

REVISTA

# XTREMSECURE®

EL MUNDO DE LA SEGURIDAD



11 años de experiencia



ESPECIALISTAS EN UNIFORMES  
PARA SEGURIDAD

[www.xtremsecure.com.mx](http://www.xtremsecure.com.mx)

[www.uniformesjr.com.mx](http://www.uniformesjr.com.mx)

# Multiproseg

A quien **valor** merece







## **V** GUARDIAS **INTRAMUROS**

Ofrecemos un servicio de alta calidad con mejora continua en donde la capacitación constante de los guardias, la supervisión frecuente y la asistencia personalizada forman gran parte de nuestro éxito. Desde la selección estricta del personal hasta la calidad de los uniformes - cuidamos los detalles para satisfacer las necesidades de nuestros clientes.



## **V** CUSTODIA DE **TRANSPORTE**

Nuestro servicio de custodia al transporte se enfoca en la prevención de robos de los bienes. Contamos con el apoyo permanente de nuestro propio Centro de Monitoreo (24/7) y conexiones importantes con las autoridades, permitiéndonos una reacción inmediata en caso de un siniestro.



## **V** SISTEMAS ELECTRÓNICOS DE **SEGURIDAD**

Dependiendo de las estrategias de seguridad definidas, complementamos la protección de nuestro personal con sistemas tecnológicos como Alarmas, Control de Acceso, Videovigilancia, Seguridad Perimetral y GPS, entre otros.



## **V** ANÁLISIS Y EVALUACIÓN DE **RIESGOS**

Elaboramos esquemas de seguridad de acuerdo a las necesidades de cada caso. En el Análisis y Evaluación de Riesgos que realizamos, se valoran las amenazas y vulnerabilidades actuales para generar recomendaciones específicas y soluciones apropiadas.

**¡Contáctanos!**

Av. Armada de México No. 1500 Col. Residencial Cafetales Del. Coyoacán, CP 04930, CDMX

☎ 5594.5513 | 5594.5759 | 5603.0497

# EDITORIAL

Una de las principales tareas de los administradores de espacios públicos y privados es controlar la entrada y salida de las personas que transitan a diario por allí. Hoy en día es más necesario que nunca ofrecer condiciones de seguridad, bien sea para el libre tránsito, bien sea para la restricción de personas no autorizadas.

La percepción de seguridad de los habitantes de una ciudad o de los residentes de una edificación se basa, en gran medida, en la instalación de sistemas de control de acceso —como torniquetes— que controlen el ingreso y salida de estos lugares.

Por otro lado, saber quiénes entran, quiénes salen, cuántas personas lo hacen al día y con qué finalidad, son aspectos que, además de ofrecer seguridad, permiten tener un control mayor sobre los perímetros y evitar accidentes, robos y demás situaciones que puedan poner en peligro la vida o los bienes de quienes habitan estos espacios.

Por esta razón, es indispensable que las unidades residenciales y las oficinas cuenten con sistemas de control de acceso que les permitan monitorear en tiempo real y durante las 24 horas del día quienes entran o salen de allí.

Torniquetes, puertas, lectores de huella o tarjetas son algunas de las herramientas más utilizadas en la actualidad por las edificaciones para este fin, pues con su instalación se logra un control total del acceso peatonal.

*Estimados lectores ya estamos en el año 2020 y a nombre de la revista Xtrem Secure "El Mundo de la Seguridad" les deseamos excelente inicio de año, mucho éxito y abundancia, les mando un abrazo y no olviden escribir a [cvillatoro@xtremsecure.com.mx](mailto:cvillatoro@xtremsecure.com.mx)*



15

# DIRECTORIO

Enero - febrero 2020

**César Villatoro Ramírez**  
DIRECTOR GENERAL

**Mariano Botey Hernández**  
DIRECTOR EDITORIAL

**Mayte Caracas**  
GERENTE COMERCIAL

**Jazmín Rodríguez González**  
CREATIVIDAD & DISEÑO

**Voces de Seguridad**  
WEBMASTER

**Víctor Cruz García**  
REDACCIÓN

**Publicaciones GBM**  
DISTRIBUCIÓN

David Rusell,  
Ing. David Chong Chong,  
Juan Manuel Harán,  
Javier Olmos

Jake Moore  
COLABORADORES EN ESTE NÚMERO

52 (55) 7663 3711  
52 (55) 5207 4704  
VENTAS

[cvillatoro@xtremsecure.com.mx](mailto:cvillatoro@xtremsecure.com.mx)  
COMENTARIOS



XTREM SECURE, revista dirigida a directivos, ejecutivos, empresarios, políticos y personas encargadas de contratar los productos o servicios de seguridad para su protección personal, casa o negocio.

Los juicios y opiniones de nuestros colaboradores son de carácter estrictamente personal y no representan necesariamente la opinión de nuestra revista. XTREM SECURE es una publicación bimestral de Palabras Aladas, S.A. de C.V.

Se distribuye con circulación controlada y calificada. C2020. Todos los derechos reservados. Prohibida la reproducción total o parcial por cualquier medio, incluso los electrónicos sin autorización por escrito de los editores. La información ha sido obtenida de fuentes que se consideran fidedignas, pero en ningún caso deberá considerarse como recomendación para adquirir o utilizar bienes o servicios. El contenido de los anuncios es responsabilidad del anunciante. Editor responsable: César Leobardo Villatoro Ramirez. No. de Certificado de Reserva otorgado por el Instituto Nacional del Derecho de Autor 04-2008-041411145200-102. No. de Certificado de Licitud de Título 14085. No. de Certificado de Licitud de Contenido 11658. Domicilio de la publicación: Londres 75 Desp 401-E Col. Juárez, C.P. 06600 CDMX, Impreso en Ciudad de México.

Impresora Litho Signus, S.A. de C.V. tiraje 10,000 ejemplares distribuidos en toda la República Mexicana en oficinas y exposiciones. PUBLICIDAD. Para contactar con los ejecutivos de ventas o solicitar información sobre tarifas y espacios publicitarios, comuníquense al Cel. (55) 7663 3711, Tel: 5207 4704, o escriba a: [cvillatoro@xtremsecure.com.mx](mailto:cvillatoro@xtremsecure.com.mx)



# CONTENIDO

ENERO - FEBRERO - 2020



www.seguridadprivadamx.mx

29

SEGURIDAD PRIVADA



www.seguridadpublica.mx

55

SEGURIDAD PÚBLICA



www.controldeaccesosmx.com

63

CONTROL DE ACCESOS



www.seguridadindustrialmx.com

71

SEGURIDAD INDUSTRIAL



www.ciberseguridadmx.com

79

CIBERSEGURIDAD

SÍGUENOS EN REDES SOCIALES



[www.facebook.com/revistaxtremsecure](https://www.facebook.com/revistaxtremsecure)



[www.twitter.com/xtremsecure](https://www.twitter.com/xtremsecure)



[www.youtube.com/xtremsecure](https://www.youtube.com/xtremsecure)

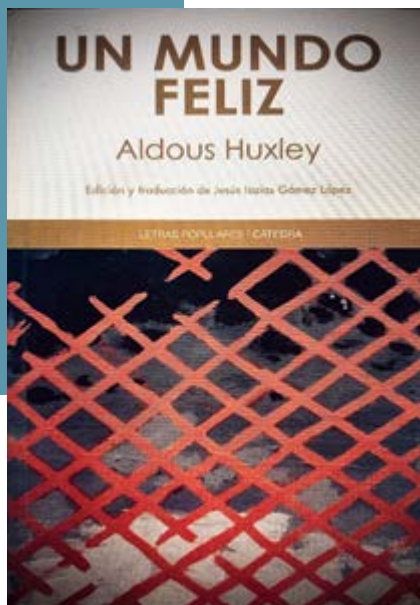
# LA SEGURIDAD DE LEER

Por Mariano Botey, mboteyh@gmail.com



## Un mundo feliz

de Aldous Huxley, Editorial: Cátedra, 2013, España.



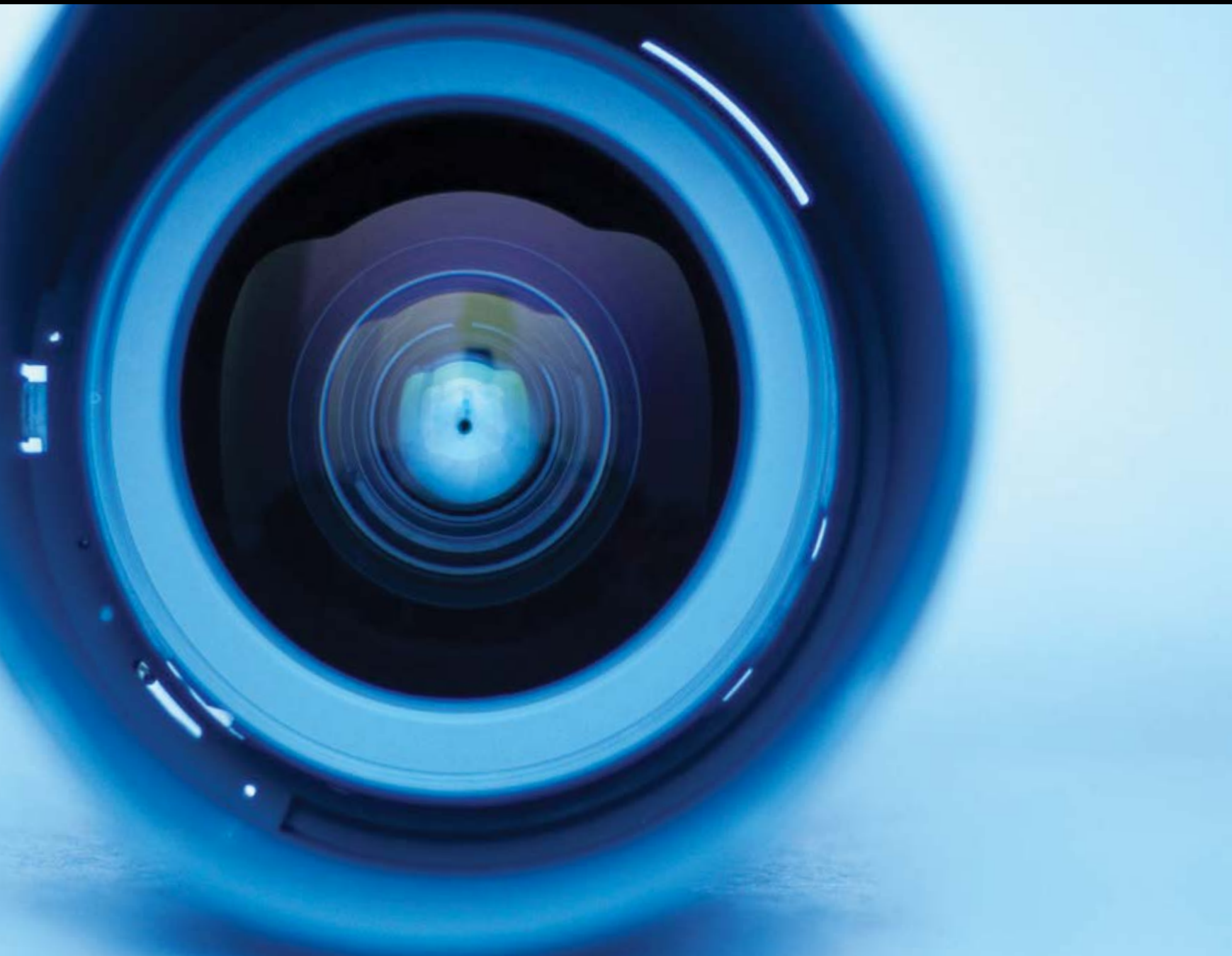
Lo más viable para llevar este mundo sin adjetivos, sería en no darse cuenta de un detalle que nos afecta emocionalmente; es decir, "qué bien se pasaría si no se tuviera que pensar en la felicidad". En caso de que estuviese consciente de estar próspero o triste, -o de cualquier modo-, le invito a trasladarse a nuestro mundo que se retrató -aún en esa alargada sombra- desde 1932, rebasando la realidad sin desvirtuar los matices y agudeza intelectual del autor; desde que me subí a aquel satélite literario, sea este libro un buen referente para hallarse en ese extraviado mundo globalizado, en lo cual me invita con urgencia, de que se lea y actúe de inmediato con ironía: "Un Mundo Feliz" de Aldous Huxley. Este libro confeccionado al estilo británico como Brave New World, sigue su vigencia con posibles añadidos, aprovechando el grave problema de la humanidad: la superpoblación; vayamos pues con valentía como los viejos tiempos en este 2020, cada uno de sus

deseos se vayan cumpliendo en la transición del día, desde la congruencia de nuestras posibilidades; no seamos dados a fantasear en las expectativas -ajenas ni propias- sino donde vamos plasmando nuestro destino con nuestros pies. Ser genuino, primer responsabilidad: "Prefiero ser yo mismo, yo y desdichado, antes que cualquier otro y alegre". Es menester que atendamos nuestras dudas, abarcando las fuentes de los libros, desde el sonido de cada palabra como el contexto mismo de su significado, se percatará que "Las extrañas palabras penetraron, rumorosas, en su mente como la voz del trueno; como los tambores de las danzas de verano, si es que los tambores supieran hablar; como los hombres cuando entonan el Canto del Maíz, tan hermoso que hace llorar"; tan poéticamente para acudir a la etimología, porque "Las palabras pueden llegar a ser como los rayos X, que atraviesan cualquier cosa, si uno las emplea adecuadamente". Un mundo feliz es un planteamiento de posibilidades en torno a una sociedad doblegada por la tecnología y la ciencia, en la que los ciudadanos de Utopía, están comfortable y meramente condicionados por una dañina droga "soma" (jamás he pensado que las drogas favorezcan; más bien, suplen un proceso de la realidad). Cada uno toma sus decisiones, aunque es indispensable que uno esté informado y no esté a las influencias de amigos y datos de dudosa información. Lo que nos choca nos checa y basta con asociar esta postura y discernir una con respecto a las otras: "La felicidad es un patrón muy duro, especialmente la felicidad de los demás. Un patrón mucho más severo, si uno no ha sido condicionado para aceptar más que la verdad. La felicidad universal mantiene en marcha constante las ruedas, los engranajes; la verdad y la belleza, no". Aunque cueste trabajo en aceptar que ese "mundo feliz" no te quita la libertad, -implícitamente- es un algoritmo en el que el producto eres tú ¿Acaso consideras vivir libremente a través de la redes sociales?. Nuestras maneras de laborar y estar relacionándonos a través de una interconexión, no nos ha favorecido

en la calidad de vida, ni trato humano. "En el campo de las comunicaciones en masa, cómo en casi todo otro campo de actividad, el progreso tecnológico ha perjudicado al hombre modesto y ha favorecido al hombre poderoso". Somos imperfección; por tanto, no nos desgastemos en buscar la perfección. "La felicidad real siempre aparece escuálida por comparación con las compensaciones que ofrece la desdicha. Y, naturalmente, la estabilidad no es, ni con mucho, tan espectacular como la inestabilidad. Y estar satisfecho de todo no posee el hechizo de una buena lucha contra la desventura, ni el pintoresquismo del combate contra la tentación o contra una pasión fatal o una duda. La felicidad nunca tiene grandeza". Por eso, no tengamos ese delirio de grandeza, ni gastemos en créditos bancarios, que nos hacen creer que es nuestro dinero. Además, hemos asistido a lugares y a eventos que son muy costosos; por ende, el consumismo es muy latente en muchos aspectos de nuestras vidas; se siguen incrementando nuestras deudas materiales, cuando se tendría que invertir en nuestros bienes espirituales y, se dejan cautivar por esos escenarios llenos de asombro: "Las flores y los paisajes: son gratuitos". Añado el hábito de leer: "El regreso a la cultura. ¡Sí, a la cultura! No se consume gran cosa cuando se pasan las horas de ocio leyendo libros". Medite por cada sigla del tiempo y sin precipitación revalorice el concepto de antigüedad... y seguirá descubriendo que lo arcaico es la belleza oculta y no una belleza nueva pues en la actualidad se deteriora en un neologismo, "La belleza ejerce una atracción, y nosotros no queremos que la gente se sienta atraída por cosas antiguas. Queremos que les gusten las nuevas". Es pertinente buscar en: recuerdos; sueños no realizados; viejas enseñanzas de los abuelos, de la vieja escuela... porque no necesitamos gente nueva, sino gente que valore y aproveche lo que tiene y no de lo que carece. "¿No deseas ser libre? 'hoy día todo el mundo es feliz'. Eso es lo que les decimos a los niños. Pero, ¿no te gustaría tener la libertad de ser feliz... de otra manera?".



# VIDEOVIGILANCIAMX



**REVISTA DIGITAL**  
ESPECIALIZADA EN VIDEOVIGILANCIA

[www.videovigilanciamx.mx](http://www.videovigilanciamx.mx)



## 4 DE CADA 10 CÁMARAS DE SEGURIDAD están en riesgo de ataques cibernéticos

El firmware desactualizado de la cámara y el hecho de no cambiar las contraseñas predeterminadas de fábrica son algunas de las mayores vulnerabilidades en la defensa de ciberseguridad. A medida que la cantidad de dispositivos de seguridad interconectados crece, mantenerse al día con las últimas actualizaciones puede ser algo complicado e implicar mucho tiempo. Según una nueva investigación realizada por Genetec Inc. ("Genetec"), proveedor líder de tecnología de seguridad unificada, operaciones e inteligencia de negocios, el 68.4% -es decir, 7 de cada 10 cámaras- funcionan actualmente con el firmware desactualizado.

Instalar el último firmware no se trata solo de acceder a nuevas funciones, advierte Genetec. Asegurarse de que las últimas medidas de protección de ciberseguridad se implementen tan

pronto como estén disponibles, es un paso crucial para garantizar la resistencia de una organización frente a los ciberataques.

La investigación realizada muestra que casi 1 de cada 4 organizaciones (23%) no usan contraseñas únicas para cada cámara, por el contrario, conservan las contraseñas que vienen de fábrica, facilitando así el acceso a los piratas informáticos una vez que solo una de ellas ha sido hackeada.

Hasta hace poco, las cámaras IP venían con configuraciones de seguridad predeterminadas, incluida la información de inicio de sesión del administrador que a menudo está disponible públicamente en los sitios web de los fabricantes. Si bien ahora la mayoría de los fabricantes de cámaras solicitan a los usuarios configurar una nueva contraseña y credenciales de administrador para la instalación, existen empresas, negocios y organizaciones gubernamentales con equipos más antiguos que nunca actualizaron sus contraseñas, lo que podría comprometer sus datos y sistemas críticos que residen en su red.

"Desafortunadamente, nuestra investigación muestra que la mentalidad de 'configúrelo y olvídelo' sigue prevaleciendo, poniendo en riesgo la seguridad de toda una organización y la privacidad de las personas. Todo lo que se necesita es una cámara con firmware obsoleto o una contraseña predeterminada para crear un punto de entrada para que un atacante comprometa toda la red", agregó Chevalier. "Es fundamental que las organizaciones sean tan proactivas en la actualización de sus sistemas de seguridad física como en la actualización de sus redes de TI", finalizó. **XS**

*"Los principales datos de nuestra investigación apuntan al hecho de que más de la mitad de las cámaras con firmware desactualizado (53.9%) contienen vulnerabilidades de seguridad cibernética conocidas. Al extrapolar esto a una red de seguridad promedio, casi 4 de cada 10 cámaras son vulnerables a un ciberataque", señala Mathieu Chevalier, Líder de Arquitectura de Seguridad en Genetec.*





## Integradores de Sistemas Electrónicos de Seguridad



Guadalajara • León • Querétaro • Yucatán  
Monterrey • Puebla • Los Mochis

 Av. Universidad 989 – 401. Col. Del Valle,  
Benito Juárez, 03100. CDMX, Tels. 5685 7830  
5685 7837 01 800 2 COMEXA

 [ventas@comexa.com.mx](mailto:ventas@comexa.com.mx)

- **Diseño de Ingeniería**
- **Servicios**
  - Comissioning
  - Desarrollo e Integración
  - Instalación y Mantenimiento
  - Administración de Proyectos
- **Sistemas**
  - Inteligencia Artificial (IA)
  - Incendio (Detección y Extinción)
  - Control de Accesos (Biometría)
  - CCTV (IP)
  - Central de Monitoreo con reporte directo al C-4 en la Ciudad de México



*GENETEC es la empresa líder en sistemas de seguridad basados en redes IP, la innovación es su cualidad principal y sus soluciones tecnológicas han ayudado a transformar la industria de la seguridad.*

# GENETEC

## Soluciones que dan confianza

**GENETEC** proporciona a sus clientes un amplio portafolio de soluciones unificadas que van de la videovigilancia y el control de acceso, hasta el reconocimiento facial y de placas vehiculares. Sus soluciones están desarrolladas con una arquitectura abierta, lo que les permite unificar dispositivos periféricos y sistemas de terceros, y así proporcionar la flexibilidad que le permita al sistema evolucionar y crecer en medida que cambian las necesidades del cliente.

