o efectuar un ataque frontal. Luego desarrollará una secuencia específica de acciones. El instructor de seguridad también debe determinar las ubicaciones precisas por donde el adversa-



“

Un ejercicio es el ensayo general de la seguridad.

”

rio simulará penetrar o penetrará físicamente el perímetro de seguridad de la instalación (donde se espera que active el sistema de alarma). Se debe utilizar un plano de la instalación para ilustrar y aclarar los elementos.

**8. Preparaciones del adversario.** Para conseguir realismo, y en donde lo permita la seguridad, el equipo adversario debe ejecutar el mayor número posible de las acciones físicas de la situación. Por ejemplo, deben penetrar el perímetro, ingresar a la instalación, y desplazarse hasta sus blancos previstos usando las tácticas apropiadas. Aunque sólo deben simular que hacen un ingreso forzado a través de puertas con seguro y alarmas, deben portar todas las herramientas y el equipo simulado (peso aproximado) y actuar usando este equipo durante el tiempo estimado que demora penetrar la puerta. Esto es importante porque expone con realismo a la amenaza mientras franquea la puerta o el obstáculo de seguridad, y le brinda a seguridad una oportunidad más real para verificar la amenaza y enfrentarla.

Los adversarios también deben portar armas simuladas, pero las armas deben estar identificadas claramente como simuladas (pintadas de rojo) y marcadas como “Armas de ejercicio”.

La mayoría de organizaciones de seguridad utilizan a guardias de seguridad altamente motivados para representar el papel de adversario. Esto, sin embargo, frecuentemente representa la proverbial espada de dos filos. Por un lado, el entrenador no tiene que gastar mucho tiempo alimentando a los adversarios simulados con “Inteligencia” respecto a la instalación y al blanco. Por otro lado, el autor ha encontrado que este tipo de adversario simulado a veces usa excesivamente el conocimiento interno de la instalación y de las estrategias de protección y tácticas de respuesta de seguridad.

Algunos profesionales podrían considerar esta ventaja de personal interno como una cosa buena porque representa un desafío significativo (Si usted se puede proteger contra sus propios guardias de seguridad que conocen la instalación y los sistemas de seguridad al revés y al derecho, entonces usted se puede proteger contra cualquiera).

Desgraciadamente, este enfoque frecuentemente da como resultado una representación irreal de lo que el adversario probablemente sepa. Cuando los adversarios conocen cada rincón y escondrijo de la instalación, y están íntimamente familiarizados con los sistemas de alarma y respuesta de seguridad, es más frecuente que seguridad pierda que lo contrario. Un adversario tal invalida todas las medidas de protección de la información, seguridad operacional y verificación de personal y es, por lo tanto, inverosímil y contraproducente.

Una manera de evitar a adversarios irrealmente conocedores es usar en vez de ellos a especialistas de seguridad contratados, guardias de seguridad de otra instalación, e incluso policía local del equipo SWAT. Sin embargo, quienquiera que haga las veces de un adversario debe tener un nivel de conocimiento real de qué o a quién están atacando; es sumamente improbable que un adversario atacase una instalación protegida sin que primero haya reunido información y diagramas de planta de la instalación.

Para asegurar el equilibrio apropiado entre estos dos asuntos, el instructor de seguridad debe darle cierta información al adversario unas 24 horas antes de que comience el ejercicio. El tipo de inteligencia “Interna” que debe proveer seguridad (la cual le tomaría a un adversario varios meses para obtener) incluiría planos actualizados del lugar y del edificio (incluyendo los límites del área de seguridad y los diagramas de planta para cada nivel), el número de todo el personal de seguridad y todos los puestos, armas y tipo de munición que usa seguridad, y las ubicaciones de todos los puestos de vigilancia.

El autor recomienda que no se brinde demasiada información al adversario para no exceder el nivel de inteligencia que uno real podrá haber reunido. Por ejemplo, a los que hagan el papel de adversario no se les debe dar información detallada sobre el nuevo despliegue, apoyo, o procedimientos o posiciones de respaldo que tenga seguridad (excepto lo que se pueda extrapolar al revisar los puestos de seguridad y las paradas previas a un evento).

En nuestra próxima edición se seguirán analizando los detalles para la realización de un ejercicio de seguridad, enfocándose en la información previa, las precauciones, la evaluación y el mensaje final.



Queremos conocer sus comentarios a este artículo y otros publicados en esta edición, escríbanos a [editorial@estrategas.org](mailto:editorial@estrategas.org)

“ La seguridad es competencia de todos ”