Durante su participación en el **Simposio de Seguridad de ANTAD 2019** tuvimos la oportunidad de hablar con José Arellano Padilla, Account manager en **GENETEC**:

“La solución que estamos presentando en este Simposio de Seguridad ANTAD 2019 es nuestra plataforma unificada de seguridad, donde puedes encontrar la unificación de sistemas de seguridad como videovigilancia, control de acceso, lectura de placas, integración de sistemas de terceros, como por ejemplo, reconocimiento facial, entre otras muchas aplicaciones que podemos incorporar a Security Center, que es el producto insignia de **GENETEC**”.

### ¿Qué es el Security Center?

“El Security Center es la plataforma que unifica diferentes sistemas de seguridad. Los ponemos juntos para que un operador pueda hacer más fácil su trabajo al usar solamente un interfaz que le va a permitir, desde ahí, hacer toda la administración, toda la operación de todos los sensores que existen en un sistema global de seguridad. Eso es lo que hace nuestro producto, es la unificación para poder hacer también, a partir de recibir información, de datos que se están generando día con día, organizarlos, estructurarlos y poder ayudar a la operación de cualquier negocio, así como también, ya con estos datos y esta estructuración que le podemos dar con nuestra plataforma, poder inyectar inteligencia con diferentes aplicaciones que manejamos”.

### ¿Es sólo para la industria del retail?

“**GENETEC** aplica para cualquier vertical, y entre esos verticales, tenemos también un módulo específicamente para soluciones de retail, que es nuestra aplicación de Retail Sense, donde incorporamos analítica de video, tanto para la parte de intrusión como para poder también implementar inteligencia de negocio”.

“En esta analítica de video, hablando de intrusión, podemos detectar cruces de línea, merodeo, sentido de desplazamiento, tanto de personas como de vehículos, y ya enfocados cien por ciento al retail, nos enfocamos al conteo de personas, cuántas personas entraron a la tienda, una vez en la tienda hacia dónde se dirigen, para determinar cuál es la tendencia para poder lanzar campañas de marketing con base en el aglutinamiento de las personas dentro de la tienda y determinar donde pasan más tiempo, cuánto tiempo tardan en las filas, y así dar una tasa de conversión, es decir, de todas las personas que entran cuántas realmente compran algo, cuál es el monto promedio de los tickets. En fin, es toda la inteligencia de negocio que podemos darles con estos analíticos”.

“Actualmente en México tenemos participación en varios proyectos, de los que no te puedo mencionar nombres, por cuestiones de confidencialidad, pero tenemos bastante participación, tanto en gobierno como en iniciativa privada”.

“Asistir a este foro ha sido muy interesante, y nos interesa seguir haciéndolo porque vemos cómo, desde la organización misma del evento, nos han permitido conseguir entrevistas con usuarios finales, que son de nuestro interés. En el foro que está enfocado al retail; sin embargo, han participado otras verticales, que también son de nuestro interés”.

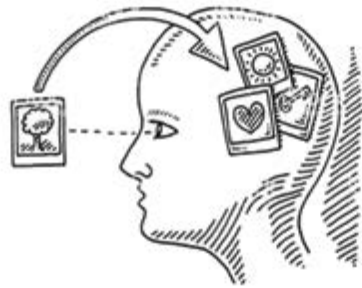


# Dinámica del Monitoreo de **VIDEOVIGILANCIA EN SEGURIDAD**

Por Ing. David Chong Chong  
[dchong@ceasmexico.org.mx](mailto:dchong@ceasmexico.org.mx)



**Detectar**



**Identificar**



**Decidir**



**Actuar**

El recurso humano constituye el factor crucial para la efectividad en el monitoreo de videovigilancia por su carácter de elemento consciente, responsable del discernimiento y decisión en el binomio hombre-máquina que se conforma en toda aplicación de tecnología. Por ello, en la medida en que se agilice y facilite su dinámica, se fortalecerá el potencial de efectividad en el monitoreo de sistemas de videovigilancia.

## Antecedentes

La dinámica genérica del recurso humano se puede describir por el acrónimo DIDA, ya que integra un proceso con las siguientes acciones:

- **Detectar** por medio de los sentidos.
- **Identificar** lo que se ha detectado.
- **Decidir** un curso de acción a seguir por lo que se ha identificado.
- **Actuar** de acuerdo con las decisiones tomadas.

El cual, aplicado los sistemas de videovigilancia se convierte en VIDA, ya que la Detección se realiza fundamentalmente de manera Visual, de tal suerte que esta labor se puede describir con el acrónimo ODA, ya que comprende el siguiente esquema de operación:

- Observar, que corresponde a la combinación de dos acciones: Ver, es decir, captar las imágenes, y Valorar, es decir, evaluar lo que se muestra en las imágenes.
- Decidir, ¿qué hacer? o ¿qué NO hacer? ante ello.
- Actuar, de acuerdo con lo que se haya decidido.

La concurrencia de estos procesos se ubica en los segmentos de Detección y Alertamiento en el contexto del Proceso de Seguridad para la atención de emergencias, CDAI., que se enfoca a la búsqueda de ciertos indicadores visuales en el contenido de la imagen, sobre los cuales se aplica una mecánica de valoración.

Estos indicadores visuales están proyectados para describir ciertas condiciones de interés, físicas (lo que hay) y funcionales

(lo que sucede), y contemplan dos aspectos:

- Indicadores de Normalidad, las condiciones que se espera que están regularmente presentes.
- Indicadores de Riesgo, las condiciones que deben estar ausentes, ya que su surgimiento regularmente implica la ocurrencia de alguna forma de riesgo.

## Panorama

La dinámica del recurso humano en el contexto particular del proceso CDAI con Sistemas de Videovigilancia, corresponde al desarrollo del esquema ODA, en el cual el factor crucial es la mecánica de valoración aplicada al contenido de las imágenes proyectadas.

La manera más efectiva de realizar el monitoreo de Videovigilancia es procesando una imagen a la vez, para lo cual la mecánica de valoración consiste en:

1. Captar y retener mentalmente el contenido de la imagen.
2. Analizar el contenido de la imagen.
3. Si no se detecta algún riesgo continúa con la siguiente imagen.
4. Si se detecta algún riesgo, se activa un protocolo de reacción.

La ejecución de esta mecánica de valoración debe realizarse, idealmente, en un lapso de 5 segundos o menos por imagen, con el propósito de incrementar las posibilidades de detección oportuna de las situaciones de riesgo. Para esto efectos, las tareas que se deben realizar comprenden:

- Memorizar, los grupos de parámetros conformados para los campos visuales del entorno de vigilancia.
- Diferenciar y correlacionar el grupo de parámetros pertinente para cada imagen.
- Cotejar el grupo de parámetros seleccionado contra la imagen y proceder en consecuencia.

## Perspectiva

El factor crucial de efectividad en el monitoreo de Videovigilancia

## EL PROCESO DE SEGURIDAD



- **Captación** de los hechos que ocurren en un entorno.
- **Detección** de una contingencia de seguridad, en particular Emergencias, en los hechos captados.
- **Alertamiento** a las corporaciones pertinentes para atender el tipo de contingencia detectada.
- **Intervención** de las corporaciones alertadas para atender la contingencia detectada.

es la carga de trabajo que representan los elementos de información que debe memorizar, diferenciar y correlacionar, tales como:

- Los parámetros de referencia.
- Los posibles escenarios de situación y los criterios para su valoración.

En este contexto, la carga de trabajo básica comprende el manejo de:

1. Un conjunto de al menos 3 grupos de parámetros para cada campo visual de cobertura en el entorno de vigilancia.
2. Un campo visual por cada cámara fija, y al menos 3 campos visuales por cada cámara móvil con una cobertura de 360°.
3. Un conjunto de al menos 3 grupos de parámetros para cada campo visual para cada rango de horarios a lo largo de una jornada de servicio.
4. Un conjunto de parámetros diferentes para cada día de la semana, así como para jornadas especiales.
5. Adicionalmente, conjuntos de parámetros para situaciones estacionales que modifiquen los perfiles "normales" de dinámica en el entorno de vigilancia.

Todo lo cual proyecta un problema de manejo de volumen y diversidad, tan sólo para memorizar y diferenciar los grupos de parámetros, así como para correlacionarse con los posibles escenarios que se pueden presentar.

También se proyecta un potencial de confusión para el monitorista por la complejidad de la dinámica en el entorno de vigilancia, la alteración emocional ante contingencias, la concurrencia de indicadores, en particular de riesgo, ya sea en la misma imagen o en diferentes imágenes en el mismo mosaico, así como situaciones de riesgo aparente de acuerdo a los elementos visuales proyectados, pero que en realidad resultan ser inocuos, como juguetes con apariencia de armas reales, o juegos bruscos entre personas.



Finalmente se tiene la posibilidad de que se presenten condiciones inéditas o no previstas, de tal suerte que, si el monitorista se concentra exclusivamente en los elementos de información conocidos, pasen desapercibidas, en una especie de efecto de "escotoma", ya que dichas condiciones suelen ser variaciones aparentemente inocuas de los indicadores de normalidad.

## Conclusiones

El potencial de efectividad en el monitoreo de Videovigilancia está determinado por la capacidad operativa del recurso humano, resultado de la conjunción de sus competencias personales con los apoyos con que se le doten, en especial los elementos de información que se derivan de un trabajo previo de análisis, y cuyo valor reside en su claridad y precisión a fin de que sean comprendidos por el monitorista.

Por parte del monitorista, la mayor exigencia se enfoca a la memorización y diferenciación, lo que induce presión a la valoración por la premura de respuesta ante emergencias. Por ello, cualquier forma de ayuda en este aspecto redundará en mayor efectividad del monitorista. Algunas alternativas para ello son la integración de los elementos información a analíticos de video, así como reducirle al monitorista los esfuerzos de memorización e incluso de diferenciación, a fin de que se focalice más en la valoración y se agilice la respuesta ante emergencias, lo que redundará en mejores posibilidades de proteger y preservar bienes y vidas, objetivo connatural de la Seguridad, al que pretende contribuir el monitoreo de Videovigilancia. **RS**

FÍSICO		FUNCIONAL	
¿Qué debe haber?	¿Qué debe suceder?	Indicadores de Normalidad	
¿Qué NO debe haber?	¿Qué NO debe suceder?	Indicadores de Riesgo	





## LAS 3 MEJORES CÁMARAS de videovigilancia para casa

### 1. Cámara WIFI LESHP

Con un precio muy accesible, la LESHP es una cámara HD con conexión a internet, que te da la tranquilidad de saber en todo momento qué ocurre en tu casa o el interior de tu negocio.

La cámara se maneja desde cualquier dispositivo mediante Sricam, una app gratuita muy sencilla (quizá demasiado) que puede dar problemas si usas el sistema operativo de Apple.

Con ella puedes enfocar o girar la cámara hasta casi 360° (80° en vertical y 355° en horizontal).

Además de ver las imágenes en directo, puedes programar la opción de grabar en una tarjeta microSD de hasta 128 Gb. Es mucha más capacidad, por ejemplo, que la que admite la cámara de seguridad YI, de modo que dispondrás de imágenes grabadas durante más tiempo.

El detector de movimiento es muy sensible, y puede saltar incluso con los cambios de luz. Pero a cambio es programable para que le indiques con qué intensidad de movimiento debe hacer saltar las alarmas, que se envían directamente a tu móvil.

También puede grabar imágenes nocturnas, en un perímetro de hasta 10 metros.





## 2. Yi Home Camera

La marca de cámaras Yi pertenece a Xiaomi, conocida sobre todo por sus teléfonos móviles de altas prestaciones a precio razonable. Es la misma tónica que siguen con Yi, que se dedica a cámaras de todo tipo: de vigilancia interior y exterior, para coche, cámaras deportivas...

El modelo que nos ocupa tiene un gran angular para aumentar el perímetro de visión, además de un zoom 4x si nos interesa centrar la atención en algún detalle.

El único pero es que el movimiento vertical tiene que hacerse manualmente. Es decir que tú la apuntas hacia donde quieres monitorizar y la cámara queda fija en esa dirección.

La app es muy sencilla de utilizar, y con ella puedes definir la zona de actividad que quieres grabar, la frecuencia y los horarios de alerta, o compartir la cámara con otro dispositivo, entre otras funciones.

Además de ver las imágenes en streaming, puedes instalar una tarjeta de hasta 32 Gb. No es mucho comparado con otras como la LESHP pero llega para unas 72 horas de grabación. Además es AutoLoop: cuando se acaba el espacio disponible, borra la primera hora de video para seguir grabando.

También tienes la opción de contratar grabación en la nube con Yi Cloud, con acceso seguro. Al comprar la cámara tienes un mes de prueba gratuito.



## 3. FREDI 360 grados

La cámara FREDI tiene todos los boletos para estar en este Top 3: un precio razonable, todas las prestaciones básicas y una buenísima valoración de los usuarios en internet.

Quizá lo único que te pueda echar para atrás a la hora de comprarla es que requiere colocación fija, cuando hay otras como la LESHP o la Yi que incluyen su propia base y por lo tanto puedes cambiarlas de lugar según te convenga.

Sin embargo, la instalación es sencilla. Su lugar natural es el techo y, una vez colocada, la cámara es tan discreta que te olvidarás de que está ahí.

La imagen es muy nítida, tanto a distancia como con el zoom y, si bien la calidad no es oficialmente Full HD, la resolución se acerca tanto que casi no notarás la diferencia.


El objetivo de ojo de pez permite obtener una visión de 360°, tanto de día como de noche, gracias a unos discretos sensores infrarrojos.

Las funciones se controlan mediante una app móvil, que responde bien en cualquier sistema operativo. Sin embargo, es importante tener en cuenta que el software no está planteado para usar desde la PC.

Incluye también detección de movimiento, alertas en el móvil y audio bidireccional, para poder mantener conversaciones a distancia.



## ¿Cómo escoger la mejor cámara de vigilancia para interior?

- Lo primero es pensar dónde vas a colocarla. Muchas cámaras de interior ya vienen con una base para que te ahorres tener que instalarla en la pared, evitando agujeros de taladro. De este modo puedes cambiar de habitación sin complicaciones, dependiendo del lugar que necesites monitorizar. Si tienes claro que vas a dejar la cámara fija, por ejemplo en la puerta de casa, puedes optar por una de pared o techo, que son bastante fáciles de colocar, y una vez instaladas te olvidas de ellas. Al ser de interior, un parámetro a tener en cuenta es el diseño. La mayoría son pequeñas y discretas, ya sea en forma de ojo (domo) o alargadas (bullet).
- Aunque ya prácticamente todas las cámaras son IP, las de precio medio no suelen admitir WiFi de 5 Ghz. También es necesario que la señal de WiFi sea de gran intensidad, porque si no es posible que la recepción de imagen sea floja o incluso llegue intermitentemente. Si realmente no quieres colocarla en otro lugar con mejor recepción, puedes instalar un repetidor de internet en cualquier enchufe cercano.
- Por último, hay que hacer una llamada a la seguridad. Casi todas las cámaras permiten proteger las imágenes con contraseña, y no deberías dejar de hacerlo. Si no, lo que pasa en tu casa podría ser accesible para cualquier hacker con un mínimo de conocimiento técnico y demasiado tiempo libre. 



### TABLA COMPARATIVA: CÁMARAS HOGAR

Características	LESHP	YI	FREDI
Conexión a Internet	Si	Si	Si
Visión nocturna	Si	Si	Si
Micrófono y altavoz	Si	Si	Si
Detección de movimiento	Si	Si	Si
Requiere instalación	No	No	Si
Tarjeta micro SD	hasta 128 GB	hasta 32 GB	hasta 128 GB





# TENABLE RESEARCH encuentra nuevas vulnerabilidades en las populares cámaras de seguridad inteligentes



Tenable®, Inc., la compañía de Cyber Exposure, anunció que su equipo de investigación ha descubierto siete vulnerabilidades graves en los sistemas de cámaras de seguridad Blink XT2 propiedad de Amazon. De ser explotadas, las vulnerabilidades podrían dar a los atacantes el control total de un dispositivo afectado, permitiéndoles ver de forma remota el metraje de la cámara, escuchar la salida de audio y secuestrar el dispositivo para usarlo en una botnet para realizar, por ejemplo, ataques de denegación de servicio distribuido (DDoS), robar datos o enviar spam.

Según Strategy Analytics, se vendieron más de 50 millones de cámaras domésticas inteligentes en 2018. Sin embargo, estos dispositivos también son una puerta de entrada potencial para que los malos actores obtengan acceso a información personal y redes domésticas. Si se explotan las fallas en Blink XT2, un atacante podría obtener información confidencial sobre la cuenta del propietario, lo que le permitiría ver fotografías y videos almacenados, agregar o eliminar dispositivos de la cuenta o bloquear completamente las comunicaciones de la cámara.

"Dispositivos conectados, como las cámaras Blink, están en todas partes. Precisamente por esa razón, los ciberdelincuentes se centran en comprometerlos", dijo Renaud Deraison, cofundador y director de tecnología de Tenable. "Los fabricantes de dispositivos IoT tienen la oportunidad y la obligación de garantizar que la seguridad efectiva se incorpore al diseño

general desde el principio y no sea agregada posteriormente. Esto es especialmente crítico cuando el dispositivo en cuestión es una cámara de seguridad. Agradecemos a Amazon por colaborar con nosotros en esta divulgación y garantizar que los parches se hayan lanzado de manera oportuna. Tenable Research continúa identificando y divulgando vulnerabilidades en la tecnología empresarial y de consumo, para mantener a las personas más seguras".

A medida que la superficie de ataque se expande con la adopción de dispositivos conectados, los que incluyen IoT y tecnología operativa (OT), la ciberseguridad fundamental es primordial. Tenable es líder en el tema al construir la mayor base de conocimiento de inteligencia de vulnerabilidades en la industria, y contar con uno de los mas grandes equipos de investigación de seguridad, quienes han superado su descubrimiento número 100 de día-cero en 2019. Su amplia investigación y experiencia en vulnerabilidades se extiende más allá de la TI tradicional e incluye todo, desde infraestructura crítica hasta aplicaciones empresariales. Tenable trabaja junto con los proveedores y toda la comunidad de seguridad para identificar, divulgar y parchear tecnología vulnerable, manteniendo a las organizaciones y a sus clientes más seguros.

Amazon ha lanzado parches para las vulnerabilidades y se insta a los usuarios a confirmar que su dispositivo esté actualizado a la versión de firmware 2.13.11 o posterior. **XS**

# ELECTRÓNICA Y TECNOLOGÍA



REVISTA DIGITAL  
ESPECIALIZADA EN ELECTRÓNICA Y TECNOLOGÍA

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





# Predicciones tecnológicas **VEEAM 2020**

Por David Rusell, Vicepresidente de Estrategia Enterprise de Veeam



*Durante el 2019, la tecnología ha beneficiado en la transformación de las empresas y comunidades. Desde los primeros despliegues de 5G hasta las empresas que comienzan a familiarizarse con la inteligencia artificial (IA), y por ende, ha sido otro año de rápido progreso.*

Desde la perspectiva de TI, hemos visto dos tendencias principales que se mantendrán en 2020. La primera es que las nubes locales y públicas se convertirán cada vez más en "ciudadanos iguales". Cloud se está transformando en el nuevo modelo normal de implementación, con el 85% de las empresas que hoy se auto identifican como predominantemente en nube híbrida o multi-nube. Relacionado con esto, están los problemas de ciberseguridad y privacidad de datos, que siguen siendo las principales preocupaciones de los tomadores de decisiones de TI en la nube. En 2020, las amenazas cibernéticas aumentarán en lugar de disminuir, por lo que las empresas deben asegurarse de que se pueda recuperar el 100% de sus datos críticos para el negocio.

Estas son algunas de las tendencias tecnológicas claves que las empresas buscarán aprovechar para prepararse en este año que comienza.

## 1. La adopción de contenedores se convertirá en mainstream

En 2020, la adopción de contenedores conducirá a una producción de software más rápida a través de capacidades DevOps más robustas y Kubernetes que consolidará su estado como la plataforma de orquestación de contenedores de facto. La popularidad de la adopción de contenedores o "contenedorización" se debe a dos cosas: velocidad y facilidad. Los contenedores son tipos de datos abstractos que aíslan una aplicación de un sistema operativo. Con los contenedores, los microservicios se empaquetan con sus dependencias y configuraciones. Esto hace que sea más rápido y fácil desarrollar, enviar e implementar

servicios. La tendencia hacia la nube múltiple significa que las empresas necesitan que los datos sean portátiles en varias nubes, especialmente los principales proveedores: AWS, Microsoft Azure y Google Cloud. 451 Research proyecta que el tamaño del mercado de las tecnologías de contenedores de aplicaciones alcanzará los \$ 4.3 mil millones para 2022 y en 2020 más empresas verán los contenedores como una parte fundamental de su estrategia de TI.

## 2. La Gestión Inteligente de Datos aumentará la movilidad y portabilidad de los datos

Las empresas recurrirán a la Gestión Inteligente de Datos para garantizar la disponibilidad de datos en todos los entornos de almacenamiento en 2020. Los datos necesitan ser fluidos en el panorama híbrido y en la multinube, y la capacidad de la Gestión Inteligente de Datos para aumentar la movilidad y portabilidad de los mismos es la razón por la que se ha convertido en una industria en sí misma. El informe de Veeam Cloud Data Management de 2019 reveló que las organizaciones se comprometieron a gastar un promedio de USD\$ 41 millones en la implementación de tecnologías de Cloud Data Management (CMD) este año. Para cumplir con las expectativas cambiantes de los clientes, las empresas buscan constantemente nuevos métodos para hacer que los datos sean más portátiles dentro de su organización. La visión de "sus datos, cuando los necesita, donde los necesita" solo se puede lograr a través de una estrategia sólida de CMD, por lo que su importancia solo crecerá en el transcurso de este 2020.

## 3. El triunfo del Backup y la velocidad dan paso a la restauración del éxito y la velocidad

Los acuerdos de nivel de servicio de Disponibilidad de datos (SLA) y las expectativas aumentarán en los próximos 12 meses. Mientras que el umbral para el tiempo de inactividad, o cualquier interrupción del servicio, continuará disminuyendo. En consecuencia, el énfasis en el proceso de Backup y recuperación se ha desplazado hacia la etapa de recuperación. El respaldo solía ser desafiante, laborioso y costoso. Las redes más rápidas, los dispositivos de destino de respaldo, así como las capacidades mejoradas de captura de datos y automatización han acelerado el respaldo. Según nuestro informe de gestión de datos en la nube de 2019, casi un tercio (29%) de las empresas ahora respaldan y replican continuamente aplicaciones de alta prioridad. La principal preocupación para las empresas ahora es que el 100% de sus datos sean recuperables y que ésta sea posible en minutos. Además de proporcionar tranquilidad cuando se trata de mantener la disponibilidad de datos, se puede utilizar un complemento completo de datos respaldados para fines de investigación, desarrollo y pruebas. La maximización del uso de estos datos ayuda a las empresas a tomar decisiones más informadas acerca de la transformación digital y las estrategias de aceleración empresarial.

## 4. Todo se está siendo definido por el software

Las empresas continuarán eligiendo las tecnologías de almacenamiento y el hardware que mejor funcionen para su organización, pero la administración del centro de datos se focalizará aún más en el software. El abastecimiento manual de la infraestructura de TI se está convirtiendo rápidamente en algo del pasado. Infraestructura como Código (Infrastructure as Code: IaC) continuará su proliferación. Al permitir a las empresas crear un plan de lo que debe hacer la infraestructura, luego implementarlo en todos los entornos y ubicaciones de almacenamiento, IaC reduce el tiempo y el costo de abastecer a la infraestructura en múltiples sitios. Sin embargo, los enfoques definidos por software como IaC y Cloud-Native, una estrategia que utiliza de forma nativa los servicios y la infraestructura de los proveedores de computación en la nube, no tienen que ver con el costo. La automatización de los procesos de replicación y el aprovechamiento de la nube pública ofrece precisión, agilidad y escalabilidad, lo que permite a las organizaciones implementar aplicaciones con rapidez y facilidad. Con más de las tres cuartas partes (77%) de las organizaciones

que utilizan software como servicio (SaaS), un enfoque definido por software para la gestión de datos ahora es relevante para la gran mayoría de las empresas.

## 5. Las organizaciones reemplazarán, no actualizarán, cuando se trata de soluciones de Backup

En 2020, la tendencia hacia el reemplazo de las tecnologías de Backup se acelerará. Las empresas priorizarán la simplicidad, flexibilidad y confiabilidad de sus soluciones de continuidad comercial a medida que la necesidad de acelerar las implementaciones tecnológicas se vuelvan aún más críticas. En 2019, las organizaciones dijeron que habían experimentado un promedio de cinco interrupciones no planificadas en los últimos 12 meses. Las preocupaciones sobre la capacidad de los proveedores heredados para garantizar la disponibilidad de datos están impulsando a las empresas hacia el reemplazo total de las soluciones de backup y recuperación en lugar de aumentar las soluciones adicionales que se utilizarán junto con las herramientas heredadas. Los factores que impiden dejar de lado las soluciones y actualizaciones provisorias de ser reemplazadas por completo incluyen costos de mantenimiento, falta de virtualización y capacidades en la nube, y deficiencias relacionadas con la velocidad de acceso a los datos y la facilidad de administración. Comenzar de nuevo les da a las empresas la tranquilidad de saber que tienen la solución adecuada para satisfacer las demandas de los usuarios en todo momento.

## 6. Todas las aplicaciones serán de misión crítica

La cantidad de aplicaciones que las empresas clasifican como de misión crítica aumentará durante 2020, allanando el camino hacia un escenario en el que cada aplicación se considera de alta prioridad. Anteriormente, las organizaciones estaban preparadas para distinguir entre aplicaciones de misión crítica y aplicaciones que no lo son. A medida que las empresas se vuelven completamente dependientes de su infraestructura digital, la capacidad de hacer esta distinción se vuelve muy difícil. En promedio, el informe de Veeam Cloud Data Management de 2019 reveló que quienes toman las decisiones de TI afirman que su negocio puede tolerar un máximo de dos horas de inactividad de aplicaciones de misión crítica. Pero, ¿qué aplicaciones verdaderamente pueden permitirse su falta de disponibilidad dentro de una empresa durante este período de tiempo? El tiempo de inactividad de las mismas les cuesta a las organizaciones un total de USD\$20.1 millones a nivel mundial en ingresos y productividad perdidos cada año, así como un promedio de USD\$102.450 por hora por los datos perdidos de aplicaciones de misión crítica. La verdad es que cada aplicación es crucial. **IS**







## MÁS ALLÁ DE LA CIUDAD "INTELIGENTE":

### Prepárese para la ciudad "hiperconectada"

Entre los objetivos: crear nuevas oportunidades de negocio, aumentar la eficiencia de los procesos gubernamentales y mejorar la seguridad y la salud pública, según un nuevo estudio realizado por la firma de investigación ESI ThoughtLab y patrocinado por Oracle. Esos beneficios vendrán con un retorno apreciable de inversión que crece a medida que se expande la conectividad, según el informe.

Un hallazgo sorprendente es la medida en que las ciudades hiperconectadas, incluso algunas con grandes inversiones en tecnología, admiten no estar en gran medida preparadas para los ataques cibernéticos.

#### Amplitud y rigor

El nuevo informe se basa en uno publicado el año pasado titulado "Ciudades más inteligentes 2025: Construyendo un plan sustentable de negocios y financiamiento", en el que ESI ThoughtLab investigó las iniciativas o planes de ciudades inteligentes de 136 municipios en 55 países. Ese informe encuestó a líderes de la ciudad, empresas y ciudadanos, incorporó datos de fuentes secundarias y recurrió a expertos externos para su análisis.

El nuevo informe, "Construyendo una ciudad hiperconectada", reduce el enfoque a 100 ciudades, desde Atenas a Varsovia, Bratislava a Washington, DC, que están gastando un total de \$ 141 mil millones de dólares en proyectos de conectividad en 2019, lo que representa una inversión promedio de \$1,220 dólares por ciudadano. Esas ciudades, un tercio de ellas en países en desarrollo, tienen una población de menos de 200,000 a más de 24 millones de habitantes.

*¿Qué pasó con la "ciudad inteligente"? Está viva y bien, pero transformándose en la "ciudad hiperconectada", impulsada por análisis de datos, inteligencia artificial, Internet de las cosas (IoT) y otras tecnologías avanzadas.*



El estudio agrupa las 100 ciudades en tres categorías: "implementadores" (25 ciudades), "anticipadores" (50) y "líderes" (25).

## Apuestas tecnológicas

El primer informe estableció las apuestas de la tabla de tecnología: cómputo en la nube, aplicaciones móviles, sensores y redes de IoT. Especialmente importante es la capacidad de adquirir, agregar, integrar y analizar datos, tantos datos como sea posible, de una variedad de fuentes, utilizando una plataforma de gestión de datos sofisticada.

El nuevo estudio refuerza la criticidad de los datos. Una mayoría (57%) de las 100 ciudades dicen que recurren a fuentes no gubernamentales para obtener esos datos, incluidas empresas, academia y redes sociales. Eso se eleva al 80% para las ciudades "líderes". Alrededor de las tres cuartas partes (76%) de los líderes describen sus ciudades como "avanzadas" en la recopilación y extracción de valor de los datos, mientras que el 68% dice que utilizan un sistema de gestión de datos para integrar los datos.

El análisis de datos está creciendo en importancia. Un porcentaje significativo de ciudades conectadas analiza datos para obtener información sobre su infraestructura de TI (64%), sistemas de pago y financieros (56%), sistemas de movilidad y transporte (49%) y seguridad física y digital (46%).

Entre las 100 ciudades estudiadas, el 90% usa la nube, Wi-Fi y tecnologías móviles, mientras que el 82% informa el uso generalizado (y creciente) de herramientas de Inteligencia Artificial, especialmente en relación con iniciativas de seguridad pública y gobernanza. Alrededor del 91% de las ciudades en el informe usan IoT hoy, un porcentaje proyectado para aumentar al 97% en tres años.

## Analizando el retorno de inversión

Las ciudades en el nuevo estudio de ESI ThoughtLab dicen que sus inversiones en conectividad generan un rendimiento promedio de entre 3% y 4%. Sin embargo, para los "líderes", el retorno de

inversión promedio es del 5%. La misma disparidad existe con los esfuerzos municipales específicos. Los líderes informan un retorno de la inversión del 7.1% de los sistemas digitales de presentación de impuestos, por ejemplo, mientras que el rendimiento promedio general es del 5.2%.

Las aplicaciones de transporte público digital son a menudo los primeros y más populares proyectos de conectividad. Entre las ciudades que los implementan, más de un tercio (38%) informan una mayor satisfacción de los pasajeros. Entre las ciudades que han implementado sistemas relacionados con el agua, por ejemplo, para monitorear la calidad y el uso en tiempo real, el 40% menciona mejoras en la salud pública y el bienestar de los ciudadanos.

La capacidad de generar estimaciones de retorno de inversión ayuda a las ciudades a obtener aprobaciones para sus proyectos de conectividad inteligente. Más de dos tercios (68%) de las ciudades en la categoría líder crean un caso de negocios detallado para todos sus proyectos inteligentes, y el 64% espera demostrar un retorno de inversión positivo antes de invertir en dichos proyectos. Ese hallazgo apunta, una vez más, al papel fundamental que juegan los datos y los análisis en los esfuerzos de las ciudades inteligentes.

## Para tomar en cuenta

El nuevo estudio contiene notas de advertencia sobre la preparación de seguridad, la adquisición de talento y los problemas de privacidad y normativos.

Menos de la mitad de las ciudades encuestadas se consideran "bien preparadas" para los ciberataques. Ese hallazgo sugiere que a medida que las ciudades invierten en proyectos y procesos de conectividad, se dan cuenta de sus vulnerabilidades en expansión.

Las pérdidas municipales relacionadas con eventos de seguridad cibernética promediaron \$ 3.4 millones de dólares durante el último año, con un 11% de las ciudades perdiendo más de \$10 millones de dólares, según el nuevo estudio. Las ciudades líderes informaron una pérdida promedio de \$ 6.2 millones de dólares.





Más de las tres cuartas partes (82%) de las ciudades conectadas dicen que planean aumentar sus presupuestos de ciberseguridad el próximo año, más de un tercio en más del 10%.

Encontrar el talento tecnológico necesario es tan desafiante para las ciudades conectadas como para las empresas modernas. Menos de la mitad (46%) de las 100 ciudades dicen que su personal tiene las habilidades necesarias en análisis de datos, pensamiento estratégico y resolución de problemas para avanzar en sus proyectos de conectividad.

El uso de la tecnología biométrica está muy extendido (83%) y está aumentando, según el estudio. Al mismo tiempo, el público está empezando a rechazar el uso de sistemas de reconocimiento facial, citando preocupaciones de privacidad.

Del mismo modo, los trabajadores desconfían del uso cada vez mayor de Inteligencia Artificial, debido a la preocupación de que sus trabajos puedan automatizarse. Por lo tanto, no es sorprendente que casi la mitad (45%) de los defensores de las ciudades inteligentes encuestados digan que los esfuerzos regulatorios podrían afectar su capacidad de recopilar y analizar datos.

### La inversión aumentará

El gasto general en iniciativas de hiperconectividad municipal aumentará en un 14% durante el 2020, según las ciudades que participaron en el nuevo estudio. Los implementadores dicen que aumentarán más sus inversiones, en un promedio del 21%. El tránsito y los proyectos de tránsito están recibiendo la mayor atención, seguidos de iniciativas de seguridad y salud pública.

Entre otras tecnologías emergentes, dos tercios de las ciudades conectadas dicen que ya están invirtiendo en redes de contabilidad

distribuidas de blockchain, y se espera que esas inversiones aumenten durante los próximos tres años, especialmente en las áreas de gobierno, financiamiento, construcción y mantenimiento. Las ciudades encuestadas también expresaron interés en usar redes móviles 5G, robots, drones y realidad aumentada.

El estudio ESI ThoughtLab del año pasado reveló una desconexión considerable entre los desafíos que las ciudades buscaban abordar con proyectos de ciudades inteligentes y aquellos que los ciudadanos y las empresas consideraban prioritarios. Este nuevo estudio muestra que las ciudades hiperconectadas están abordando esa desconexión. Más de la mitad (52%) dice que es fundamental obtener el apoyo de los ciudadanos y otras partes interesadas, mientras que casi un tercio de las ciudades líderes (32%) han designado un "oficial jefe de experiencia ciudadana", responsable de, entre otras funciones, la eficacia de una gama cada vez mayor de plataformas de comunicación, incluidos sitios web, correo electrónico, centros de llamadas, aplicaciones móviles, mensajes de texto y sitios de redes sociales.

El estudio anterior señaló que las ciudades inteligentes deben establecer un marco tecnológico, alinear sus iniciativas con las prioridades del gobierno, priorizar la recopilación y el análisis de datos y mantenerse al día con las tecnologías emergentes.

Un año después, el nuevo estudio señala que esos esfuerzos son solo los medios para un fin. El éxito requiere que las ciudades optimicen sus relaciones con las empresas, mejoren las interacciones con los ciudadanos y, en última instancia, eleven la calidad de vida de sus electores. Solo entonces llegará realmente la "ciudad hiperconectada". **ES**



# TALLER

## ESPECIALIZADO EN GERENCIA DE PROYECTOS MITIGACIÓN DE RIESGOS Y DISEÑO DE CONTRAMEDIDAS DE SEGURIDAD EN CADENA DE SUMINISTRO





# BIOMETRÍA DE VOZ

## evita fraude en el sector bancario



- *Los estafadores se están volviendo más sofisticados, trabajando a través de las redes y la ingeniería social en cuentas para cometer crímenes intrincados y devastadores, utilizando la información que obtienen a través de un ataque para obtener acceso a otras cuentas que una persona puede tener.*
- *Los bancos, las empresas de telecomunicaciones y los minoristas más grandes del mundo evitan el fraude y mejoran la experiencia del cliente a través de la tecnología.*

Nuance Communications, Inc (NASDAQ: NUAN), líder en innovaciones de IA conversacional, informa que Nuance Security Suite, basado en biometría, les ahorró a las organizaciones más de \$1 mil millones de dólares en costos totales de fraude durante 2018, al tiempo que permitió una manera más fácil y sin fricciones para que los clientes puedan validar sus identidades y acceder al servicio.

El fraude en los centros de contacto empresariales siempre ha sido un desafío para gestionar, pero con la explosión de canales digitales, las organizaciones se enfrentan hoy a asegurar un ecosistema cada vez más complejo. Al mismo tiempo, los estafadores se están volviendo más sofisticados, trabajando a través de las redes y la ingeniería social en cuentas para cometer crímenes intrincados y devastadores, utilizando la información que obtienen a través de un ataque para obtener acceso a otras cuentas que una persona puede tener. Javelin Strategy & Research informa que las adquisiciones de cuentas (ATO) se triplicaron durante el año pasado, lo que resultó en pérdidas de \$5.1B y un informe de CFCA (Communications Fraud Control Association) dijo que la industria de telecomunicaciones sufrió casi \$30B en pérdidas por fraude el año pasado.

En la actualidad la tecnología de Nuance está siendo implementada por más de la mitad de las instituciones financieras más grandes del mundo, así como en las 8 de las 10 compañías de telecomunicaciones más reconocidas mundialmente. Más de 400 millones de consumidores realizan anualmente más de 8 mil millones de autenticaciones exitosas utilizando la biometría de Nuance. Incluyendo casos de estudio en México de biometría de voz como el de Banorte.

Nuance Security Suite ayuda a las empresas a frustrar el fraude omnicanal a través de una oferta en capas de tecnologías de inteligencia artificial, que incluyen biometría de voz y comportamiento, detectores inteligentes de canales, geo y redes y algoritmos ConversationPrint™ y DevicePrint. Juntas, estas tecnologías pueden identificar a clientes legítimos a través del sonido de su voz, ubicación, dispositivo y la forma en que hablan, tocan y escriben, marcando cuando una llamada o interacción en línea es probablemente fraudulenta mediante el análisis de patrones de conversación típicos, características de voz y otros aspectos de una comunicación, identificando a los autores cuyos perfiles no coinciden con los de un cliente determinado.

"Con la biometría de voz de Nuance, obtenemos una visión más clara del comportamiento de los clientes y los estafadores, por lo que podemos mantener a los clientes genuinos protegidos y luchar contra los delincuentes que están apuntando a sus cuentas", menciona Jason Costain, Jefe de Estrategia de Fraude y Gestión de Relaciones en RBS Group. "En menos de un año, RBS ha analizado 17 millones de llamadas entrantes con Nuance Security Suite. De estos, 23,000 han llevado a alertas, y el banco ha descubierto que una de cada 3,500 llamadas es un intento de fraude. "El retorno de la inversión de la herramienta supera el 300%, por lo que la recuperación de nuestra implementación de tecnología ha sido muy impresionante".

A medida que los consumidores se sienten más cómodos con la identificación biométrica y las organizaciones buscan formas innovadoras de autenticación, la adopción de Nuance Security Suite está creciendo a un ritmo acelerado. Las implementaciones recientes incluyen Lloyds Banking Group, Allied Irish Bank, Deutsche Telekom, Rakuten Life Insurance y RBS Group. Además de frenar el fraude, la biometría de Nuance reduce el tiempo total que los agentes dedican a resolver las consultas de los clientes, con una empresa multinacional de servicios financieros que reduce el tiempo de gestión del agente en 89 segundos después de implementar el producto.