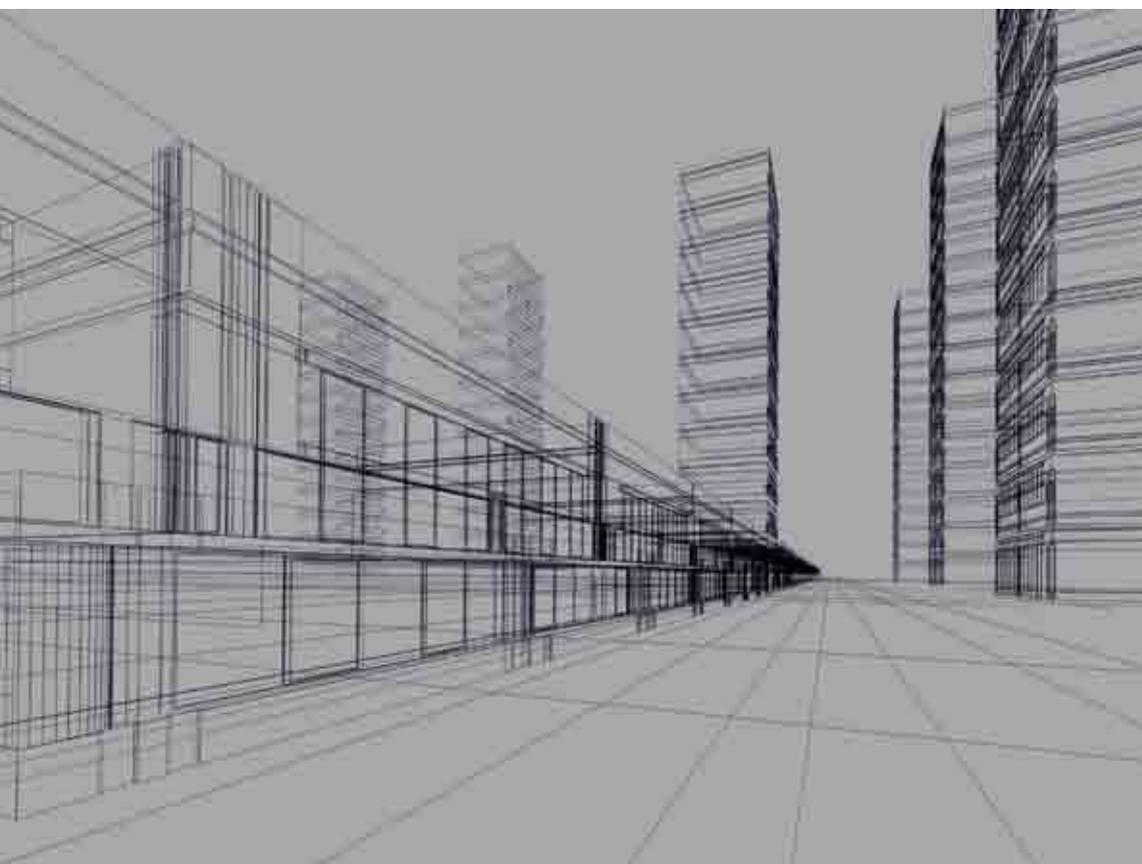
# Control de acceso

## ¿Quién tiene la llave de su empresa?

Por: Óscar Javier López

**H**oy en día estamos acostumbrados a que se prioricen las inversiones destinadas a la planificación de la seguridad informática, específicamente controles relacionados con antivirus, Internet, uso del correo electrónico y manejo de contraseñas seguras, muchas veces pasando por alto los temas que se refieren a los accesos físicos.

### ¿Es el control de accesos físicos un tema irrelevante?



Según el informe 2320 de TRENDS - IDC, de las 117 empresas encuestadas: el 63.2%, tenían proyectos para el año 2010 relacionados con seguridad informática y el 72.6% lo priorizaban en segundo lugar.(1)

Los programas de seguridad de muchas empresas tienen como gran objetivo prevenir las amenazas tecnológicas, pero poco se formula, y muchas veces no se cuenta con un responsable para la implementación de un esquema de seguridad física, en lo que respecta tanto a accesos físicos, como también a conceptos relacionados con seguridad e higiene, amenazas, contingencias, desastres naturales o creados por el hombre.

Últimamente se han vivido situaciones extremas en donde ocurrieron hechos que quebraron los controles previamente instalados, y desencadenaron en la posterior implementación de un conjunto de medidas de seguridad radicales, con el fin de que dichos eventos no se volvieran a repetir.

Como ejemplo se puede mencionar el atentado terrorista que ocurrió en el aeropuerto de Moscú el pasado 24 de enero, que desencadenó un proceso enérgico en los controles de accesos a sitios públicos neurálgicos de la ciudad, como entradas del metro, estaciones de buses y centros comerciales.

Esto demuestra que a pesar del avance de las tecnologías de la información, el control de acceso físico sigue siendo importante para garantizar la seguridad ciudadana en una época en donde son latentes las amenazas terroristas.

Hablemos de las realidades de la vida cotidiana. Nuestras casas resguardan elementos de valor monetario y sentimental. En algunos casos esos elementos valiosos son colocados en una caja fuerte, o en algún lugar de difícil acceso, a fin de impedir que alguien pueda tomarlos. Todas

1 SCHMITZ OSCAR. “La Importancia de la Seguridad en los Accesos Físicos”, Cxocommunity, 2010.

nuestras puertas y ventanas poseen llave o algún tipo de cerrojo para impedir que personas del exterior puedan acceder al interior del hogar.

Todos los días cuando salimos a trabajar o tenemos que realizar alguna actividad fuera de los hogares, seguramente cerramos la puerta con llave. No deseamos ni permitimos que un extraño pueda ingresar cuando nosotros estamos ausentes.

Reflexionemos sobre estas preguntas: ¿Alguien de nosotros dejaría las puertas abiertas? ¿Entregaría la llave a algún desconocido? O ¿Dejarían la caja fuerte abierta para que cualquier persona que ingrese a nuestra casa, pudiera tomar el contenido valioso que hay en ella?

Una analogía significativa, que nos permite una mejor comprensión sobre la trascendencia que tiene para el sector corporativo actual, el control de acceso físico.

## ¿Qué entendemos por un acceso físico?

Básicamente cuando se habla de “tipos de accesos”, estos son clasificados en dos categorías con rasgos bien diferenciados. En primer lugar tenemos *los accesos físicos*, relacionados con permisos a empleados, terceros, proveedores y clientes, a oficinas, centro de cómputos, depósitos, archivos confidenciales y áreas restringidas. En segundo lugar *los accesos virtuales*, que se relacionan con ingresos lógicos a base de datos, aplicaciones en red y sistemas de tecnología de la información en general.