"Nuestros clientes acuden a nosotros no solo porque desean que su proceso de autenticación sea más conveniente para los clientes, sino que quizás lo más importante sea desarrollar su estrategia de seguridad del centro de contacto. Nuestro enfoque es único en el sentido de que nuestros algoritmos no solo pueden identificar y validar a las personas por su voz, sino que también entienden qué tipos de patrones de conversación suelen usar los estafadores. Eso es poderoso cuando considera cuánto dinero se pierde debido al acceso fraudulento a la cuenta cada año, ya sea a través de canales telefónicos tradicionales o en ataques complejos entre canales", explica Brett Beranek, Gerente General del área de Negocio de Seguridad en Nuance Enterprise. **MS**



*Los días 5 y 6 de junio de 2019, en el Centro Convex, en la ciudad de Monterrey, se realizó la vigésimo octava edición del congreso de la AMPPAC, "La Seguridad y Protección Hoy".*

La Asociación Mexicana de Profesionales en Prevención de Pérdidas A. C. fue constituida hace más de 33 años por iniciativa de algunos ejecutivos de la seguridad en el estado de Nuevo León. La finalidad de la asociación es

propiciar intercambios de experiencias y conocimientos profesionales relativos a la seguridad y la protección. En estos años, la AMPPAC se ha convertido en una de las asociaciones de mayor prestigio y presencia a nivel nacional.

La asociación realiza constantes acciones de capacitación, y a través de cursos y diplomados promueve la profesionalización de los servicios de seguridad. Pero sin duda el evento más exitoso ha sido el congreso anual, realizado ininterrumpidamente desde hace 28 años ocasión, en los dos días del congreso, se realizaron 12 conferencias, todas relativas a la seguridad, algunas

enfocadas en la prevención, otras en la administración y capacitación de recursos humanos.

Cientos de profesionales de la seguridad asistieron al congreso, y entre los conferencistas había expertos en seguridad provenientes de Colombia, México y los Estados Unidos. En esta ocasión fue evidente el incremento en el número de expositores y asistentes al congreso.

No hay duda de que este congreso fue un éxito. Entre los asistentes hubo profesionales de seguridad del estado de Nuevo León, pero también de otros, como Jalisco, Puebla, Guanajuato y el Distrito Federal. **MS**





*La INTCOMEXPO contó con la participación de más de 40 fabricantes, y además de las capacitaciones técnicas y comerciales de las marcas, se dieron charlas especializadas en mercados verticales como: seguridad, punto de venta, descarga digital y gaming.*

## 25<sup>a</sup> Edición de **INTCOMEXPO**

Como parte de las celebraciones del 30 aniversario de Intcomex se realizó, los días 23 y 24 de octubre, en el hotel Hilton Reforma de la Ciudad de México, la edición número 25 de INTCOMEXPO, uno de los eventos más importantes de tecnología a nivel del sector tanto de seguridad como de tecnología.

También hubo dos conferencias magistrales, una a cargo de Dimas Gimeno, presidente de El Corte Inglés, uno de los retailers europeos más importantes, y la otra a cargo de Marcus Dantus, un famoso conferencista y líder de Startup México, el programa más ambicioso para el fomento del emprendimiento y la innovación en nuestro país.

Durante la inauguración, Sandra Mendoza, gerente de marketing en Intcomex, agradeció a los clientes su lealtad durante los 30 años de existencia de la empresa mayorista y destacó que el formato del evento fue diferente a los años anteriores:



“Este año los asistentes pudieron experimentar algo diferente, viviendo dentro de las temáticas y conociendo la manera de utilizar la tecnología que vendemos en cada una de las verticales”.

No se trató solo del tradicional centro de exhibición, sino que fue un lugar donde pudieron comercializar sus soluciones: “Queremos que vivan esta experiencia y encuentren la forma de darle la vuelta al negocio, es una herramienta más a nuestros canales para poder encontrar más oportunidades en diferentes nichos de mercado y poder desarrollar de mejor forma su negocio”, aseguró.

“Este año cumplimos 30 años de la empresa y contamos con 14 sucursales en Latinoamérica, somos una empresa que se dedica al 100 por ciento a la distribución de productos de tecnología y seguridad, y estamos empezando a trabajar en retail y en la parte del transporte. Somos, sin duda, el mejor mayorista de servicio de tecnología a los distribuidores”.

En transporte, la intención de la empresa es llevar soluciones de IoT y tecnología a los distribuidores, y para ello dispone de varias alianzas, una es con Mobileye, un fabricante israelí que compró Intel hace algunos años que es un sistema de previsión de colisiones y desvío de carril. También tienen otra aplicación de GPS y telemetría que se llama Amber Connect, encaminada a recuperación, monitoreo y rastreo con un sistema de dashboard orientado al mercado de las aseguradoras.

En esta ocasión, los asistentes a la INTCOMEXPO tuvieron una sorpresa muy interesante: por cada 5 mil pesos de compra, ganaron un boleto para participar en la rifa de un automóvil, un viaje con destino a la playa y dos motos. **XS**





## IP USERGROUP

culmina exitosamente el año 2019,  
en Uruguay

*Con la asistencia  
de más de 80  
profesionales de  
la industria de la  
seguridad uruguaya,  
el pasado miércoles  
20 de noviembre,  
se llevó a cabo  
EXPO Seguridad  
& Conferencias  
"IP-in-Action LIVE  
Montevideo"*


El ciclo de eventos "IP-in-Action LIVE" propuesto en el transcurso del 2019, siguió puntualmente su cronograma y en esta ocasión, el turno fue para la ciudad de Montevideo en el Hotel Hyatt Centric Montevideo. Este evento superó ampliamente el número y el perfil de los asistentes con respecto a nuestra anterior visita en el año 2014.

La apertura del evento estuvo a cargo de Manuel Hernández - Sales Manager South America LAR Group para Milestone Systems con la conferencia: "Milestone, la plataforma de Comunidad Abierta, segura: por diseño, por defecto y por desarrollo".

Posteriormente, continuaron con sus presentaciones los expositores que participaron de este exclusivo evento en la acogedora y amable ciudad de Montevideo, representantes de: Raytec Systems, Optex, Genetec, InVidTech, VSS (Video Storage Solutions) y Security College US a quienes les agradecemos por su valioso aporte, activa y excelente participación durante toda la jornada.

"Excelente evento generado en una región que no posee mucha difusión de tecnología de seguridad, contentos por la participación y concurrencia. Mucho interés en las soluciones presentadas y expectativas favorables de continuar trabajando en las mismas". - José Luis Martínez, Sales Manager Southern Cone, Raytec Systems / Optex.

Otorgamos un especial agradecimiento para nuestros Medios y Organizaciones Aliadas que brindaron su apoyo en la ejecución de este evento: En especial a la Revista Xtrem Secure.

Finalmente, es importante resaltar que la asistencia a los eventos "IP-in-Action LIVE" es totalmente gratuita. Cada evento siempre va a la vanguardia de los avances tecnológicos y conceptuales en el área de la seguridad y es por ello que incluye un amplio programa de seminarios educativos, junto con un área de exhibición y demostración de los más recientes productos y servicios utilizando Tecnología IP y sus aplicaciones. Los próximos encuentros se realizarán en Bogotá - 26 de febrero 2020 y en Santo Domingo - 15 de abril 2020. 



El centro para el aprendizaje y conocimiento de la seguridad física y en red.

Oportunidad única para ampliar su red de contactos.

El evento de actualización y networking por excelencia!

**2020**

Tel.: +593 2 604 08 06

E-mail: [pr@ipusergrouplatino.com](mailto:pr@ipusergrouplatino.com)

MEDIO ALIADO



IP-in-Action LIVE

**Bogotá**

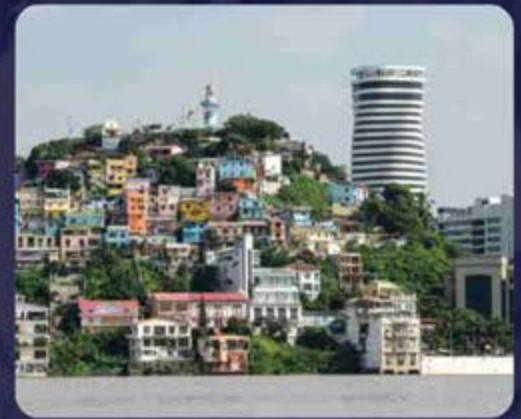
Febrero 2020



IP-in-Action LIVE

**Santo Domingo**

Abril 2020



IP-in-Action LIVE

**Guayaquil**

Junio 2020



IP-in-Action LIVE

Ciudad de **Guatemala**

Agosto 2020



IP-in-Action LIVE

Ciudad de **México**

Octubre 2020



IP-in-Action LIVE

**Lima**

Noviembre 2020





## FBI advierte sobre los riesgos de seguridad asociados a los SMART TV

Por Juan Manuel Harán

A través de un comunicado, la entidad norteamericana busca concientizar a los usuarios sobre los riesgos de seguridad asociados a los televisores inteligentes.

El Buró Federal de Investigaciones (FBI, por sus siglas en inglés) aprovechó la previa al Black Friday, fecha que se ha extendido a nivel global y en la cual se registra un alto volumen de compras por parte de los usuarios, para informar sobre los riesgos de seguridad asociados a los dispositivos inteligentes, particularmente a los Smart TV.

En la actualidad, con la popularidad de plataformas de streaming como Netflix, Amazon o YouTube premium, entre otros, la mayoría de los usuarios prefiere televisores que tengan conexión a Internet.

Sin embargo, más allá del hecho de que los fabricantes de televisores y desarrolladores de aplicaciones nos estén escuchando y monitoreando, muchos usuarios no son conscientes de que por el hecho de estar conectados a Internet estos dispositivos pueden permitir a un atacante ingresar a nuestro hogar, explica el comunicado del FBI. Esto último lo explicó en profundidad la investigadora en seguridad de ESET, Denise Giusto, en su artículo Smart TV: ¿una puerta de acceso al hogar para un atacante?

En este sentido, a partir de la explotación de un fallo de seguridad en un televisor inteligente un atacante podría acceder a otros dispositivos conectados a la misma red Wi-Fi y robar información personal, como credenciales de acceso. También puede suceder al revés, que un atacante explote un fallo de seguridad o una mala configuración en un router que le permita acceder al televisor, como fue en caso que ocurrió a principios de este año cuando atacantes tomaron posesión de Smart TVs y otros dispositivos IoT para desplegar anuncios.

*A través de un comunicado, la entidad norteamericana busca concientizar a los usuarios sobre los riesgos de seguridad asociados a los televisores inteligentes.*

Otro punto que menciona el FBI es que muchos de los modelos de los nuevos televisores que salen al mercado incorporan cámaras, las cuales son utilizadas en algunos casos para el reconocimiento facial y saber qué usuario está frente al televisor para poder realizar sugerencias. En este sentido, si un atacante toma el control de nuestro televisor podría llegar a controlar la cámara y el micrófono incorporado para espiarnos. Una opción que recomiendan desde el FBI, en caso de no poder desactivar la cámara, es colocar cinta negra para taparla.

Si bien no son comunes los ataques a televisores inteligentes, esto no quiere decir que no se hayan registrado casos. Muchos dispositivos de este tipo son inseguros debido a malas configuraciones que vienen de fábrica, principalmente como consecuencia de la falta de consideración de aspectos de seguridad durante la etapa de diseño y manufactura de los equipos.

En cuanto a las recomendaciones para estar protegido, además de instalar las actualizaciones que el fabricante vaya lanzando, al igual que los desarrolladores de las apps instaladas en el televisor, otras recomendaciones para mantener los televisores inteligentes es utilizar una solución de seguridad contra amenazas para Smart TV, revisar las configuraciones para evitar dejar puertas abiertas y revisar las políticas de privacidad, los permisos del dispositivo y de las aplicaciones, para averiguar, entre otras cosas, qué información recopilan y cómo la utilizan. **XS**





## DRON MQ-9 DE EEUU asesinó a líder militar de Irán

Estados Unidos confirmó la muerte de Qassem Soleimani, quien era el militar más poderoso del régimen iraní, mediante el uso de un dron. Y pese a que no dio detalles sobre su naturaleza, numerosos medios lo identificaron como el MQ-9 Reaper, la principal aeronave no tripulada a la que las Fuerzas Armadas recurren para operativos de esta naturaleza.

El MQ-9 Reaper tiene 20 metros de envergadura y 11 de largo, y pesa más de 2 toneladas. Es un avión armado multimisión, con techo de vuelo medio, larga autonomía y pilotaje remoto que se emplea principalmente para la ejecución de objetivos en movimiento, además de como activo de inteligencia.

Fuentes del Pentágono no confirmaron ni negaron que el dron fuera el modelo de aeronave no tripulada empleado para terminar en la madrugada con la vida de Soleimani y el número dos de las milicias chiítas iraquíes, Abu Mahdi al Muhandis en una carretera cercana al aeropuerto de la capital iraquí de Bagdad. Sí dejó en claro que Donald Trump fue quien ordenó la operación y que éste fue exitosa.

El MQ-9 Reaper fue diseñado por General Atomics Aeronautical Systems y entró en servicio en 2007. Cada unidad tiene un costo de USD 64,2 millones. Actualmente, la Fuerza Aérea de EEUU cuenta con una flota de 93 de estas naves.

Este dron tiene una altitud máxima de vuelo de 15,240 metros, una autonomía de 1,850 kilómetros y alcanza una velocidad de crucero media de 370 kilómetros por hora. Las misiones estándar requieren de un piloto para controlar la aeronave y comandar la misión, y otro miembro de tripulación para operar los sensores y armas. En ocasiones, se suma también un coordinador de misión.

La aeronave cuenta con un Sistema de Apuntado Multiespectral



que le permite descubrir y designar objetivos mediante sensores láser e infrarrojos así como mediante el uso de diversas cámaras que, además, permiten ver su actividad en directo desde cualquier rincón del planeta.

Es gracias a este sistema que el MQ-9 Reaper puede emplear sus bombas guiadas Unit-12 Paveway II y GBU-38, así como los misiles aire-tierra AGM-114 Hellfire, que la Fuerza aérea afirma que permiten llevar a cabo ataques sobre objetivos con una bajo porcentaje de daños colaterales.

El dron puede además ser desplegado en cualquier parte del globo gracias a su capacidad de ser almacenado en contenedores capaces de transportarse en aviones con una capacidad de carga igual o superior a la del avión militar estadounidense C-130 Hércules. ✖





**20 & 21**  
Febrero 2020



**Descuentos para:**

Socios ALAS, Usuarios finales, Gobierno,  
Asistentes a eventos ALAS y Grupos.

---

 [eventos@alas-la.org](mailto:eventos@alas-la.org)  
 321 615 3368

---

[www.alas-la.org/congresoalas](http://www.alas-la.org/congresoalas)



Esto es un evento de la:







# SEGURIDAD PRIVADA **MX**



REVISTA DIGITAL

ESPECIALIZADA EN SEGURIDAD PRIVADA

[www.seguridadprivadamx.mx](http://www.seguridadprivadamx.mx)





Blanca Breña, Jefa de Relaciones con Gobierno de la ANTAD

# ANTAD “Simposio de Seguridad 2019”

*El objetivo del encuentro, que reúne a empresas y expertos en temas de seguridad, es ofrecer a los ejecutivos la oportunidad de actualizarse y conocer mejor los principales problemas que enfrenta el sector del retail, así como obtener herramientas que les permitan mejorar sus prácticas.*



Jaime Domingo López, Presidente de la Comisión de Seguridad del Consejo Coordinador Empresarial



Los días 29, 30 y 31 del pasado mes de octubre se llevó a cabo, en el hotel Marquis de la Ciudad de México, la 29ª edición del Simposio de Seguridad, evento organizado por la Asociación Nacional de Tiendas de Autoservicio y Departamentales (ANTAD).

En esta edición del simposio se abordaron diversas áreas temáticas, como los ejes de desarrollo de cadenas, eficiencia operativa para reducir mermas, procesos y protocolos, manejo eficiente de inventarios y gestión de crisis, entre otros.

La bienvenida a los más de 200 asistentes del encuentro estuvo a cargo de Vicente Yáñez, presidente ejecutivo de la ANTAD, y Jorge Rodríguez, consejero delegado del comité de seguridad de esa organización.

# GECSA

## SEGURIDAD PRIVADA



*SI LO PUEDES PREVER*  
***LO PUEDES RESOLVER***

[www.gecsa.com.mx](http://www.gecsa.com.mx)

01 (55) 5363 2868 | 01 (55) 5373 1761

Calle Limoneros No. 9-A, Col. Valle de San Mateo Naucalpan, Estado de México, C.P. 53240





La primera conferencia del simposio estuvo a cargo de Macario Schettino, reconocido analista político, quien analizó la situación actual del país y los posibles escenarios para el futuro. Después vinieron las ponencias de Jaime Domingo López, presidente de la comisión de seguridad del Consejo Coordinador Empresarial y Muna Buchahin, presidenta de la Asociación de Examinadores de Fraudes Certificados.

Durante los tres días del simposio, expertos del sector, de empresas como Soriana, Liverpool, Home Depot y Oxxo, compartieron con los asistentes algunos casos de éxito y metodologías para mejorar la productividad de sus negocios a través de medidas de seguridad.

Blanca Breña, Jefa de Relaciones con Gobierno de la ANTAD, nos comentó que: “el objetivo del Simposio de Seguridad es ofrecer a los ejecutivos del área de seguridad de las cadenas detallistas, la oportunidad de actualizarse, conocer los temas de vanguardia y propiciar un ambiente de negocios”.

“Está dirigido a directores generales, ejecutivos de prevención de pérdidas, capital humano, auditoría, protección de activos, operaciones, mandos medios, de áreas legales, y a toda persona relacionada con el área de prevención de pérdidas y seguridad”.

“Los temas que se presentan y los conferencistas a los que se invita se determinan cuando enviamos una encuesta al Comité Nacional de Seguridad de ANTAD para conocer las necesidades del sector y buscar a los profesionales en los temas. En el programa de capacitación estuvieron presentes más de 20 profesionales en el área de Seguridad y Prevención de Pérdidas”.

La industria del retail en México requiere de capacitación, gestión y estrategias que permitan reducir incidencias delictivas en las cadenas de autoservicio. De acuerdo con cifras de la ANTAD, de enero a septiembre de 2019 se registraron 64 mil 805 incidentes delictivos en el sector y este organismo hizo una medición de 19 tipos de delitos que afectan la operación del comercio.

La ANTAD está conformada por 104 cadenas comerciales, 32 de ellas de autoservicio, 16 departamentales y 56 especializadas, que en conjunto suman más de 51 mil establecimientos.



Macario Schettino, Analista Político



El Comité de Seguridad de ANTAD realiza reuniones mensuales con la Comisión Estatal de Seguridad y Fiscalía del Estado de México, así como con la Secretaría de Seguridad Ciudadana a fin de establecer estrategias que permitan reducir incidencias delictivas en las tiendas.

Sin duda, la edición 29 del Simposio de Seguridad fue todo un éxito, tanto por la organización y selección de temas, como por la participación de los cientos de asistentes. ■



Armando Zuñiga, Coordinador General de ASUME (extremo derecho)



**10 años**  
Gracias por tu  
confianza



**GRUPO LK**  
SEGURIDAD PRIVADA

*“ La experiencia  
está anclada al plan  
maestro del cuerpo ”*

[grupolk2020@gmail.com](mailto:grupolk2020@gmail.com)



VIGILANCIA  
INTRAMUROS



CUSTODIAS



SEGURIDAD  
ELECTRÓNICA



MONITOREO Y  
RASTREO VEHICULAR

**Contamos con Cobertura a Nivel Nacional**

Tel: (55) 8848 8264





## NUEVA GENERACIÓN DE DSI

**E**l diplomado DSI es un esfuerzo que nació en 1996 como una respuesta a la necesidad de encontrar un foro de actualización y especialización de los profesionales, gerentes y ejecutivos, de la seguridad. Comenzó un poco a contracorriente porque mucha gente decía que no se podía llevar la seguridad a las aulas de las universidades y ese reto llevó a arrancar, en el 96, una primera generación. Fue tal el éxito que ahora se llega a la graduación de la generación 25 del diplomado.

El DSI se fue convirtiendo, poco a poco, en una de las mejores opciones que tienen las empresas para preparar a sus ejecutivos de seguridad con una visión realmente global y



*El pasado 25 de octubre, en las instalaciones de la Cámara de Comercio de la Ciudad de México, se realizó la ceremonia de graduación de la generación número 25 del diplomado de Director de Seguridad Integral.*

muy práctica. El DSI tiene la virtud de que lo que ahora se ve en la clase, mañana lo está aplicando el alumno en su trabajo.

Al principio, el diplomado fue respaldado académicamente, y por 22 generaciones, por la Universidad del Valle de México. Después hubo un cambio de rumbo en la institución y se tuvo que buscar el respaldo de otro centro de estudios, ahora esa responsabilidad la tiene la Universidad Internacional de la Rioja en México.

Por su conformación, por su fortaleza, el diplomado tiene dos características, el que sabe de seguridad aprende de administración y el que sabe de administración aprende de seguridad, y el que sabe de ambas cosas consolida su perfil profesional para ser un especialista en seguridad con capacidades gerenciales.

Actualmente las empresas demandan dos tipos de competencias en sus ejecutivos: competencias de nivel, como liderazgo, la toma de decisiones, el análisis de problemas, y competencias de área, como el análisis de riesgo, la protección ejecutiva, las investigaciones y la protección civil.

El diplomado ofrece una gama de temas, en cada uno de los ocho módulos que lo componen, en donde se ven temas técnicos, administrativos y humanos. Eso da una solidez y un balance a los conocimientos que se adquieren.

Para conocer un poco de su sentir, conversamos con del Lic. Teodoro Serralde graduado en esta generación, esto fue lo que comentó:

## Teodoro Serralde Medina, de Serralde Consultores Jurídicos

*"Significa para mí la conclusión de un periodo en el que asimilamos conocimientos sobre seguridad de una manera metodológica, científica, que nos permite tener mayor sustento y mayor soporte de nuestro trabajo cotidiano".*

*"Me gusta ser parte de un grupo de profesionales, y de amigos, que complementan la parte profesional. En el diplomado se generan vínculos que nos van ayudando en el sentido individual y en el colectivo".*

*"Representa un enorme esfuerzo, de nueve meses de estar en el aula. Son 290 horas de clase, pero hay que considerar todo el tiempo que se destina estudiando, o investigando, o realizando los diferentes trabajos. Son nueve meses de esfuerzo que impactan también a nuestras familias".*

*"Pero vale totalmente la pena, por los conocimientos que se adquieren. Al final, el tema de ser parte de un grupo de amigos es invaluable. El conocimiento se puede adquirir de manera individual, pero el grupo nos da una fortaleza que influye profundamente en nuestras vidas".*



## GENERACIÓN 25

- Gigliolla Agassini Tellez
- Claudia Teresa Ávalos Jaimes
- Victoriano Benitez Chávez
- Héctor Joel Bernechea Solórzano
- José Manuel Cadena Moya
- Jorge Alberto Córdova Gama
- Rodrigo Funcia Díaz
- David García Morales
- José Guadalupe González García
- Rodolfo Jaime Hernández Falcón
- Juan Carlos Hernández Morales
- Paola Huerta Reyes
- Héctor Iván Mendoza Tellez
- Alfredo Miranda Medina
- Edgar Morales Espinosa
- Luis Francisco Paz Pérez
- Juan Carlos Perea Gómez Arzapalo
- Xavier Pérez Flores
- Martín Reyes Álvarez
- Hermelindo Rodríguez Sánchez
- Miguel Ángel Romero Villalobos
- Roberto José Rosello Latrónico
- Raymundo Gabriel Sánchez Segura
- Teodoro Antonio Serralde Medina
- Edgar Li Vázquez Amador





# ESPECIALISTAS EN UNIFORMES PARA SEGURIDAD



**E**n este año que inicia Xtrem Secure “El Mundo de la Seguridad” se dio a la tarea de entrevistar a uno de los principales proveedores de la industria, Uniformes JR quien es liderado por el Lic. Emmanuel González Sojo, a continuación les presentamos un extracto de lo que nos comentó:

**UNIFORMES JR SA. DE CV.** es una empresa orgullosamente mexicana que día con día realiza un esfuerzo constante por proveer de uniformes a la industria de la seguridad. Nace de la experiencia, amistad y lealtad de sus socios fundadores: El Ing. Jorge Septién Esnaurizar y el Mayor Roberto González quienes hicieron posible que esta empresa iniciara actividades en 2008; teniendo como objetivo el cumplimiento estricto de los requerimientos y necesidades de los clientes.

El esfuerzo y la dedicación constante de quienes conforman la empresa ha derivado en un crecimiento constante en el mercado de uniformes para seguridad y al mismo tiempo se ha contribuido a que las empresas en Seguridad Privada sean más competitivas.

Actualmente UNIFORMES JR SA. DE CV. es dirigida por el Lic. Emmanuel González Sojo, DSE, DSI, encabezando la administración y desarrollo del negocio.

## ¿Cuál es su mercado principal?

Uno de nuestros principales mercados es el de seguridad en todos sus rubros, pero también estamos en otros mercados como el sector industrial, corporativo y escolar.

## ¿Qué tanta aceptación ha recibido por parte de las empresas de seguridad privada?

MUY POSITIVA, debido que una de las necesidades de la

seguridad privada, es tener uniformes nuevos y listos en corto tiempo, por tal motivo es uno de nuestros objetivos primordiales.

## ¿Precio o calidad? ¿Por cuál se inclina Uniformes JR?

Nuestro lema siempre ha sido “LA CALIDAD NO ESTA PELEADA CON EL PRECIO” esto marca un equilibrio a través de nuestras propuestas económicas ofreciendo variedad de productos a su elección, generando la satisfacción del cliente.

## ¿Cuáles son las expectativas de Uniformes JR para el 2020?

Acceder a clientes potenciales, generar mayor servicio y calidad, principalmente seguir manteniendo la confianza de nuestros clientes actuales.

## ¿Están manejando alguna promoción especial?

Tenemos promociones regulares de 10% de descuento para asociados de AMEXSI.


## ¿Distribuyen a toda la república mexicana?

Tenemos puntos de venta estratégicos en ciudades como Monterrey, Guadalajara, Toluca y la CDMX a demás de contar con alianzas con mensajerías como Estafeta y DHL, dando precios preferenciales.

## ¿En dónde pueden contactarlos?

Estamos a sus órdenes en la página de internet:  
[www.uniformesjr.com.mx](http://www.uniformesjr.com.mx)

## ¿Algo más que desee agregar?

Nuestro Plus, es la realización de stock exclusivos con nuestros clientes, con la finalidad de que los tiempos de entrega sean casi inmediatos. 



Ing. Jorge Septién Esnaurizar, DSI y DSE (en el centro).



Lic. Emmanuel González Sojo, con su familia en la fiesta de AMEXSI.



Patrocinador oficial en la cena AMEXSI 2019.



¡LA CALIDAD  
NO ESTÁ EN CONTRA  
DEL PRECIO!

UNIFORMES A LA MEDIDA  
PARA EMPRESAS DE SEGURIDAD



Federal



Privada



Pública



Militar

CLIENTES  
LEALES:



- INFORMES -

Cerrada de Palmira No.14, Francisco Villa, Tlalnepantla, Estado de México,  
C.P. 54059, Tels: (0155) 2873 0771 y (0155) 5082 2968, ventas@uniformesjr.com.mx

[www.uniformesjr.com.mx](http://www.uniformesjr.com.mx)





## REUNIÓN MENSUAL DE ASIS

### Capítulo México

*El pasado 12 de noviembre se llevó a cabo, en la Hacienda de los Morales de la Ciudad de México, la tradicional reunión mensual de ASIS Capítulo México. Al hacer uso de la palabra, Pedro Sanabria, presidente ejecutivo del Capítulo, presentó su informe mensual de actividades, en donde destacó el éxito que tuvo el Security Week LATAM ASIS 2019, realizado del 13 al 17 de octubre de 2019.*

**D**urante el Security Week se realizaron diferentes webinars, que conjuntaron a más de 600 socios de distintos países latinoamericanos, se impartieron 45 conferencias, a las que asistieron más de 300 personas, y hubo tres conferencias magistrales, un smoking challenge y una jornada de escuelas seguras.

Antes de concluir el penúltimo desayuno del año, Pedro Sanabria firmó un nuevo convenio de colaboración con Círculo Laboral y entregó reconocimientos, por su trayectoria, a los expresidentes del Capítulo: César Romero, Armando Zúñiga, Marcos Solórzano y Gabriel Bernal.

En esta ocasión **Corporativo COMEXA** fue la patrocinadora del desayuno. Esta empresa se caracteriza por la creatividad y la innovación al ofrecer diferentes soluciones en campos como alarmas, videovigilancia, control de accesos, detección de incendios y sistemas de intercomunicación.

La conferencia estuvo a cargo de Carlos Juárez Cruz, director del Instituto para la Economía y la Paz, institución fundada hace 14 años, en Australia. Esta organización ha crecido y actualmente cuenta con sedes en seis países, de cuatro continentes. Los estudios que realiza están enfocados a la construcción de la paz y la transformación de conflictos. Su producto más conocido es el Índice de Paz Global, mencionado con frecuencia en los medios de comunicación.

En su ponencia, Carlos Juárez aseguró que en México las empresas de seguridad privada están atendiendo una gran demanda en materia de protección, ya que los cuerpos de seguridad pública no pueden dar solución a este problema, y afirmó que México invierte el 0.81% de su Producto Interno Bruto (PIB) en sistemas de seguridad pública y justicia, una cantidad muy baja si se compara con otros países de región.

“Perú, Bolivia, Guatemala, Honduras, Brasil y Argentina, invierten más del doble de lo que destinamos nosotros como proporción



del PIB. Parece que se invierte mucho, que se gasta demasiado y que sale muy caro, pero lo que hace falta es inversión estratégica, aprovechar mejor la tecnología para fortalecer las capacidades de las policías, además de dignificar a los elementos policíacos”.

De acuerdo con el Índice de Paz México 2018, los homicidios se incrementaron en un 14 por ciento, es decir, por cada 100 mil habitantes, 28 personas son asesinadas. En el caso del estado de Guanajuato, la tasa de homicidios creció 126% el año pasado, en Quintana Roo se duplicaron los delitos con armas de fuego en un 85%, y en Oaxaca tanto los homicidios como los delitos con armas de fuego aumentaron más del 250% desde el 2015.

Una de las conclusiones del experto fue que “en el país la paz se deterioró un 5% el año pasado, y también se han disparado los ataques contra políticos y periodistas, aunque los aspectos que más inquietan tienen que ver con la falta de gasto estatal en seguridad y los pocos crímenes que se denuncian, solamente un 10%, y en algunos casos, menos”. **RS**



# PROGRAMA DE PREPARACIÓN PARA PRESENTAR EXAMEN DE CERTIFICACIÓN



CERTIFÍCATE ESTE 2020  
CON ASIS MX



SOMOS EL ÚNICO CURSO DE  
PREPARACIÓN CON RECONOCIMIENTO DE  
**ASIS INTERNACIONAL**



PRONTO CONOCERÁS NUESTRAS FECHAS DE  
INICIO PARA MODALIDAD PRESENCIAL  
Y EN LÍNEA

**¡APARTA TU LUGAR!**



55-4172-1132 / 55-1321-1289



Hamburgo 26, Juárez  
06600 CDMX



capacitacion@asis.org.mx  
formacion@asis.org.mx





## Aumenta 12 mdp gasto en **SEGURIDAD PRIVADA**

Por Javier Olmos

*Erogación en servicio de vigilancia en las oficinas estatales de la entidad pasa de 16 a 28 millones de pesos*

**D**e 16 a más de 28 millones de pesos incrementó en el último año el gasto que ha hecho el Gobierno del Estado para la contratación de servicios de seguridad privada para las diferentes oficinas ubicadas en la entidad.

Así lo muestra la Clasificación Partida Genérica por Dependencia de la Secretaría de Hacienda estatal al cierre del tercer trimestre del 2019, cuando reportó en este renglón denominado "servicios de vigilancia" erogaciones por 28 millones 117 mil 670 pesos.

En comparación, en el año 2018 el monto devengado fue de 16 millones 426 mil 997 pesos.

Esto surge a pesar de la drástica disminución de lo reportado al finalizar 2017, año en que la administración ejerció en este tipo de servicios 51 millones 296 mil 777 pesos, como lo indican los documentos oficiales.

Lo anterior significa que en estos tres años el monto de contratación por servicios de seguridad privada para edificios públicos alcanza los 98 millones 841 mil 444 pesos, según la suma.

El informe ubica a la Secretaría de Hacienda con la mayor parte del gasto en este rubro, con 10 millones 207 mil 711 pesos devengados al 30 de septiembre.

Uno de los últimos contratos asignados por esta dependencia a través de una adjudicación directa tuvo un costo de 261 mil pesos para servicios de vigilancia para los edificios Héroes de Reforma, Héroes de la Revolución y Plazas de Gobierno, con la asignación de seis elementos.

Hasta el 30 de septiembre, la Secretaría de Desarrollo Social había devengado 3 millones 22 mil 531 pesos; en tanto que la Secretaría de Cultura, que según documentos de Transparencia hace contrataciones de personal de seguridad privada para la realización de eventos, llevaba 4 millones 324 mil 313 pesos ejercidos.

También la Fiscalía General del Estado se encuentra en los niveles más altos de gasto por servicios de vigilancia con 4 millones 353 mil 803 pesos.

La FGE erogó este año, por citar algunos contratos, un monto de 545 mil 758 pesos para instalar elementos privados en algunas instituciones como el Centro Estatal de Información, Análisis y Estadística Criminal, en Babícora; en el departamento de Servicios Periciales y Ciencias Forenses, en la Dirección de Adquisiciones y Recursos Materiales, y diversos módulos de dependencias estatales en todo el estado. **ES**





*Protegerte, nuestro Compromiso*

Generamos ahorros importantes al adaptarnos a tus diversas locaciones, ya que contamos con protocolos que hacen efectiva nuestra adaptabilidad geográfica.



Nuestra capacidad de adaptación a las diferentes plazas y costumbres, hace posible entregar un servicio con la calidad que necesitas.

### **NUESTROS SERVICIOS**

Protección Ejecutiva • Seguridad Intramuros  
Custodia de Bienes • Seguridad Electrónica  
Geolocalización GPS • Monitoreo de Alarmas  
Videovigilancia • Administración de Riesgos  
Protección Perimetral

**Contamos con 32  
sucursales a  
nivel nacional a tu  
servicio**

[www.mspv.com.mx](http://www.mspv.com.mx)



**ASIS**

**AMEXSI**





# ASIS CAPÍTULO MÉXICO

## Última reunión mensual de 2019

*El pasado 3 de diciembre, ASIS Capítulo México llevó a cabo su última reunión mensual del año. Fue una reunión con una gran asistencia, sobre todo porque ese día se realizó la elección de la nueva planilla que formará parte del Consejo Directivo del Capítulo.*



Con 96 votos a favor, la planilla número 1, integrada por Miguel Ángel Champo del Valle, vicepresidente ejecutivo, Kael Malo-Juvera, vicepresidente de enlace, Midori Llanes, tesorera y Alberto Friedmann, secretario ejecutivo, fue la elegida.

En esta ocasión, Multiproseg fue la empresa patrocinadora del desayuno, y como siempre suele hacerlo, la empresa mostró una vez más su apoyo y total compromiso con la asociación y todos sus integrantes.

En el evento también se realizó un emotivo reconocimiento a Enrique Tapia, CPP, quien fungía como vicepresidente para México, Centroamérica y el Caribe de ASIS Internacional, y decidió cerrar este ciclo. Por más de 15 años, Enrique Tapia brindó todo su apoyo y experiencia a la organización, y su trabajo contribuyó a abrir espacios para los profesionales de la seguridad. Sin duda, un merecido reconocimiento.

También se reconoció el trabajo de cuatro expresidentes del Capítulo: Héctor Coronado, CPP (2017). Rubén Escoto, CPP (2006). Ricardo Torres, CPP (2005) y Jorge Septién, CPP (1999).

El conferencista invitado fue el Dr. Alfonso Ruiz Soto, que presentó su ponencia: Autoconocimiento, clave del éxito profesional.

El Dr. Ruiz Soto es fundador y director del Instituto de Semiología S.C., y creador de un nuevo modelo educativo sustentado en el desarrollo de la conciencia para elevar la calidad de vida de las personas: la Semiología de la Vida Cotidiana.

Desde 1985, año en que inició la impartición de sus postulados en distintos formatos: conferencias, cursos, diplomados, talleres y programas de radio y televisión; decenas de miles de alumnos se han visto beneficiados por esta revolucionaria propuesta educativa.

Y lo explica de esta forma: “el proyecto de vida sólo puede ser realizado de manera exitosa cuando los individuos logran tener armonía y plenitud del ser. Lo anterior es posible cuando los individuos logran un equilibrio entre los pilares fundamentales de la vida cotidiana: trabajo, familia, vida social y salud”.

“Nos capacitan en muchas cosas: aprendemos gramática, geografía, física, química y muchas cosas más, pero lo que nunca nos dieron fue una mirada interior, lo que nunca hicimos fue estudiarnos a nosotros mismos”.

“Por eso debemos aprender a identificar potencialidades físicas, emocionales y racionales. Lo anterior con el objetivo de aprender a ubicar los desbalances o limitaciones personales y con ello trabajar en ellas para alcanzar el bienestar”.

“A partir del conocimiento de las potencialidades es posible estructurar los horizontes vocacionales, y con ello encontrar las actividades profesionales que ayudarán a las personas a sentirse realizadas. La ausencia de este estudio personal provoca frustración en las personas”.<sup>15</sup>





**Consultoría de Servicios Jurídicos especializada en regulación de prestadores de servicios de Seguridad Privada, Tecnologías de la Información, así como de estrategia corporativa y administrativa.**

**Contamos con amplia experiencia en materias:**

- Corporativa
- Administrativa
- Protección de Datos Personales,
- Comercio Electrónico, Mercantil y Laboral.



Servicios profesionales jurídicos y administrativos de la más alta calidad



Firma de regulación jurídica con la mejor y alta calidad en la prestación de servicios jurídicos y administrativos



Nuestros servicios jurídicos se basan en el trabajo profesional y responsable

**[www.serralde.com](http://www.serralde.com)**

Ignacio Allende 283A, Colonia Clavería, Alcaldía Azcapotzalco, CDMX  
Teléfono (55) 70906639 (55) 70907385 | Correo teodoro@serraldeconsultores.com



# 35 AÑOS DESPUÉS, de la explosión de San Juan Ixhuatepec



En la pasada reunión mensual de AMEXSI, celebrada en noviembre, se presentó el panel de discusión "35 años después de la explosión de San Juan Ixhuatepec", conformado por el Capitán Piloto Aviador y Paramédico de Vuelo, Ricardo Martín Montoya Martínez; el Comandante del Heroico Cuerpo de Bomberos, Salvador Dávila Álvarez y el Capitán de Cobertura en Reserva, Aeromédico Naval, Mauricio Montaña Rodríguez; quienes desde su perspectiva hablaron sobre lo que vivieron en este trágico acontecimiento que quedó marcado en la memoria del país como la peor fuga de gas jamás registrada.

El 19 de septiembre de 1984, se vivió la trágica consecuencia de fallas en los sistemas de almacenamiento de gas en las gaseras ubicadas en la zona de San Juan Ixhuatepec, las cuales provocaron una serie de explosiones que devastaron al pueblo mejor conocido como San Juanico, en Tlalnepantla, Estado de México y que dejaron 498 muertos y cuatro mil 248 heridos, según cifras oficiales. Ni gobierno o población estaban preparados para una tragedia de esa magnitud ya que no existía Protección Civil, ni había cuerpo de bomberos en la zona. Un día antes, 18 de noviembre, se registró una fuga de gas en la estación de almacenamiento de Petróleos Mexicanos y la explosión que sobrevino al día siguiente, a las 5:35 horas, despertó a toda la capital del país ya que el gas a presión provocó que las llamas se elevaran hasta unos 600 metros de altura (más de 2 veces la altura de la Torre Mayor) y que cientos de personas prácticamente quedaran desintegradas por el calor de las llamas y el impacto de la onda expansiva.

El Capitán Ricardo Montoya, recuerda su primera impresión, se trataba de momentos difíciles que se borraron rápidamente para poder cumplir con su deber y que lo marcaron para siempre pues en ese momento se encontraba en escuela de socorristas y fue la primera emergencia real que atendía, recuerda que los camiones del ejército se transformaron en ambulancias e incluso se transportaron personas heridas en metro y que por ser asentamientos irregulares muchos no pudieron ser identificadas.

La respuesta de la sociedad nuevamente se vio en este acontecimiento, recuerdan los ponentes, y fue fundamental para la ayuda y rescate pues el accidente rebasó la infraestructura y la capacidad de respuesta de las agrupaciones existentes hasta ese momento. "Protección civil en México debutó en esta emergencia, no existían conocimientos médicos previos para una ayuda de calidad en trauma" mencionaron, por lo cual un punto crucial en la actualidad es la capacitación; que si bien la capacidad de improvisación de México es reconocida se necesita mucho más que eso: capacitación, entrenamiento y recursos son fundamentales para salvaguardar la seguridad.