El concepto de *área segura* se relaciona con control de accesos físicos, teniendo como objetivo impedir el ingreso sin autorización, daños e interferencia a las instalaciones de la empresa, así como de su información privilegiada.

Las áreas de seguridad de una empresa serán más o menos protegidas, de acuerdo a las actividades que desarrollen y al tipo de activos de información que gestionen, en donde la seguridad que se les dará, dependerá de la evaluación de riesgos efectuada y la factibilidad de implementación de mecanismos de protección en relación a su costo y al beneficio marginal que provean. Se pueden clasificar de la siguiente manera:

- **Áreas abiertas:** como estacionamientos. Les corresponde un nivel nulo de seguridad.
- **Áreas públicas:** La recepción o entrada general a la empresa. Les corresponde un nivel bajo de seguridad.
- **Áreas estándares:** Oficinas y salas de reunión. Les corresponde un nivel estándar de seguridad.
- **Áreas restringidas:** Áreas técnicas y sala de comunicaciones o cableado. Le corresponde un nivel estándar superior de seguridad.
- **Áreas seguras:** El centro de cómputos, búnker de seguridad y área de pagos o manejo de efectivo. Le corresponde un nivel seguro.
- **Áreas altamente seguras:** Bóvedas. Le corresponde un nivel de alta seguridad.

La protección de estas áreas, se lograrán con perímetros de seguridad física, determinados por barreras tangibles pensadas en forma concéntricas a las instalaciones y a los activos de información que corresponda proteger.

El concepto de concéntrico apunta a desarrollar barreras físicas generales, iniciando con el acceso a un edificio, pasando por el ingreso propio a la oficina, y llegando hasta la barrera interna menor que será la que depende directamente con la responsabilidad y/o la conducta del individuo, por ejemplo, el cuidado y manejo de los documentos que maneja en su propio escritorio.

“Las tarjetas de acceso que identifican a empleados y los permisos de ingresos a las distintas áreas seguras de la empresa, son la “llave personal” para acceder a diferentes fuentes de activos de información.”

Al desarrollar estas barreras tangibles, se está estableciendo “*el control de accesos físicos*”, garantizando que solamente se permitirá el ingreso al personal autorizado. La decisión sobre qué persona tiene acceso a la empresa y en consecuencia a qué activos de información podrá tener conocimiento, deberá ser un trabajo en conjunto realizado por el responsable de seguridad, los dueños o responsables de dicha información y el directivo correspondiente.

### Situaciones recomendadas en el control de accesos físicos.

Consideremos algunos puntos a tener en cuenta en el proceso de control en los accesos:

- Los empleados internos de la empresa deberán poseer algún tipo de identificación visible, que permita que tanto el personal de seguridad como los mismos compañeros de trabajo, puedan determinar la presencia de un extraño.
- Los visitantes, (sean proveedores, terceros y clientes), deberán anunciarse, registrarse en la recepción, en donde se les suministrará una tarjeta identificadora de visita, estando acompañados en todo momento por un empleado “identificable”.
- Las tareas realizadas por proveedores dentro de áreas seguras no deberán ser efectuadas, a menos que estén acompañados y/o supervisados por un empleado de la empresa.
- El ingreso de los empleados (autorizados y no autorizados) y de terceros deberá ser registrado en cada uno de los accesos, sea en forma digital o en forma manual mediante libros de inspección.
- Se deberá impedir el acceso a áreas seguras de elementos que permitan capturar información confidencial, como equipos fotográficos, cámaras de video, grabadoras de sonido y audio.
- Las puertas y ventanas deberán encontrarse cerradas cuando no exista personal.
- Instalar sistemas de detección de intrusos (sensor de movimiento, cámaras y alarmas), a fin de proporcionar cobertura en todo momento de las áreas en cuestión. Estos sistemas deberán ser mantenidos y controlados las 24 horas durante los 7 días a la semana.
- La asignación de tarjetas y permisos de acceso (o el mecanismo de ingreso que posea la empresa), deberán ser revisados, controlados y actualizados periódicamente.

“Los accesos físicos son los relacionados con permisos a empleados, terceros, proveedores y clientes, a oficinas, centro de cómputos, depósitos, archivos confidenciales y áreas restringidas. Los accesos virtuales se relacionan con ingresos lógicos a base de datos, aplicaciones en red y sistemas de tecnología de la información en general”.



- El uso impropio de las tarjetas de accesos no debe ser permitido (robo, pérdida, préstamos a otras personas o no uso de las mismas). Este accionar debe ser reportado y si fuera necesario deberá ser sancionado.
- Todos los empleados de la empresa deberán tomar cursos y recibir la concienciación en lo que respecta a seguridad física, y el riesgo e impacto para la empresa en caso de ocurrir algún tipo de incidente.



## El control de visitas

Los visitantes de la empresa son de enorme responsabilidad, por ello controlar su ingreso no es un tema menor:

- Anuncie las visitas en la recepción.
- En el acceso, acompañe a los invitados desde la recepción, hasta las salas de reunión, así como a la salida una vez finalizada la visita.
- Asegúrese que los visitantes deben estar acompañados en todo momento por un empleado calificado.