El Comandante, Salvador Dávila recuerda que en aquel momento sólo se tenían 24 ambulancias para atender a los lesionados y los tres ponentes concuerdan en que hablar de números oficiales, no se puede ya que se rebasan los datos por las autoridades pues no hay manera de cuantificar verdaderamente a las víctimas y no existe un padrón oficial ya que fueron más de 4 hectáreas las afectadas y se evacuaron a más de 60,000 personas.

Desde su experiencia los ponentes concordaron que no se contaba con la atención necesaria y que fueron rebasados en esta situación, recuerdan el miedo vivido que después se volvió consternación, jamás olvidarán el calor abrazador que se sentían y que ante todo esto lo que siempre los impulsó a sobreponerse y continuar fue el espíritu de servicio. **XS**





**CORPORATIVO**



su **seguridad** tranquilidad **y** satisfacción



### **NUESTROS SERVICIOS**

- > GUARDIAS INTRAMUROS
- > PROTECCIÓN A EJECUTIVOS
- > CUSTODIA DE TRANSPORTES
- > SEGURIDAD EN EVENTOS
- > ESTUDIOS DE SEGURIDAD
- > CENTRAL DE MONITOREO PROPIA

### **SEGURIDAD ELECTRÓNICA**

- > CCTV
- > ALARMAS
- > CONTROL DE ACCESOS
- > PROTECCIÓN PERIMETRAL
- > SISTEMAS CONTRA INCENDIOS
- > LOCALIZACIÓN SATELITAL GPS/GPRS

**Servicios de calidad  
en forma continua y  
permanente**

**Comprometidos con  
nuestros clientes en obtener  
su total satisfacción**

**Empresa conformada  
por profesionales con  
amplia experiencia**

Tels: (55) 55-32-48-30, (55) 56-72-86-92 y (55) 24-55-59-15 Y 16  
Miguel Laurent 1695 Col. Letrán Valle, Alcaldía Benito Juárez, C.P. 03650, Ciudad de México  
seguridad@zncorporativo.com | direccion@zncorporativo.com

**[www.zncorporativo.com](http://www.zncorporativo.com)**





## TOP SECURE, Seguridad Privada

*Benjamín Santos Jiménez, Director General de Top Secure, habló con Xtrem Secure sobre puntos específicos que se deben de tomar en cuenta como empresa de seguridad privada y empresa de retail.*

Desde su punto de vista el retail requiere cierta especialización a fin de poner atención en aspectos como las jornadas, la productividad, el entrenamiento de los guardias, la convivencia en el piso de ventas y el modelo de seguridad diseñado para cada cliente, principalmente y reconoce que las empresas minoristas por la sensibilidad que tienen al retail son las que sufren y recientes más el incremento de la delincuencia.

Existe otra cara de la moneda para las empresas de retail pues se tiende a ver a la seguridad privada como un mal necesario, pero no es así, dijo Santos Jiménez, ya que el monto del gasto que ocupa el primer lugar en las empresas de retail es el capital humano, personas que dan seguridad, es decir la seguridad privada. "Tener la óptica de que la seguridad privada es un mal necesario hace que se caiga en errores desde proveedores hasta clientes por lo cual los profesionales de la seguridad debemos ponernos de acuerdo para darle la vuelta a esta percepción con profesionalismo" dijo, sin embargo reconoce que el lado oscuro del gremio son las empresas no reguladas.

El aspecto legal, una buena gestión del capital humano, cultura organizacional actual y funcional deben de ser puntos a analizar antes de contratar a una empresa de seguridad, así como otros detalles como la integración de tecnología en los esquemas que se ofrecen, las buenas prácticas y las historias de éxito. Top Secure es una empresa joven con apenas tres años en el mercado, pero con un inicio a lo grande ya que su meta siempre fue nacer grande, afirma el entrevistado, ya que buscan ser una oferta irresistible para sus clientes.

En cuanto a su historia personal Benjamín Santos Jiménez, igual que otros, inició como guardia de seguridad y al combinar estudio y trabajo llegó a mirar esta profesión como

su pasión y su camino; misma que disfruta por lo que quiere que lo vean como un punto de cambio para aquellos que inician en esta carrera "la cual no tiene un límite si se combina la educación académica y la preparación". Y en su opinión el principal error de las empresas de seguridad, como en otros ramos, es el no dar el valor a la gente, ya que el éxito de una empresa de seguridad sólo puede darse si hay éxito en sus colaboradores. Por esta mentalidad la empresa invierte tiempo, recursos y esfuerzo para perfilar a sus colaboradores y distinguir qué habilidades y aptitudes poseen y qué formación requieren para poder empatar y hacer una carrera a futuro en Top Secure, una empresa que ofrece soluciones, valor y que continuará creciendo en el mercado de la seguridad a nivel nacional y mundial, comentó. **XS**





# A SUME

Agrupaciones de Seguridad Unidas por México

## PRINCIPALES OBJETIVOS

Fortalecer al sector en la cúpula empresarial.

Impulsar la Ley General de Seguridad Privada y la Cámara de la Industria.

Participación destacada de la seguridad en proyectos de desarrollo económico y social.



[asumeseguridad.org](http://asumeseguridad.org)







## ARMAS NO LETALES, el futuro para la seguridad privada y pública

*ABASTECEDOR PRINCIPAL NACIONAL, S.A. DE C.V., llamada "APRINSA" por sus siglas, nace en el año del 2003, su misión es proveer soluciones para mantener la vida, preservando la Paz social a toda costa, donde sus soluciones inmediatas sean una opción a las armas de fuego como último recurso. Nuestra empresa con más de 15 años de experiencia en suministrar, distribuir y proveer tecnologías no letales marca "APRINSA" en el mercado nacional, demuestra la inocuidad, profesionalidad, seguridad en la aplicación de dichos dispositivos de acuerdo al uso de la fuerza.*

**E**ntrevistamos a una de las principales empresas en México acerca de las Armas no letales, su director General Ing. Antonio Trewick, nos habla a continuación de ello:

Las Armas no letales son de uso defensivo, son dispositivos que proveen una reducción en las lesiones y muertes, preservando en mayor medida la vida.

**XS.-** ¿Cuál es la regulación legal en México al respecto?

**Antonio Trewick.-** En México está regulado por el uso de la fuerza, de acuerdo a la aplicación de los protocolos de uso. Dichos Protocolos son de acuerdo a nuestro mercado cultural.

**XS.-** ¿Serán las armas no letales el presente y futuro en nuestra sociedad?

**Antonio Trewick.-** Creemos que la mejor arma a futuro se compone de dos elementos fundamentales, la paz y la seguridad. Dichos elementos proveerán una excelente calidad humana, garantizando la preservación de la vida en todo momento, es cuando así se vencerá toda oposición.

Por ello enunciamos "Con la paz y seguridad no es necesario tener que pelear", las tecnologías no letales proveerán el respaldo para que esto suceda en el presente y futuro.

**XS.-** ¿Dicen que el Weapons effect es un fenómeno descrito y evidenciado por el campo científico del comportamiento social, y se refiere a que la sola presencia de un arma o una imagen de un arma producirá un fenómeno agresivo en humanos, que puede decir al respecto en la aplicación de tecnología no letal APRINSA?

**Antonio Trewick.-** El Efecto Weapons Effect se refiere en particular en situaciones donde los humanos han sido previamente provocados y tienden a proveer una respuesta agresiva. Así mismo imagínense que aplicara cuando la gente ve a los policías armados en las plazas comerciales, centros, clubes ... esto provocaría agresividad en las personas y reducción en las ventas. Hemos encontrado que en el uso de Tecnologías de No Letales APRINSA se reducen las agresiones tanto a los elementos de seguridad como a los detenidos, porque las personas se vuelven muy cooperativas y en ocasiones no es necesario utilizarlas. (Gráfica 1)

**TECNOLOGÍA NO LETAL  
PROVEE PAZ Y SEGURIDAD...  
PORQUE LO MEREZCO Y LO VALGO!!!**

**PISTOLA  
ELÉCTRICA**



Pistola Eléctrica de Alto Voltaje a Bajo Amperaje. Ideal para Seguridad. Tiene un alcance de 7 metros.



Expulsa Irritante hasta 4 metros de distancia. Ideal Protección.



JPX Expulsa Irritante a 7 metros. Ideal Seguridad. Hasta 2 aplicaciones.



JPX4 Expulsa Irritante a 7 metros. Ideal Seguridad. Hasta 4 Aplicaciones.

**LANZADOR  
38 MM**



Lanzador de 38 mm, Sistema control de Motines. Capacidad de 6 tiros.

**PISTOLA MOD. VALENTINA**



Lanza Municiones de Talco, Goma, Sal, Olearesin Capsicum, y Eléctricas. Con Alcance 50 metros. Ideal Control Disturbios.

**PISTOLA MOD. TIGER**



Ideal para Control de Disturbios y entrenamientos. Expulsa bolas de Goma, Talco, Sal. Distancia de Hasta 30 metros.

**BASTON  
ELÉCTRICO**



Ideal para cuerpos de Seguridad, Descargas de alto voltaje a bajo amperaje.

**RONIN**



Carcasa para brindar mayor estabilidad y precisión. Diferentes modelos y colores.



Lanzador Calibre 37 mm , accionado. Rango Efectivo 150 metros. Medidas 54cm x 18cm x 6 cm ancho.

**PISTOLA**



**COMMANDO**

Pistola ideal para entrenamiento. Expulsa bolas de entrenamiento(talco).

**PISTOLA MOD.  
M16**



Pistola tipo rifle para entrenamiento. Expulsa bolas de entrenamiento (talco, pintura).



Municiones para Lanzador., Azul : Impacto Directo  
Azul Fuerte : Sonido  
Rojo : Impacto OC  
Amarillo : nube OC

En "Los principios básicos sobre el uso de la fuerza y armas de fuego por los agentes responsables por la aplicación de la ley" , aprobados el 7 de Septiembre de 1990, la ONU recomienda la adopción de armas no letales en las acciones de seguridad pública, esperando reducir al mínimo el uso de medios que provoquen lesiones permanentes o muerte.



SOLICITE SU COTIZACIÓN  
VIA EMAIL  
[ventas@aprinosa.net](mailto:ventas@aprinosa.net)  
SU PRINCIPAL SEGURIDAD

**APRINSA**  
[www.aprinosa.net](http://www.aprinosa.net)  
MARCA MEXICANA



## ESTADÍSTICAS EN EL USO DE TECNOLOGÍA MENOS LESIVA



Gráfica 1

**XS.-** ¿Debemos dotar únicamente de armas de fuego a los policías?

**Antonio Trewick.-** Una persona goza del principio de inocencia hasta que no sea juzgado. El llevar armas de fuego a un evento incrementará el resultado funesto. El pensar de manera violenta proveerá resultados violentos y por ende un uso excesivo de la fuerza, un proceso administrativo y vergüenza para los elementos que participarán. Por ello huyen a los encuentros violentos y pregunto ¿Quién quiere morir?

**XS.-** ¿Los policías accionan sus armas seguído?

**Antonio Trewick.-** El traer un arma de fuego es un elemento de respuesta para situaciones violentas, en nuestro país el 99% de los policías no tienen enfrentamientos diarios con terroristas, delincuentes armados, matones, sicarios, las armas no letales APRINSA proveen una solución para las situaciones en dónde no va su vida de por medio.

**XS.-** ¿Se cuenta con algún respaldo de estadísticas en el uso de tecnologías no letales?

**Antonio Trewick .-** Sí, a continuación las menciono:

- **Lesiones a oficiales bajaron 96%**

Antes 60 lesiones por año

Después 2 lesiones por año

Fuente: Policía de la ciudad de Kloten-Suiza

- **Lesiones a sospechosos bajaron 77%**

Periodo de prueba 6 meses

Fuente: Policia de la ciudad de Kloten-Suiza

- **Quejas de Ciudadanos bajaron 60%**

Periodo de prueba 2 años

Fuente: Policia de la ciudad de Kloten-Suiza

- **Uso de fuerza Letal bajo 78%**

Antes 18 disparos en 24 meses

Después 4 disparos en 24 meses

Fuente: Condado de Orange

- **Ahorro en pago de reparaciones de daños 2.5 MDD**

Incidentes evitados 3 en el periodo de 1 año

Fuente: L.A.

**XS.-** ¿Se reducirán los incidentes contra civiles?

**Antonio Trewick.-** Correcto, ya que son equipos de precisión.

**XS.-** ¿Cuándo se aplica la tecnología menos lesiva es más sencillo el proceso?

**Antonio Trewick.-** Sí, el proceso se simplifica, se utilizan protocolos de actuación en donde el elemento de seguridad pública o privada llenara su informe detallando su procedimiento, respaldando su actuar de acuerdo al uso de la fuerza, sin que se enfrente un juicio.

**XS.-** ¿Dónde pueden utilizar la tecnología no letal?

**Antonio Trewick.-** En lugares de concentración masiva, barrios, bancos, estadios, centros comerciales, patrullajes, unidades deportivas, parques, zonas turísticas, centros de negocios, exposiciones, alcaldías, etcétera, es ideal para fortalecer el equipo policiaco.

**XS.-** ¿Funcionan?

**Antonio Trewick.-** ¿Cuándo deseas ser nuestro voluntario?

**XS.-** ¿Qué países utilizan la tecnología letal menos lesiva?

**Antonio Trewick.-** Estos son solo algunos países que la utilizan: Algeria, Tunes, Marruecos, Libia, Argentina, Australia, Austria, Bosnia, Bulgaria, Camerún, China, Colombia, Costa Rica, Croacia, Republica Checa, Ecuador, Egipto, El Salvador, Etiopia, Francia, Alemania, Guatemala, Hon Kong, India, Indonesia, Irlanda, Israel, Italia, Japón, Kenia, Korea, Madagascar, Malta, México, Mongolia, Noruega, Qatar, Pakistan, Panamá, Polonia, Puerto Rico, Rumania, Arabia Saudita, Serbia, Singapur, Estados Unidos. Instituciones de Seguridad, Seguridad Privada, Seguridad Pública, empresarios entre otros.

**XS.-** ¿Puedes dar razones porque sí a las Armas no letales APRINSA?

- Proveen la oportunidad al elemento de seguridad de arrestar al sujeto con el menor daño posible.
- Son una alternativa ideal para la protección personal de las personas.
- Ayudan al elemento de seguridad para actuar siguiendo los principios del uso de la fuerza.
- Reducen la violencia y la agresión física.
- Son menos lesivas y evitan daños permanentes en el sujeto al que son aplicadas.
- Son altamente efectivas en su aplicación respetando en todo momento sus derechos humanos.
- Son ideales para el control en manifestaciones.
- Si se usan de manera correcta son seguras y efectivas.
- Son para utilizarse de manera defensiva y para tenerlas como alternativa de respaldo.
- Son un complemento a la fuerza letal.

**XS.-** ¿Cuál es la posición de la ONU respecto a esta tecnología?



**Antonio Trewick.**-La ONU en "Principios básicos sobre el uso de la fuerza y armas de fuego por los agentes responsables por la aplicación de la ley" aprobados el 7 de septiembre de 1990 recomendó la adopción de armas no letales en la acciones de seguridad pública, esperando reducir al mínimo el uso de medios que provoquen lesiones permanentes o muertes, ósea el uso de armas de fuego queda restringido a las situaciones en las que los medios no letales se muestran insuficientes para neutralizar al infractor de la Ley o para defensa propia.

**XS.**- ¿Es cara esta tecnología, de ser así podría abarataarse?

**Antonio Trewick.**- La tecnología es económica, además de si lo comparas con el arma de fuego.

**XS.**- ¿Algo más que desee agregar?

**Antonio Trewick.**- Se ha encontrado que el 99% de las ocasiones es por desconocimiento de las BONDADES Y BENEFICIOS DEL USO DE TECNOLOGIA NO LETAL APRINSA, décadas de usar armas de fuego y la violencia se incrementa, evitemos muertes innecesarias, el futuro de la seguridad privada y pública está en las armas no letales, quien preste servicios con tecnología APRINSA puede vender sus servicios MAS COMPETITIVAMENTE, Y MEJOR RENUMERADOS. **XS**

Nuestros datos de contacto:  
ABASTECEDOR PRINCIPAL NACIONAL, S.A. de C.V.  
Tel: 333 641 2350  
Whatsapp: 333 700 7721  
[www.aprinosa.net](http://www.aprinosa.net)





# MEJORES PRÁCTICAS DE SEGURIDAD en la Cadena de Suministro



El pasado 29, 30 y 31 de octubre se llevó a cabo en la Ciudad de México el Simposio de Seguridad 2019 de ANTAD, siendo uno de los ponentes principales Dagoberto Santiago, Director Sr. de Seguridad Corporativa, con la ponencia "Mejores prácticas de Seguridad en la Cadena de Suministro" habló del papel crucial de la seguridad en este rubro ya que es indispensable contar con protocolos, políticas, procedimientos y bases de

seguridad fuertemente arraigados tanto en personal como proveedores, a fin de no sólo reducir pérdidas, sino también desarrollar empresas confiables y mejor calificadas, lo que representa una ventaja competitiva en el mercado.

Para PepsiCo, la seguridad de sus asociados es la prioridad número "Entrenar, capacitar y certificar a todos los empleados de la compañía para así fortalecer y preservar la seguridad del empleado ante alguna situación delictiva o de riesgo, es de vital importancia para nosotros", comentó Santiago durante su participación y asegura que la prevención es la herramienta más efectiva contra la delincuencia así como la autoprotección personal para mantenerse lo más ileso posible ante una situación de conflicto.

Con más de 25 años de experiencia en la gestión y desarrollo de programas estratégicos de seguridad; además de ser miembro del Consejo Directivo de OSAC, organización responsable de la promoción de la seguridad, Dagoberto Santiago, reconoce que para poder llevar a cabo una cultura de autoprotección se requiere de materiales, una estrategia de difusión, campañas ya sean electrónicas o digitales y otras herramientas como pláticas constantes con el personal a fin de que se tome conciencia y se reconozcan las situaciones de riesgo y la respuesta ante éstas, siendo el no oponer resistencia una solución.

Para PEPSICO, otro de los pilares importantes es el tema de la inteligencia en los puntos de reparto, por lo cual diseñan un análisis de riesgo y de entorno apoyados por estadísticas para así formar cuadros de decisiones donde se requiere más el localizar y reconocer el modus operandi de la delincuencia a fin de generar nuevas estrategias como el establecimiento de rutas de reparto y mantener siempre contacto con los centros de control, sin dejar de lado la importancia de mantener acercamientos con los tres niveles de seguridad: pública, municipal y federal. ■



**PROBABLEMENTE**

TE HAS PREGUNTADO CUÁL ES

**LA MEJOR EMPRESA**

DEL SECTOR



**GRUPO IPS**

GARANTÍA EN SEGURIDAD

| MÉXICO • PERÚ |

Síguenos



Tel. (55)55 25 3242

[grupoipsmexico.com](http://grupoipsmexico.com)







# AMEXSI celebra cena de fin de año

*AMEXSI, Asociación Mexicana de Especialistas en Seguridad Integral, A.C. celebró el fin de año con una cena para todos sus integrantes en el Hotel del Ejército y Fuerza Aérea Mexicanos el día 6 de diciembre de 2019. Durante la cena hubo varios reconocimientos para los asociados y mesa directiva, el encargado de entregar los reconocimientos fue su presidente el Ing. Arturo Martínez Avalos, CPP, PCI, DSI quién deseo a todos un año 2020 lleno de éxitos profesionales y personales.*



Lic. Rubén Fajardo Correa, Director de SIPROSI



Lic. Jorge Romo, Director general Grupo LK

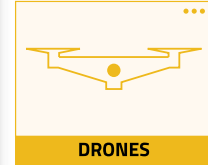


Ing. Arturo Martínez Avalos

# EXP<sup>®</sup> SEGURIDAD MÉXICO

**21-23 | Abril**  
**2020** Ciudad de México  
Centro Citibanamex

La mayor exhibición de  
productos y soluciones  
de seguridad en América Latina



## ¡Te esperamos!

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

Patrocinadores Fundadores



Patrocinadores Corporativos



Aliados Estratégicos



Powered by



Organizado por



En conjunto con



El logotipo de Expo Seguridad México es una marca registrada de Reed Exhibitions Mexico SA de CV.