## La relevancia de las tarjetas de acceso

Las tarjetas de acceso que identifican a empleados y los permisos de ingresos a las distintas áreas seguras de la empresa, son la "llave personal" para acceder a diferentes fuentes de activos de información, por eso:

- Asegúrese de llevar siempre consigo su tarjeta de acceso.
- No la descuide y en ningún momento debe abandonarla, aunque crea que lo hace por poco tiempo.
- No preste nunca su tarjeta. Usted es el único responsable por los accesos que ella otorga.
- En caso de pérdida, reporte este incidente al responsable de seguridad.

"Los programas de seguridad de muchas empresas tienen como gran objetivo prevenir las amenazas tecnológicas, pero poco se formula, y muchas veces no se cuenta con un responsable para la implementación de un esquema de seguridad física, en lo que respecta tanto a accesos físicos"

Cuando se ausente de su escritorio, guarde bajo llave la información restringida y confidencial que usted maneja. Usted no sabe quien estará en la oficina durante su ausencia. Evite que la información restringida y confidencial sea de público conocimiento.



Equipos ■ Insumos ■ Mantenimiento  
■ Tarjetas Mifare y de Proximidad

## SUS CARNETS EN 30 SEGUNDOS

14 Años en Colombia nos acreditan como la empresa con mayor experiencia en soluciones de identificación.

- ☛ Imprima e identifique a todo el personal de su empresa.
- ☛ Fácil de operar.
- ☛ Por seguridad maneje internamente sus bases de datos.
- ☛ Excelente relación costo / beneficio.



Representantes para Colombia y Venezuela de:  
**DatacardGroup**

# Hábitos de polígono que lo hacen vulnerable en la calle

## Parte II

Por: Ernesto Carrera  
Director Escuela de Protección Personal  
[www.proteccionpersonal.net](http://www.proteccionpersonal.net)



**E**n la primera parte de este artículo, se analizaron tres tendencias que describían de qué manera la práctica en el polígono condiciona las respuestas del defensor ante una agresión en situación real, qué tan eficaces son esas respuestas desde el punto de vista táctico y cuáles son los errores más comunes que se comenten en un enfrentamiento. A continuación se explican las demás tendencias:

### Tendencia N°4: Manejar el enfrentamiento en función de precisión, zonas de impacto y agrupación.

En el polígono la precisión y agrupación son valores importantes porque nos indican el nivel de eficacia con el arma. Apuntar y pegarle a lo que se supone que queremos darle es una destreza obvia y necesaria para cualquiera que porte armas.

Bajo esta línea, muchos consideran que los tiros que no llegan al “centro de la masa” y la “cabeza” de la silueta son “tiros perdidos” y de allí que se esfuercen en conseguir las miras rápidamente o entrenarse para ser tremendamente efectivos usando sólo el guión. Pero apartando el hecho que se le dispara a una silueta cuyas principales dimensiones son Ancho y Alto (no profundidad, como la que tiene el cuerpo humano) hay algunas cosas que hay que poner en perspectiva.

A usted le interesa pegar y agrupar la mayor cantidad de impactos en esas zonas porque significan más puntos en la competencia y son las mejores áreas para anular la amenaza, según la balística terminal.

Pero en la práctica sería lo mismo que un boxeador que piense que la única manera de ganar la pelea es lograr golpear en el switch a su adversario y que los demás golpes no importan. Lo más probable es que mientras busca ese golpe mágico, reciba unos cuantos que lo pueden dejar K.O.

Un boxeador no sale buscando el switch de su contrincante. Simplemente trata de golpearlo y, si encuentra la oportunidad, golpea en la zona. Cualquier golpe que llegue es bueno porque suma oportunidades para buscar el definitivo. De igual manera, en el enfrentamiento cualquier tiro que llegue es bueno.

La Escuela de Protección Personal ha realizado más de 300 simulaciones con distintas personas y en todas pasa lo mismo: nunca hemos encontrado evidencias de que alguien haya tratado de apuntar y dirigir los tiros a zonas terminales de forma consciente y premeditada. Simplemente dispara contra el agresor o, concretamente, contra la zona del agresor que en ese momento esté mirando.



Dado que la mayoría de las veces en enfrentamientos de 0 a 5 metros el defensor mira la cara o el arma del agresor, si tiene buena coordinación ojo – mano logra a colocar los impactos en la cabeza, manos y brazos.

Aquellos que no tienen esta destreza desarrollada o tratan de apuntar, simplemente o no le dan a nada o son impactados porque perdieron tiempo.

De hecho es extremadamente difícil ver miras en situaciones reactivas por un fenómeno básico de comportamiento bajo estrés: todo ser vivo que es amenazado tiende a concentrarse en la amenaza y pierde perspectiva de detalles y cosas pequeñas. Y las miras son tremendamente pequeñas.

El segundo aspecto a considerar es que tanto defensor como agresor se mueven, cosa que hace bastante difícil colocar impactos quirúrgicos. La mayoría de los participantes en escenarios dice lo mismo: “simplemente vi al agresor y le disparé”. Algo que se corrobora al terminar el ejercicio cuando le preguntan al agresor en qué parte de su cuerpo recibió los impactos.

Esto plantea dos trabajos necesarios: por un lado aprender a pegar y a agrupar para dominar el arma, pero por otro desarrollar una destreza combativa que no tiene que ver con zonas y puntos: pegarle simplemente a lo que miramos.

#### **Tendencia N°5: Mantener reactividad en el enfrentamiento sin tomar iniciativa.**

La falta de una práctica donde haya interacción Humano Vs. Humano dificulta que el defensor pueda acostumbrarse al stress real de la situación. Imposibilitado de entender qué sucede y cómo actuar en consecuencia, muchas veces pasa por alto señales inequívocas de que el agresor frente a él tomó la decisión de desenfundar y disparar o está tratando de acorralarlo.

Esta fase de protocolo previo al enfrentamiento, momento en el cual aparecen los gritos, amenazas y empujones, tiende a “desbaratar” la defensa psicológica y emocional de la persona.



Incapaz de “interceptar” la pelea antes de que comience, para el momento en que los agresores atacan (desenfundan y disparan) ya es demasiado tarde.

Sin embargo, hemos notado que aquellas personas con experiencia de calle o entrenamientos previos en actividades combativas (sobre todo combate cuerpo a cuerpo) tienden a desempeñarse mejor en este aspecto. Acostumbradas a la interacción violenta, reaccionan mejor ante los avances del agresor.

Esto confirma un planteamiento que hemos venido haciendo desde hace tiempo: el tirador debe ser integral y no conformarse exclusivamente con el dominio del arma de fuego. Dado que el hecho de estar armado lo hace más proclive a enfrentamientos de vida o muerte, su perfil técnico, condiciones físicas y condicionamiento psicológico debe ser mayor.

**Tendencia N°6: Ver el enfrentamiento desde el punto de vista técnico, no táctico.**

Imbuidos en la idea de que los enfrentamientos son un asunto exclusivamente de técnicas, muchos participantes dejan de lado el componente táctico de la situación que tarde o temprano termina volteándose en su contra.

Superioridad y movilidad de los agresores, premeditación en el ataque y pérdida de iniciativa ante situaciones que no se anticiparon, difícilmente puedan resolverse si no se maneja un esquema de planes sobre cómo actuar en consecuencia.

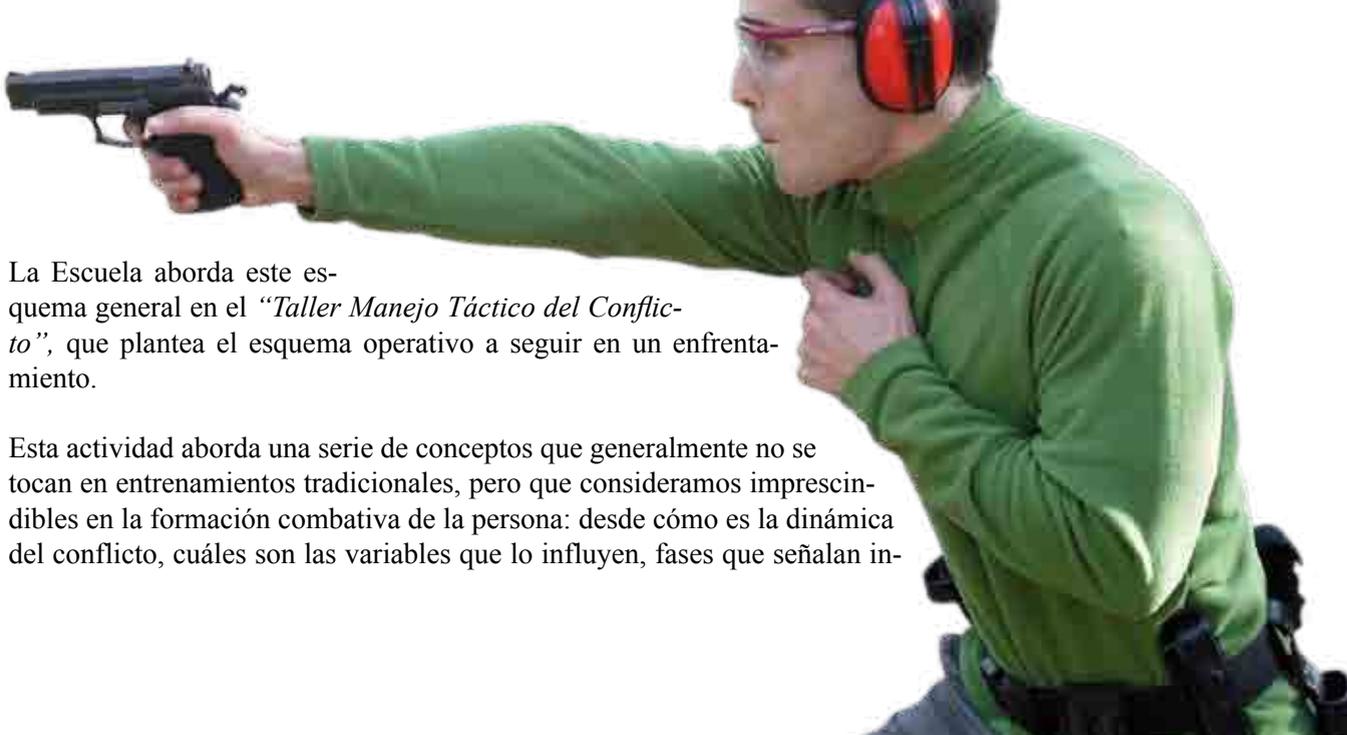
No se puede confiar exclusivamente en el desempeño técnico a la hora de lidiar con situaciones violentas. Es necesario un esquema general de procedimientos que guíen al defensor a lo largo de la situación.

Mantener un esquema general de desempeño ayuda a la persona a resolver sobre la marcha tres preguntas fundamentales: ¿Qué sucede? ¿Qué va a pasar? Y ¿Qué debo hacer? Cuestiones básicas a la hora de evaluar probabilidades y poner en marcha acciones defensivas.