# LA BIBLIOTECA DEL SENSEI

*Como siempre, damos la bienvenida a la gustada sección del maestro, del Sensei, que ya nos tiene acostumbrados a sus recomendaciones de lecturas de gran utilidad. Veamos.*

*En esta ocasión queremos aprovechar este inicio de año para compartir dos textos de gran utilidad para los ciudadanos de cualquier parte del mundo. El primero de ellos se llama *Sálvese... ¡Usted sí puede!*, escrito por María Eugenia Valles Septién, una de las primeras mexicanas, que en el 2001, se hizo CPP.*



**E**l primero de ellos se llama *Sálvese... ¡Usted sí puede!*, escrito por María Eugenia Valles Septién, una de las primeras mexicanas, que en el 2001, se hizo CPP.

En este libro, de muy fácil lectura, la autora hace grandes reflexiones sobre cosas fundamentales, pero que desde 1995, el año en que ella comenzó a escribir este texto, siguen siendo totalmente válidas y útiles.

En este pequeño libro, de apenas 112 páginas, casi de bolsillo, la autora divide su planteamiento de seguridad en seis grandes apartados. El primero, al que denomina "Mantenga su hogar seguro" nos da exactamente algunos pasos y consejos prácticos para la casa. Después nos habla de la seguridad en la calle, de cómo ser precavidos al salir a la calle, tener cuidado en los estacionamientos, precauciones para cuando uno va a abordar el automóvil, etcétera.

Un tercer tema que aborda es la seguridad en el vehículo y nos habla de distintas situaciones y respuestas que debemos tener preconcebidas. También se refiere a la convivencia que tenemos en nuestros ratos de esparcimiento en un capítulo que se llama "Sea precavido en su tiempo libre".

Posteriormente nos habla de la seguridad que debemos tener en nuestro centro de trabajo, habla de las precauciones que debemos tener para prevenir posibles ataques o actos delictivos. Finalmente cierra con un tema que se vuelve muy importante, sobre todo en estas fechas de fin de año, que son las precauciones al hacer sus compras en los centros comerciales.

Este es un libro para toda la familia que todos deberíamos leer y comentar con nuestros seres queridos. Muchos de ustedes conocen el Manual de Seguridad de David Lee, sin embargo este libro, que fue escrito 10 ó 12 años antes, trae las bases todavía más simples, más sencillas y más prácticas, va muy enfocado a la parte familiar, al hogar y al bienestar de las personas.

Consideramos que este es un libro que no puede faltar y es un buen regalo en este inicio de año.

**E**l segundo libro se llama *Manteniendo a los niños sanos y salvos*, consejos fáciles para defenderlos del delito. Este libro es una recopilación de textos de varios autores editado a finales del siglo pasado, principios del 2000, en donde se trata de proteger lo más valioso que tenemos: nuestra niñez, nuestra juventud.

Los niños y los jóvenes son una población desvalida en casos de riesgos delictivos por su propia condición de fragilidad. En este libro los autores nos hablan de la reflexión de cómo proporcionar a nuestros hijos la capacitación que se requiere para sobrevivir adecuadamente en esta era de delito.

Habla de cómo están en peligro nuestros hijos en las escuelas, en los parques, en los centros comerciales. Toca temas como las pandillas, los traficantes, los ladrones, los abusadores, y todo enfocado a qué hacer para tratar de prevenir y preparar a nuestros hijos para que eviten ser víctimas del delito.

En una fácil lectura, habla de cómo comienza la seguridad en casa, cómo debemos enseñar a nuestros hijos algunos principios y fundamentos de la seguridad, cómo involucrarlos en los programas que han sido más exitosos sobre la seguridad residencial, que son los de seguridad vecinal.

Nos dice: nunca asuma cosas, porque el asumir que no hay peligro es el primer paso para padecerlo. Qué hacer cuando los hijos están solos en el hogar, cuando se van de fiesta. O al ir de compras o de viaje. Cómo a veces, cuando salimos de nuestra rutina, olvidamos lo que es la seguridad.

Este libro resulta fundamental para todos los padres de familia en sociedades como las que vivimos en América Latina, en donde las cosas ya no son como eran cuando nosotros fuimos jóvenes o niños, cuando todavía a las 8 ó 9 de la noche podíamos estar en la calle jugando con nuestros amigos y no había problema. **XS**





# SEGURIDAD PUBLICA



REVISTA DIGITAL  
ESPECIALIZADA EN SEGURIDAD PÚBLICA

[www.seguridadpublica.mx](http://www.seguridadpublica.mx)





*El Consejo Coordinador Empresarial (CCE) informó que ya existe una propuesta de reforma constitucional para que la seguridad privada trabaje con el gobierno federal y contrarrestar la problemática que existe.*

## SEGURIDAD PRIVADA APOYARÁ A GOBIERNO FEDERAL contra la delincuencia: CCE


El titular del organismo Carlos Salazar Lomelín, indicó que uno de los objetivos principales a trabajar, es proponer a la autoridad temas de seguridad, ya que hay lugares del país donde la empresa privada ya trabaja con la sociedad civil y ha tenido buenos resultados. "Hacia años que no se encontraba una manera de hacer una reforma legal para que todo el tema de seguridad privada tuviera una orientación a nivel nacional, creo que ya



lo logramos. Tenemos un consenso de todo el clausulado que se va a presentar como reforma constitucional, para que el estado también tenga posibilidad de sumar a su estrategia más de medio millón de efectivos", comentó.

Salazar Lomelín indicó que éste trabajo en conjunto ya se aplica en diferentes entidades, "tenemos ejemplos muy buenos como en Chihuahua, Tijuana y Monterrey, donde la sociedad civil unida con su autoridad local, han encontrado fórmulas para poder proteger a su ciudadanía, tener mejores policías y obviamente la criminalidad ha disminuido total y absolutamente".

Expuso que esta mancuerna es de vital relevancia, "imagínense la importancia y que no lo estábamos aprovechando, nos quejamos de que no tenemos suficientes policías en las calles, por el lado privado hay medio millón de policías, y no están orientados a una estrategia, una coordinación una fórmula, pues yo creo que es una magnífica noticia".

El dirigente empresarial señaló que los efectivos, serían 100 por ciento privados y que al ser así, no le costaría al gobierno, "de acuerdo a las reglas que nos ponga la autoridad en este caso la Secretaría de Seguridad, tendrán que capacitar a las empresas privadas a sus propios elementos". En días pasados el coordinador general de Agrupaciones de Seguridad Unidas, por un México Estable (ASUME), Armando Zuñiga Salinas, dijo que con más de 600 mil elementos distribuidos en 8 mil empresas en todo el país, la seguridad privada puede coadyuvar a pacificar a México. 



## ANUNCIARÁN NUEVAS PROPUESTAS DE MEJORA A LA SEGURIDAD PÚBLICA en la próxima Expo Seguridad México 2020

Ciudad de México.- Expo Seguridad México y Expo Seguridad Industrial, los eventos de seguridad referentes en América Latina que reúnen a compradores calificados con expositores para presentar lo último en productos y soluciones de la industria, anunciaron la celebración de la X Conferencia Internacional para la Administración de la Seguridad y Fuerzas del Orden (CIASFO), cuyo fin es difundir temas especializados y contribuir a la actualización de funcionarios de los tres niveles de gobierno.

En el décimo aniversario de su fundación, la CIAFO presentará en la próxima Expo Seguridad México un programa de conferencias magistrales impartidas por expertos, provenientes de la academia, del sector empresarial y el oficial. De acuerdo con Jorge Hagg, director general del evento, “actualmente estamos preparando la versión final del plan de actividades y pláticas especializadas que se impartirán del 21 al 23 de abril de 2020 en el Centro Citibanamex”.

A manera de antecedente, cabe destacar que en ediciones anteriores la CIASFO ha contado con la participación de profesionales de la seguridad pública de clase mundial; tal es el caso de ponentes nacionales como Ciro Humberto Ortiz Estrada, jefe de la División Científica de la Policía Federal; Renato Sales Heredia, coordinador nacional Antisecuestros y Comisionado Nacional de Seguridad; Esteban Islas Badillo, titular de la Unidad de Planeación, Perspectiva y Seguridad Privada; y Eunice Rendón, subsecretaria de Prevención del Delito y Participación Ciudadana de la Secretaría de Gobernación.

### *Cumple su 10º aniversario la Conferencia Internacional para la Administración de la Seguridad y Fuerzas del Orden*

Dicho foro, también ha contado con la presencia de especialistas internacionales como Ricardo A. Salas, representante del Departamento de Seguridad de las Naciones Unidas; y Daniel Lisnkey, ex Jefe de la Policía de Boston. “Para la próxima edición continuaremos bajo esa línea, ya que contaremos con profesionales nacionales y extranjeros, tanto del sector público como del privado, que se han desempeñado en el ámbito de la seguridad pública en nuestro país y otras partes, por lo que su experiencia enriquecerá nuestro programa”, declaró Hagg.

La Conferencia Internacional ha tenido la presencia de mujeres destacadas en la industria, como fueron los casos de Patricia Rosa Linda Trujillo Mariel, titular de la División Científica de la Policía Federal; Teresa Incháustegui Romero, directora general de INMUJERES; Jessica Duque Romero, especialista en Seguridad Pública; María Teresa Torres Aguilar, especialista en Seguridad Humana; Maribel Cervantes Guerrero, secretaria de Seguridad Pública del Estado de México; y Patricia Bugarin Gutiérrez, coordinadora nacional Antisecuestro, SEGOB.

“Nuestro interés va más allá de ser incluyentes, sino de buscar la participación de especialistas de alto nivel en el tema de la seguridad, y es lo que ofreceremos en nuestra próxima edición”, finalizó Jorge Hagg, director del evento. **MS**



## DETIENE EE.UU. A GENARO GARCÍA LUNA por vínculos con el Cartel de Sinaloa

Estados Unidos anunció la detención del exsecretario de Seguridad Pública mexicano Genaro García Luna, quien enfrenta cargos relacionados con el tráfico de drogas entre 2006 y 2012.

El alto funcionario del gobierno del presidente Felipe Calderón enfrenta "tres cargos por conspirar para traficar cocaína y un cargo por hacer declaraciones falsas", informó el Departamento de Justicia de EE.UU. en un comunicado.

"García Luna es acusado de tomar millones de dólares en sobornos del Cartel de Sinaloa de 'El Chapo' Guzmán mientras controlaba la Policía Federal mexicana y era responsable de asegurar la seguridad pública de México", dijo Richard P. Donoghue, fiscal federal del Distrito Este de Nueva York.



Durante el juicio a "El Chapo", testigos declararon que García Luna estaba entre los presidentes y altos funcionarios que recibieron sobornos por parte del Cartel de Sinaloa. Los señalados, incluido García Luna, rechazaron las acusaciones.

"El Rey" Zambada: el testigo en el juicio a "El Chapo" Guzmán que involucró en millonarios sobornos a ex altos funcionarios de seguridad de México.

"El arresto muestra nuestra determinación de traer ante la justicia a aquellos que ayudan a los carteles a infligir un daño devastador a Estados Unidos y México, sin importar las posiciones que ocuparan mientras cometían sus crímenes", añadió.

## Celebra SSPC ley 'ANTIJAMMER'



La Secretaría de Seguridad y Protección Ciudadana celebró la aprobación en el Congreso de la llamada "ley antijammer", la cual regula equipos bloqueadores de señal utilizados por grupos criminales para el robo de transporte de carga.

Para la dependencia, las reformas a la Ley Federal de Telecomunicaciones y al Código Penal Federal, en materia de bloqueo de señales de telecomunicación (jammers), fortalecen la capacidad del Gobierno federal para combatir ese delito a través del Plan Carretera Segura.

"Quisiera expresar el reconocimiento de la Secretaría, diputados y senadores, por la aprobación de la ley antijammer, esta fue una iniciativa que trabajamos con el sector privado, sumamente sensible", dijo Alfonso Durazo.

"Es un aparato pequeño que inhibe la señal y que imposibilita que una gente que ha sido agredida criminalmente, pueda tener comunicación para denunciar el hecho".



# ORIGINS PRIVATE SECURITY S.A. DE C.V.



**SEGURIDAD**



**PREVENCIÓN**



**CONFIANZA**

Marsella No. 60, Int. 103,  
Colonia Juárez, Alcaldía Cuauhtémoc,  
Ciudad de México, C.P. 06600

Telefónos:

**5207 6828 / 3603 3189**





## MÉXICO TIENE UN NUEVO "ORO"

Puede ser la clave para los carros del futuro  
Extranjeros lo buscan en la montaña

*En las montañas del noreste de Sonora, en México, se encuentra escondido un "oro blanco", cada vez más requerido en varias industrias: el litio.*

Este elemento químico es utilizado comúnmente para fabricar las baterías de los celulares, pero no solo: también se considera clave para almacenar la energía necesaria en los carros eléctricos, que se espera harán cada vez más irrupción en el sector del transporte. Así mismo, se usa como tratamiento para problemas como la depresión o para mejorar materiales como el aluminio.

Una empresa canadiense, Bacanora, y otra china, Ganfeng, desarrollan proyectos para explotar el yacimiento de Sonora, ubicado en el área del municipio de Bacadéhuachi. Para el sitio especializado Mining Technology, si se confirma la cantidad de litio prevista, sería el más grande del mundo, con 243.8 millones de toneladas de este elemento, que asume el aspecto de un polvo blanco cuando se extrae como carbonato de litio (de ahí que se suele definir "oro blanco").

Gracias a esta reserva, que se suma a otras en fase de estudio situadas en Baja California, San Luis Potosí y Zacatecas, México tiene potencial para convertirse en un productor de primera plana de este valioso material, indican varios reportes. Algo que interesó, por ejemplo, también a la empresa estadounidense, Tesla, que apuesta fuerte por el desarrollo de autos eléctricos: en 2015 firmó un acuerdo para que las empresas que explotan este recurso se lo proporcionen para fabricar baterías útiles para sus carros, según reportes de aquel año.

Entre los que están convencidos de la oportunidad de aprovechar este material están algunos representantes de las instituciones mexicanas. "El litio se va a convertir en el nuevo petróleo", dijo en una rueda de prensa el secretario mexicano de Medio Ambiente, Víctor Toledo.

La secretaria de Energía, Rocío Nahle, tuiteó que "existen varios proyectos de investigación muy avanzados sobre el uso del litio para el desarrollo de baterías y otros temas como el de salud".

Mining Technology explica que la explotación del yacimiento de Sonora será una operación a cielo abierto que se propone desarrollar en dos etapas de creciente aprovechamiento, la primera con una capacidad de producción de 17,500 toneladas por año (tpa) de carbonato de litio. La segunda etapa duplicará la capacidad de producción a 35,000 tpa.

Jorge Vidal, secretario de economía de Sonora, explicó además, según declaraciones recogidas por Forbes México, que la empresa china Ganfeng tiene "más de siete mil empleados" y está interesada "en venir en enero, vienen en una misión comercial a Sonora, porque ellos tienen interés de estar aquí viendo la posibilidad de instalarse para poner una fábrica de baterías".

Pese al optimismo, no todo va a ser fácil. El Subsecretario de Minería de la Secretaría de Economía, Francisco José Quiroga, ha llamado a la calma respecto al yacimiento de Sonora afirmando a Aristegui Noticias que "no hay que echar las campanas al vuelo, porque todavía hay que sacarlo y dominar la parte metalúrgica, separar el litio de los otros minerales que tiene".

El funcionario agregó que el litio ubicado en Sonora está en forma de roca, lo que dificultaría su extracción y separación de otros minerales, a diferencia de explotaciones en Bolivia, Chile y Argentina (países entre los principales productores mundiales), donde está en estado líquido.

Otro aspecto para monitorear es si estas explotaciones prometedoras pueden tener impactos negativos para el entorno en el que se van a llevar a cabo, algo que preocupa por ejemplo a los habitantes de zonas ricas en litio en Argentina y Portugal.

También habrá que entender hasta qué punto México se beneficiará directamente de este nuevo oro. Como dejó claro el presidente Andrés Manuel López Obrador, el país no tiene presupuesto para explotar el litio sin "participación privada".

# Crece en México la marca **TACTICAL 5.11**



**H**ace 23 años surge en el norte de California la empresa Royal Robbins, fundada por un escalador profesional quien junto con su esposa crearon una marca de pantalones para escalar que pronto se extendieron en el gusto y uso del FBI local como uniformes y dentro de la gama de productos había un modelo de pantalones denominado 5.11. Para 2002 se crea una segunda compañía que llevará este nombre, siendo Francisco Morales su presidente desde entonces, y quien la ha encaminado hacia un desarrollo de crecimiento del doble dígito en tiempo récord, pues del 2002 al 2019 ha pasado de vender 50 millones de dólares a casi 500, un ejemplo de crecimiento exponencial con valor visionario que actualmente cuenta con un catálogo de más de 10,000 productos en el mercado; logrando transformarse en una compañía global con presencia en más de 122 países, 4 corporativos mundiales y varios regionales.

El concepto del producto es un poco disperso, menciona para este medio Alexander Tavares, Director de 5.11 para

México, ya que toda la inteligencia de diseño se genera en California, la administración está en Hong Kong y la producción se realiza en varios países asiáticos, lo que les ha permitido firmar contratos de exclusividad con 20 compañías en más de 10 países del sur de Asia y desarrollar desde Estados Unidos dos lanzamientos por año de nuevos productos, tecnologías e innovación.

Desde 2008, 5.11 Tactical, se encuentra formalmente en México. Hace 10 años su objetivo al 100% era llegar a las fuerzas del orden, ya que en esencia es un producto táctico, pero hoy se ha modificado un poco su visión y se han abierto a nuevos mercados enfocándose más al parte de deporte de alto riesgo y rendimiento, el área de caza, pesca y en los últimos años cubriendo el mercado de estilo de vida, es decir, que cualquier persona pueda utilizar su ropa con componentes tácticos. En cuanto a la línea enfocada a seguridad privada, esta es de gran desarrollo para sus operaciones, pues el servicio en nivel persona día a día requiere de diseños de alto confort, materiales de calidad y utilidad multifuncional. Debido a que 5.11 cuenta con un avanzado equipo en California de arquitectos e ingenieros textiles cubren y ofrecen diferentes líneas: consumo general; especial y profesional que involucra uniformes para las fuerzas del orden.

Tavares, también asegura que los productos especializados para fuerzas del orden son personalizados y cuentan con tecnologías como chips y hologramas incrustados, que las vuelve una prenda altamente segura y difícil de copiar por parte de la delincuencia.

En México se pueden obtener sus productos de manera física en 19 tiendas de la república y también en línea. La diversidad de productos de 5.11 Táctil va desde ropa hasta accesorios con diseños innovadores, tácticos de alta calidad. "Contamos con diseños para hombres y mujeres. La línea profesional sigue siendo la más importante pero el nicho de la persona común que use estos productos es primordial para nosotros", afirma Tavares. **XS**







### Temas:

- Robo de Identidad.
- Ética Corporativa y Gestión de un programa de protección de datos para América Latina.
- Derechos ARCO.
- Trazabilidad de un ataque.
- Nuevas Normas, Nuevos Riesgos.
- Fraude Cibernético y Ciberseguridad, la brecha digital.
- Protección y Manejo de Datos Sensibles y Estratégicos.
- Biométricos, medios de autenticación.
- Big Data y Protección de Datos.
- Decisiones automatizadas.
- Confidencialidad y Transparencia.
- Gente, Procesos y Tecnología, las 3 dimensiones de la PD.

6 y 7 de Febrero  
Hotel Fiesta  
Americana,  
México Reforma



Networking entre 50  
PROFESIONALES

Agradecemos a nuestro  
MEDIA PARTNERSHIP

REVISTA  
**XTRM SECURE**  
EL MUNDO DE LA SEGURIDAD

### SPEAKERS:



**Gerdau Corsa**  
Luis Reynoso  
Compliance



**The Sherwin Williams Co**  
Lourdes Villaseñor  
Global Privacy Manager LATAM



**Nestlé**  
Wendy Alcalá  
VP Legal & Compliance



**GM**  
Estrella Jiménez  
Compliance & Privacy Officer



**INAI**  
Jonathan Mendoza  
Secretario de Protección de Datos Personales



**BGBG**  
Héctor Guzmán  
Socio Director del área de Protección de Datos Personales y Privacidad



**ASLO InformationTechnology**  
Oscar Lazcano  
Business Leader



**Grupo Televisa**  
Alberto Velazquez  
Compliance & Data Privacy Manager



**AT&T**  
Alma Hawk  
Data Protection, Privacy & Cibersecurity Director

# CONTROL L

DE ACCESOS MX



REVISTA DIGITAL

---

ESPECIALIZADA EN CONTROL DE ACCESOS

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





*La percepción de seguridad de los habitantes de espacios residenciales o de los visitantes de áreas públicas como estadios o aeropuertos depende en gran medida de adaptaciones tecnológicas a la infraestructura. Los torniquetes CAME son perfectos para este tipo de adecuaciones.*

## TORNIQUETES CAME control de acceso multipropósito respaldado con calidad y experiencia Compact

Una de las principales tareas de los administradores de espacios públicos y privados es controlar la entrada y salida de las personas que transitan a diario por allí. Hoy en día es más necesario que nunca ofrecer condiciones de seguridad, bien sea para el libre tránsito, bien sea para la restricción de personas no autorizadas.