Cuando la persona no maneja un esquema táctico tiende a cometer errores fatales:

- No anticipa el momento en que el agresor decide desenfundar y disparar.
- Pierde la iniciativa y juega bajo las reglas de los agresores.
- Pierde manejo del entorno, desaprovechando sus oportunidades.
- Se coloca, o permite que la coloquen, en posiciones de desventaja respecto al entorno.

Sin embargo, no existe manera de que conceptos tácticos de esta naturaleza sean instalados en polígono por la simple razón de que se necesitan agresores activos (humanos) con los cuales interactuar en entornos parecidos a la calle. La capacidad de desarrollar y manejar esquemas tácticos se logra mediante escenarios con variables cambiantes, que obliguen a la persona a resolver sobre la marcha basada en un plan general.



Continuación

La Escuela aborda este esquema general en el “Taller Manejo Táctico del Conflicto”, que plantea el esquema operativo a seguir en un enfrentamiento.

Esta actividad aborda una serie de conceptos que generalmente no se tocan en entrenamientos tradicionales, pero que consideramos imprescindibles en la formación combativa de la persona: desde cómo es la dinámica del conflicto, cuáles son las variables que lo influyen, fases que señalan in-



tención de atacar y consideraciones de entorno, hasta tácticas para retomar iniciativa y manejar el entorno, entre otras.

Esta combinación entre técnicas y tácticas incrementan exponencialmente la tasa de supervivencia del defensor, incluso en situaciones de desventaja.

### **Tendencia N°7: Falta de costumbre al lidiar con ropa y fundas cotidianas.**

Existe una “*Boutique del Tirador*” con todo un guardarropa de prendas y accesorios para ir al Polígono y cuyo objetivo es hacerle la vida más fácil. Muchas de estas prendas y dispositivos (chalecos, pantalones, fundas y otros) están especialmente diseñadas para optimizar el acto de desenfundar y disparar. Pero aunque son muy bonitas, nadie las lleva puesta al trabajo a riesgo de llamar la atención.

Existe la costumbre en muchas personas de usar estas cosas en sus prácticas, mientras que en su día a día visten y usan accesorios cotidianos cuyo diseñador jamás contempló el hacerlos cómodos para alguien armado. Esta falta de costumbre de emplear prendas cotidianas en las prácticas se transforma en una pesadilla en un enfrentamiento.

### **La Moraleja.**

Las prácticas en polígono en sus distintos grados de complejidad son necesarias porque condicionan actos reflejos y perfeccionan el dominio del arma. Sin embargo, hay dos problemas con los que hay que tener cuidado:

#### **El polígono no es la calle:**

Hay que tener claro que en el polígono todo lo que practique le saldrá bien porque es un entorno inerte y aséptico:

- Todos saben qué va a pasar.
- Todos saben dónde están los blancos.
- Sólo disparan los defensores, cuya única preocupación es pegar los tiros, no evitar que le peguen (pequeña gran diferencia)
- Los blancos no devuelven los tiros, tratan de ganar el enfrentamiento, se mueven agresivamente, emboscan o atacan.
- No hay interferencias que limiten exponencialmente el desempeño del practicante.
- Hay una serie de accesorios, prendas de vestir y periquitos cuyo objetivo es hacer comfortable la experiencia y terminan haciendo que la práctica no tenga nada en común con la forma en que la persona está en un día cotidiano.

Pero hasta ese momento la persona sólo tiene el 50% de la información (qué tan bien dispara) y el único feedback que ha recibido es cómo está manejando sus posiciones de tiro, puntería y velocidad. Falta el otro 50% que de hecho es el más importante: qué está haciendo para que no le den.

“ No puede perderse la referencia de para qué se entrena: tener claro que el agresor va a poner también su empeño en ganar, cambia mucho la manera como se practica y previene los “errores instintivos”. El aprendizaje: lleve la calle al polígono, no lo contrario. ”

A lo largo de los enfrentamientos que hemos simulado mediante entrenamiento basado en escenarios con los asistentes a nuestros cursos, hemos observado que la falta de ese otro 50% de feedback deja por la mitad la capacidad defensiva de la persona: tenemos un excelente tirador, pero un combatiente incompleto al que se le dificulta sobrevivir a un enfrentamiento.

Hemos encontrado que aquellos participantes con poca experiencia en entornos violentos y poco entrenamiento en situaciones simuladas tienden a ser erráticos en su desempeño, incluso si su nivel técnico con armas de fuego es alto.

Hay colapso ante la crisis debido al factor adrenalina y la falta de costumbre de lidiar con entornos dinámicos. Esto imposibilita a la persona entender la “lógica” de lo que sucede allí y por ende su capacidad de trazar planes. La agresión los toma por sorpresa y terminan desplegando acciones reactivas, casi “instintivas”, que al no ser desempeñadas considerando probabilidad de éxito, terminan en respuestas desesperadas tácticamente incorrectas. El resultado es la “muerte” del defensor en manos del agresor.

**El polígono puede llegar a condicionar respuestas tácticamente peligrosas:**

Muchos de los errores comunes que comete el participante en escenarios no se debe a su falta de preparación, sino su condicionamiento a actuar de determinadas formas gracias a la práctica constante, ya que a fuerza de repetir las mismas técnicas, terminan haciéndose “instintivas” o se transforman en hábitos adquiridos. La construcción de hábitos o destrezas instintivas es algo que debe instalarse con cuidado, porque a fin de cuenta lo que practique insistentemente será lo que haga en el enfrentamiento sin siquiera llegar a pensarlo y esto puede dar pie a errores fatales.

Desenfundar sin medir consecuencias, quedarse en la línea de tiro del agresor, desplazarse partiendo de posiciones incómodas para hacerlo, desarrollar el enfrentamiento triangulado, quedarse en el mismo sitio, perder tiempo buscando miras, entre otras, son en su mayoría conductas que se instalan en prácticas con fuego vivo.

Esto no significa que las prácticas en polígono, habilidades de Marksmanship y el desarrollo de canchas, deban abandonarse. Ambas representan una fuente indiscutible de desarrollo de las destrezas del tirador al incrementar su dominio técnico y visión táctica del conflicto.

Sin embargo, no puede perderse la referencia de para qué se entrena: tener claro que el agresor va a poner también su empeño en ganar, cambia mucho la manera como se practica y previene los “errores instintivos”. El aprendizaje: lleve la calle al polígono, no lo contrario.

Queremos conocer sus comentarios a este artículo y otros publicados en esta edición, escribanos a [editorial@estrategas.org](mailto:editorial@estrategas.org)



# Se cumplió con éxito la IV versión de la carrera de los héroes

Redacción | Fotografía: Cortesía Fundación Matamorros



El pasado 13 de marzo la Corporación Matamorros, realizó en la ciudad de Bogotá, la cuarta versión de la **10K CARRERA DE LOS HÉROES**, una actividad deportiva que beneficiará a los Soldados, Infantes de Marina, Policías heridos, Viudas y Huérfanos de los caídos en combate y las familias de los secuestrados o desaparecidos.

Este evento convocó a cerca de 4.000 colombianos que corrieron 10 kilómetros, todos unidos por una misma causa: apoyar los programas de ayuda que ofrece la Corporación Matamorros a nuestros Héroes de la Patria, para lograr la reincorporación socio-laboral de sus beneficiarios.

En el Parque Córdoba Cll 116 con carrera 55 desde las 8:00 se cumplió la consigna con los 4.000 asistentes que apoyaron a soldados, infantes de marina y policías heridos en combate quienes protegiéndonos resultaron afectados por la violencia.

El evento estuvo precedido por el Ministro de Defensa, Rodrigo Rivera y Sra., Mayor General del Aire Javier Pérez, la doctora Lorenza Panero, Directora Ejecutiva de la Corporación Matamorros, el Viceministro de Defensa, Luis Guillermo Jaramillo,



Cr Rubén Darío Mestizo, Director de Caprovimpo y patrocinador oficial de la Carrera, quienes premiaron a cada uno de los ganadores.

En la Carrera participaron importantes personalidades como el Ministro del Interior y de Justicia, Germán Vargas Lleras, el General Rodolfo Palomino, Director de la Policía de Tránsito y Transporte, Esteban Santos hijo del presidente Juan Manuel Santos, entre otros.

Con el valor de las inscripciones se apoyarán los programas sociales de la Corporación Matamorros:

- **Asistencia Social:** apoyo inmediato; jurídica, acompañamiento familiar, hoteles de paso, donaciones.
- **Educación:** bachillerato por ciclos y becas escolares.
- **Formación para el Trabajo,** capacitación laboral, unidades productivas y ubicación laboral.
- **Terapias alternativas de Rehabilitación:** hidroterapia y equinoterapia.

La Carrera obtuvo los siguientes ganadores en los primeros puestos en cada categoría:

Menores Masculina:	(3km)	14 a 17 años	Jairo Wilson Silva
Menores Femenina:	(3k)	14 a 17 años	Mónica Lizbeth García
Juvenil Masculina:	(10K)	18 a 19 años	Andrés Leonardo López
Juvenil Femenina:	(10K)	18 a 19 años	Samanta Guerrero
Abierta Masculina:	(10k)	20 a 40 años	Alirio Carrasco Lemus
Abierta Femenina:	(10k)	20 a 40 años	Martha Inés Roncería
Master A Masculina:	(10k)	41 a 50 años	José Jacinto López
Master A Femenina:	(10k)	41 a 50 años	Felisa Rodallega
Master Plus Masculina:	(10k)	51 en adelante	Rodolfo Lozano
Master Plus Femenina:	(10k)	51 en adelante	Ercilia Pedraza

Personas en condición de discapacidad

- Hand Cycle: Álvaro Alfonso López
- Silla Atlética: Orlando Cortez
- Silla Convencional: Libardo Murcia

Al finalizar la competencia se realizó el sorteo de la camioneta NISSAN PATROL entre los participantes a través del Chip de medición de tiempo avalado por la Lotería de Bogotá. La ganadora fue la Señora Nohora Emilse Mora con número de competencia 2068 quien participó en la Categoría Master.

“CON CADA PASO QUE TE ACERCAS A LA META, A OTROS LES DEVUELVES LA VIDA!! Fue la consigna, para iniciar un nuevo comienzo en miles de soldados que serán beneficiados por la Corporación Matamorros.



# III Congreso virtual latinoamericano de seguridad: múltiples factores, un solo objetivo

Por: Óscar Javier López



**E**l pasado 1 de abril se realizó el III Congreso Latinoamericano de Seguridad, una reunión académica con sede en el ciberespacio a través de las páginas web, [www.admejoresseguridad.com](http://www.admejoresseguridad.com), y [www.estrategas.org](http://www.estrategas.org), en las cuales los asistentes acudieron de forma virtual, es decir, desde sus propios ordenadores, sin necesidad de desplazamientos físicos, ni sincronización horaria.

Este Congreso académico masivo y multicultural se está posicionado como un referente anual de aquellas personas involucradas e interesadas en conocer las últimas novedades en el área de la Cultura de la Seguridad, promoviendo la educación continuada y basándose en la modalidad pedagógica e-learning que permite superar limitaciones de lugares temporales a través del ciberespacio, favoreciendo la intervención de varios autores que se reúnen virtualmente para exponer y debatir opiniones. Esto ha privilegiado la variedad cultural y la cobertura internacional hispanohablante.

Entre las ponencias más sobresalientes estuvo la del Capitán Gelga Buitrago Martínez, Jefe del Frente de Seguridad Empresarial y del Observatorio del Delito de la Policía Nacional, quién realizó una disertación sobre el “*Hurto en la Cadena Logística del Transporte*”, un tema de enorme relevancia para el conocimiento de los asistentes virtuales, que se mostraron encantados por las interesantes apreciaciones de la expositora.

También se destacó la conferencia del Teniente Coronel Édgar Henao Castaño de la Policía Nacional, sobre el “*Plan Nacional de Vigilancia Comunitaria por Cuadrantes*” y la importancia de generar mecanismos de trabajo solidario y participativo entre la comunidad y la Autoridad Policial.

La Universidad Central tuvo un conversatorio sobre “*La Seguridad en Colombia y América Latina*”, a través de cuatro destacados profesionales y docentes, expertos en el tema, que generó un interesante debate entre los asistentes virtuales. Se destacó la relevancia de las empresas privadas de vigilancia y seguridad privada en la seguridad ciudadana.

El Mayor ® Germán Duarte ofreció una visión sobre la importancia del capital humano en el sector de la Seguridad, a través de su ponencia, “*La Selección y Administración del Personal Confiable para la Competitividad.*”

Finalmente fue sobresaliente la exposición del Teniente Coronel Luis Ernesto García Hernández, que presentó la ponencia: “*Desafíos de la Inteligencia Estratégica y Prospectiva*”, como aliada del modelo de inteligencia policial para la seguridad ciudadana.

El III Congreso Virtual Latinoamericano de Seguridad tuvo en total 12 conferencias magistrales, con presencia de asistentes de más de 60 países, 8.000 alumnos, 40 auspiciadores y más de 500 comentarios, una participación interactiva que aumenta cada año y genera un desafío de excelencia para el próximo evento.

La iniciativa de ADMEJORES SEGURIDAD LTDA para la realización de este Congreso tuvo el apoyo de la REVISTA ESTRATEGAS “*La Revista del Empresario de la Seguridad*”, como un espacio educativo que promueve el conocimiento sobre la realidad de la Cultura de la Seguridad y estará presente el próximo año en donde se espera una convocatoria de más asistencia con un número mayor de conferencistas. Desde ahora están cordialmente invitados.



## XVII Asamblea General Ordinaria de Afiliados a ANDEVIP Capítulo Valle, Cauca y Nariño



**E**l día 15 de marzo de 2011, se llevó a cabo la XVII Asamblea General Ordinaria de Afiliados a ANDEVIP Capítulo Valle, Cauca y Nariño y la elección de la Junta Directiva periodo 2011-2012, en la cual ha sido ratificado el Doctor Mario Fernando Arellano Romo como Presidente Capitular.

Hacemos extensiva la felicitación a los demás miembros de la Junta:

- Sergio Armando Plata Otavo - Seguridad Proviser Ltda.
- María Pía Velasco Simmonds- Seguridad Omega Ltda.
- Williams Alberto González Gallego- Microcom Ltda.
- Roberto García Ronderos- Vigilancia Agroindustrial San José
- Jesús Andrés Concha Torres- Centinela de Occidente Ltda.
- Roberto Reyes Suárez Oviedo- Seguridad Segal Ltda.
- Germán Eduardo Rodríguez Delgado- Carval de Colombia
- Carlos Felipe Molinares Navia- Seguridad de Occidente Ltda.

## Asamblea General Ordinaria De ANDEVIP

**E**l pasado miércoles 30 de marzo se realizó la asamblea general ordinaria de Andevip, en donde el presidente de la entidad, Dr. Oswaldo Parada, realizó un detallado informe de su gestión, resaltando el trabajo conjunto y proactivo que tuvo con la junta directiva y su equipo administrativo durante la vigencia pasada. Destacó la labor ejecutada para resolver los problemas e irregularidades que se encontraron al inicio del periodo, a través de dos auditorías, una a la Academia y otra a la Asociación, hechas por una comisión de cinco miembros representativos de Andevip.

La junta directiva del capítulo Bogotá y Centro del País esta compuesta por:  
Presidente: Luis Oswaldo Parada

### Principales

Dr. Germán Perilla Medrano  
Dr. José Saavedra Barraza  
Dr. Juan Carlos Forero Enciso  
Dr. Antonio Pachón Vargas  
Dr. Senon Mora Astros  
Dr. Iván Ferez Díaz

### Suplentes

Dr. Gustavo Jáuregui Olarte  
Dr. Miguel Ángel Díaz García  
Dr. José Gilberto Barón Castro  
BG José Leonardo Gallego Castrillón  
Dr. Luis Antonio García Salazar  
Dr. Raúl Quiroga Moncaleano  
Dr. Mario Aníbal Castro Rincón





Pronto, nuestros lectores serán parte de un evento que se grabará en la historia.

**ESTRATEGAS**  
La revista del empresario de la seguridad