La percepción de seguridad de los habitantes de una ciudad o de los residentes de una edificación se basa, en gran medida, en la instalación de sistemas de control de acceso —como torniquetes— que controlen el ingreso y salida de estos lugares.

Por otro lado, saber quiénes entran, quiénes salen, cuántas personas lo hacen al día y con qué finalidad, son aspectos que, además de ofrecer seguridad, permiten tener un control mayor sobre los perímetros y evitar accidentes, robos y demás situaciones que puedan poner en peligro la vida o los bienes de quienes habitan estos espacios.

Por esta razón, es indispensable que las unidades residenciales y las oficinas cuenten con sistemas de control de acceso que les permitan monitorear en tiempo real y durante las 24 horas del día quienes entran o salen de allí.

Torniquetes, puertas, lectores de huella o tarjetas son algunas de las herramientas más utilizadas en la actualidad por las edificaciones para este fin, pues con su instalación se logra un control total del acceso peatonal.

Estos sistemas, además de proteger, ayudan a optimizar recursos de personal y energía, lo que los hace aún más atractivos para todo tipo de edificios.

La necesidad de mantener a salvo los recursos, de controlar el personal que transita por un espacio y de mantener el control del paso de quienes tienen libre acceso o, por el contrario, de quienes tienen alguna restricción, son las principales razones para instalar un control de acceso peatonal.

Este componente de seguridad monitorea y controla electrónicamente el tráfico a través de elementos como puertas, entradas o ascensores.

La tecnología cada vez más se usa a favor de los seres humanos con el fin de proteger su vida y recursos y es más necesario, cada día, que las edificaciones modernas cuenten con este tipo de control de acceso.

Los residentes exigen lugares en donde se sientan seguros y en los que puedan tener la certeza de que solo entrarán a las áreas comunes (zonas verdes, ascensores y pasillos) quienes estén autorizados.

Que un edificio residencial cuente con este tipo de sistemas se ha convertido en un criterio importante a la hora de decidir en dónde comprar o alquilar un lugar para vivir.

## Torniquetes CAME, un diseño para cada necesidad

Una larga trayectoria y altos estándares de calidad son el mejor respaldo de CAME para ofrecer al mercado una amplia gama de soluciones de control de acceso peatonal, en especial sus torniquetes:

### Stile One

Son torniquetes de trípode compacto para instalaciones prácticas en espacios reducidos. Su estructura es de acero pintado y sus brazos de acero inoxidable AISI 304. Detecta eventos de forzamiento y los señala.

Cuenta con una tarjeta electrónica que incorpora una pantalla para la programación y ofrece la posibilidad de conexión al sistema de control de accesos Rbm84, también permite conectar tarjetas adicionales R700 para controlar dispositivos TSP00 o LT001.

Además, en caso de falla del suministro eléctrico, el trípode se desbloquea para permitir el tránsito en ambas direcciones (001PSMM01).



### XVIA- Twister Light- Twister

Este innovador torniquete motorizado es adecuado para la selección de tránsitos en zonas de alta intensidad de paso, está fabricado con acero inoxidable, es ideal para estaciones ferroviarias y marítimas, metros, establecimientos deportivos y, en general, sitios en donde sea indispensable controlar el flujo de personas para optimizar la entrada y salida.

Una solución robusta y funcional, adecuada a todas las exigencias de control y selección de los tránsitos, se puede instalar en cualquier sitio, incluso en lugares de flujo muy alto como estadios, estaciones, metros, oficinas públicas y centros deportivos.

Está controlado por una tarjeta electrónica incorporada, totalmente compatible con todos los sistemas modernos para el control de accesos.

### Guardian, torniquetes de altura completa para control de accesos con alta intensidad de tránsito

Guardian es la solución ideal para ofrecer seguridad en entradas amplias, incluso no vigiladas, con un gran tránsito de personas, también está diseñado para aplicaciones al aire libre: se utiliza en aeropuertos, áreas portuarias, grandes empresas, metros, estaciones ferroviarias o estadios deportivos.

Su robusta estructura y atractivo diseño lo convierten en un importante disuasor de actos criminales; por otra parte ofrece al usuario una protección total.

Su duración y fiabilidad están garantizadas también en las instalaciones al aire libre, gracias a la carrocería de acero galvanizado y a la pintura especial con polvos epoxi que le permiten resistir también en lugares en los que hay agentes corrosivos.



### Wing, torniquetes para un paso rápido y elegante y una instalación fácil y segura

La hoja, fijada dentro de la automatización, ofrece unas líneas muy armoniosas, su corona luminosa de señalización y su montaje modular señalan el movimiento de la hoja y el estado de funcionamiento del torniquete.

La tarjeta electrónica, la fuente de alimentación y el electrofreno están instalados dentro de la automatización, el electrofreno incorporado bloquea la hoja y permite el acceso solamente a los usuarios habilitados.

Tiene motor con encoder para la detección de obstáculos y para una fácil gestión de las fases de ralentización, también display, fácilmente accesible, de programación y de visualización de las funciones.

Su estructura es de acero AISI 304 con hojas de plexiglás o de cristal templado y la regulación de la velocidad de la hoja se hace directamente desde la tarjeta electrónica.





### Saloon, instalación fácil, modular y segura para tránsitos rápidos

Incorpora una corona luminosa de señalización y un montaje modular que señalan el movimiento de la hoja y el estado de funcionamiento del torniquete.

El paso se mantiene siempre bajo control gracias a una señal sonora que indica el intento de apertura forzada. Es muy segura por ser reversible, en caso de falla de suministro eléctrico, el torniquete puede operarse de forma manual tanto en la entrada como en la salida.

Tiene el sistema memory roll para garantizar el almacenamiento de la configuración y de los usuarios, es fácilmente integrable con las barreras modulares de contención.

### Compass, la gama ideal para el control de los pasos para peatones

Compass es una solución simple y barata para pilotar de una forma ordenada y eficiente los tránsitos en sitios comerciales de cualquier tamaño, desde una tienda hasta un hipermercado.

Se pueden instalar también en piscinas, centros deportivos, centros de fitness y bienestar, parques de atracciones, etc.

Cuenta con una barrera giratoria mecánica con cuatro brazos, permite el tránsito de una sola persona a la vez en ambas direcciones. Su estructura de acero inoxidable AISI 304 permite su instalación al aire libre.



### Flag, la solución polivalente para el control de los tránsitos de peatones

Esta barrera fue diseñada para facilitar el paso de las personas discapacitadas, es ideal cuando es necesario ajustar el sentido de tránsito de las personas.



# HONEYWELL

## amplía sus soluciones de control de accesos

*Honeywell está ampliando su línea de productos de lector de control de acceso OmniAssure™ con la solución de control de accesos OmniAssure™ Touch. Esta nueva gama proporciona seguridad avanzada contra la clonación de credenciales y la manipulación de lectores, aumenta la productividad del operador al implementar credenciales móviles y es interoperable con una gama de tecnologías de credenciales y protocolos de comunicación de panel.*

**O**mniaAssure Touch protege contra la clonación de credenciales y los ataques de repetición con tecnología que cumple totalmente con OSDP el Protocolo de canal seguro (PCS) y los últimos estándares de cifrado DESFire EV2. Los lectores borran el cifrado y los datos del certificado cuando se detecta la manipulación del dispositivo con todos los factores de forma disponibles con un teclado táctil capacitivo para autenticación de dos factores.



La nueva solución presenta capacidades de credenciales móviles fáciles de usar y sin problemas que eliminan la necesidad de presentar un teléfono al lector. Ofrece una fácil migración de prox heredado a tecnologías inteligentes y móviles y permite configurar los ajustes del lector en el campo a través de la aplicación móvil. Se trata de una solución integral: ahorra tiempo al implementar credenciales móviles directamente a través de las suites de seguridad integradas WIN-PAK, WINMAG y Pro-Watch de Honeywell, revoca las credenciales móviles en tiempo real y transforma la forma en que las personas interactúan con su edificio utilizando la aplicación Honeywell Vector Occupant. Es fácil de configurar ya que aprovecha la aplicación Honeywell Utility que permite a los instaladores configurar los lectores en el campo o donde sea que usen la aplicación, lo que hace que la instalación y la configuración sean más fáciles y rápidas.

OmniAssure Touch es ideal para entornos empresariales y de infraestructura crítica en una amplia variedad de industrias, incluidas defensa, educación, farmacéutica, servicios públicos y financiera. El conjunto de lectores de OmniAssure de Honeywell incorpora tecnología de tarjeta inteligente para administrar el control de acceso, acceso lógico (PC), almacenamiento de plantillas biométricas, estacionamiento, ePurse y muchas otras aplicaciones que requieren tarjetas confiables de lectura / escritura. **MS**





# INTERTRAFFIC

## Hacia una Movilidad Segura y Sustentable

*Intertraffic México es la plataforma líder en innovación y soluciones integrales en movilidad inteligente, infraestructura, gestión del tráfico, seguridad vial y estacionamientos. Del 12 al 14 de noviembre se realizó, en el Centro Citibanamex en la Ciudad de México, su 4ª edición.*



**Intertraffic México** es un evento estratégico dirigido a los profesionales que desean explorar nuevas oportunidades de negocio o establecer canales de distribución. El evento también busca incentivar la colaboración entre gobiernos, instituciones de investigación y de la iniciativa privada para promover una movilidad eficiente, sustentable y saludable.

La pieza clave de las ciudades inteligentes es la movilidad. En América Latina, la mayoría de las grandes urbes tienen problemas de tránsito, y en algunos casos el tráfico no sólo es vehicular, si no también peatonal.

En México los problemas de tráfico en las grandes ciudades, principalmente en la Ciudad de México, hacen que pierda el 36% de su capacidad en movilidad. En la capital sólo es posible recorrer un máximo de 23 km en un lapso de 30 minutos. Los automovilistas tardan 66% más en llegar a su destino, comparado con el tiempo que les tomaría cubrir la misma distancia en condiciones ideales. Se pierden en promedio 59 minutos diarios en el tráfico, lo que daría un total de 227 horas perdidas por año.

La Confederación Patronal de la República Mexicana (Coparmex) asegura que en la Ciudad de México hay pérdidas por unos 60 mil millones de pesos, además de la pérdida de 35 millones de horas-hombre, impactando significativamente en la productividad.

Un mexicano pasa casi un mes al año detenido en el tráfico, por eso nuestro país se ubica como el cuarto país con más tráfico en el mundo y se estima que para el 2040 se duplique el número de coches en las calles, mientras que la infraestructura en las grandes ciudades continuará siendo limitada.

En esta cuarta edición de **Intertraffic México** participaron, en el piso de exposición, más de 120 marcas nacionales e internacionales, además se contó con la participación de 26 conferencistas.

En el marco de la inauguración de **Intertraffic México 2019**, el titular de la Secretaría de Movilidad de la Ciudad de México, Andrés Lajous Loaeza, explicó cuáles han sido las acciones que se han efectuado para mejorar la conectividad. El funcionario reconoció que uno de los temas que siguen pendientes es mejorar la operación de los vehículos del transporte público.

De acuerdo con Laura Barrera, directora de **Intertraffic México**, se estima que para el año 2050, el 70% de la población vivirá en zonas urbanas, y por esa razón es indispensable contar con infraestructura de interconexión segura y automática en favor de los ciudadanos.

En el evento también se hizo entrega del premio **Intertraffic Latinoamérica**, un reconocimiento que se otorga a quienes ofrecen propuestas, proyectos y productos en servicio a la movilidad.

**Intertraffic México 2019** estuvo dirigido, principalmente, a las autoridades y directivos de empresas estatales y privadas, de distintos niveles, así como autoridades de transporte público y funcionarios de movilidad y seguridad pública de gobiernos municipales y estatales, aunque también estuvo abierto al público en general, a todos los interesados en el tema de la movilidad. **XS**





## La importancia de la **SEGURIDAD** **EN DISPOSITIVOS MÓVILES**

- *Existen plataformas cuyos protocolos de seguridad pueden ser obviados, permitiendo el acceso a personas maliciosas que buscan robar o bien, registrar el seguimiento de actividades dentro de las casas o negocios.*
- *Hikvision cuenta con la aplicación Hik-Connect para el monitoreo a distancia, la cual facilita el monitoreo remoto y permite a los instaladores registrar códigos de seguridad únicos de acceso propio para el cliente final evitando las vulnerabilidades de accesos externos no autorizados.*

La implementación de cámaras de seguridad en una instalación puede servir de mucho a la hora de prevenir eventos adversos, como también para reconstruir hechos que ya han ocurrido. En los últimos años se ha dado una masificación de herramientas informáticas para mantener un monitoreo constante de la seguridad de una empresa o vivienda.

Hikvision, proveedor de productos y soluciones innovadores de seguridad, comparte algunas recomendaciones importantes para que tanto los instaladores como los usuarios finales se sientan completamente seguros de la visualización de sus cámaras en dispositivos móviles pues si bien existen muchas aplicaciones gratuitas y accesibles en el mercado, es importante acceder a utilidades propias de los fabricantes, ya que con ellas se garantiza la total operatividad de los equipos instalados en los proyectos de seguridad como las cámaras, NVRs y DVRs.

Si bien otras plataformas ofrecen las mismas funcionalidades de los equipos, algunos protocolos de seguridad pueden ser obviados, permitiendo así el acceso a personas maliciosas que buscan robar o bien, registrar el seguimiento de actividades dentro de las casas o negocios.

Hikvision cuenta con la aplicación Hik-Connect para el monitoreo a distancia, es una plataforma de descarga que de manera intuitiva facilita el monitoreo remoto, permitiendo a los instaladores registrar códigos de seguridad únicos para el acceso del cliente final, evitando las vulnerabilidades de accesos externos no autorizados.

### **Protocolos y códigos de seguridad estables que ofrece Hikvision**

Hik-Connect cuenta con tres patrones de seguridad:

- Registro único de usuario final, que si bien es registrado en primera instancia por el instalador, puede ser modificado y codificado de manera individual por el usuario.
- Control de la autenticación del equipo instalado con un código de verificación único, lo que garantiza que ninguna otra persona pueda conectarse fuera del personal autorizado.
- Brindar accesos a terceros de manera remota y restringiendo el ingreso en caso de que sea necesario. Estas facultades son automáticas y limitadas desde una plataforma única, invalidando el acceso a personas maliciosas y brindando todos los recursos de seguridad que otras aplicaciones no contemplan.

### **Plataformas abiertas con limitaciones de acceso**

Hik-Connect permite visualizar de manera remota y en tiempo real a todos los usuarios que estén conectados a los dispositivos y plataformas de visualización, para verificar si un usuario, autorizado o no, está conectado a los equipos.



Incluso, permite la inhabilitación de un usuario que no cumpla con los protocolos de seguridad o que esté conectado con un código no autorizado. Esta desconexión se puede realizar desde cualquier equipo conectado a la plataforma IVMS-4200 de Hikvision para restringir de manera inmediata el acceso y solicitar un reporte de la conexión no autorizada.

### Fácil conexión sin reseteos externos

Si bien los protocolos de conexión de todos los equipos, como las cámaras, NVRs o DVRs, se realizan de manera manual con los números de serie de los dispositivos o con el escaneo de los códigos QR, para habilitar el acceso a las plataformas móviles se requieren ciertos códigos de validación como los ya mencionados. A diferencia de los equipos de Hikvision, en equipos de otras marcas cuando otras personas intentan acceder a estos dispositivos de manera remota sin conocer el código, pueden deshabilitar todo el sistema de acceso, impidiendo el acceso inclusive a los equipos centrales. Esto se debe a que los códigos y procedimientos de seguridad no son los más óptimos para el uso de recursos móviles.


Eso no pasa con Hik-Connect, ya que si el acceso queda restringido de manera remota, esto no anula el ingreso al equipo matriz. Con lo que se pueden readmitir los accesos de manera más rápida y sencilla, facilitando así la operatividad de los registros y permitiendo el acceso a las imágenes



nuevamente sin necesidad de recurrir a los servicios técnicos que hacen de la reconexión un proceso engorroso y prolongado.

### Administración única de accesos

Los instaladores deben admitir en sus proyectos que la administración de los dispositivos esté sujeta a una sola cuenta de usuario, que no sea de acceso libre a otros operarios conectados al sistema.

Para ello, Hik-Connect admite el enrolamiento un solo usuario, el cual puede ser compartido en varios dispositivos con previa autorización. Esta conexión se administra con un solo código que es ingresado una sola vez y está asociado a la cuenta del cliente final con un usuario y clave propia, administrada y registrada exclusivamente por el dueño de la cuenta. Así el cliente final y el instalador pueden tener la certeza que los accesos serán alcanzables para quienes tienen los códigos propios. 



REVISTA  
**XTREM SECURE**  
EL MUNDO DE LA SEGURIDAD




**MÁS CERCA  
DE NUESTROS LECTORES**  
¡Tu referencia en seguridad!

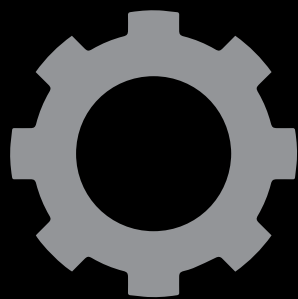
Ahora puedes consultar la revista **XTREM SECURE** de manera GRATUITA en el Aeropuerto Internacional de la Ciudad de México

**ANÚNCIATE  
CON NOSOTROS**

[www.xtremsecure.com.mx](http://www.xtremsecure.com.mx)

 Revista Xtrem Secure

 XtremSecure



# SEGURIDAD INDUSTRIAL



REVISTA DIGITAL

ESPECIALIZADA EN SEGURIDAD INDUSTRIAL

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



# La tecnología es un mecanismo para la supervisión de la **Seguridad Industrial**

*De acuerdo con Axis Communications, la seguridad de los empleados es un elemento clave en el desarrollo de las operaciones en cualquier sector económico, por ello las empresas dedican sus esfuerzos en certificar la disminución de riesgos laborales.*



Una realidad a la que se enfrentan las industrias es a la necesidad de adoptar medidas que garanticen la seguridad del personal por lo que hoy, una de las tendencias se inclina hacia la vigilancia en red, que realiza una doble función como mecanismo para la supervisión del cumplimiento de las políticas, evaluando los riesgos en vivo y mejorando las prácticas en seguridad que son indispensables para el equipo de trabajo.

Al respecto, Manuel Zamudio, Industry Associations Manager, en Axis Communications, para la región de México, Centroamérica y Caribe, refirió que todas las infraestructuras críticas tienen el deber de proteger la seguridad de sus trabajadores, por ello, las soluciones de video en red son una herramienta importante para verificar que los protocolos necesarios se lleven a cabo de manera correcta y eficiente.

La protección adecuada de los empleados requiere un cumplimiento estricto de las reglas, normativas y de las pautas establecidas, por lo que los jefes de seguridad o encargados de las industrias deben considerar que los trabajadores utilicen las herramientas y los equipos

adecuados, que conozcan muy bien los potenciales riesgos y los protocolos para mitigarlos.

Además, es necesario que sepan quiénes son las personas autorizadas para acceder a ciertas áreas, sin dejar de lado la importancia de cumplir los programas de protección civil y conocer y practicar los protocolos en caso de emergencia.

Lo anterior es el punto de partida para garantizar que los empleados puedan desenvolverse en un entorno confiable, libre de peligro y de posibles riesgos a su salud, por tal motivo las plataformas de video amplían las posibilidades de generar industrias más seguras para todos. Axis precisa que entre los principales beneficios se encuentran:

- Supervisar visualmente el cumplimiento de las políticas y evaluar los riesgos en vivo.
- Verificar el acceso en áreas restringidas con control de accesos en red integrado con un registro útil de las entradas y salidas de personas y vehículos.
- Realizar un seguimiento del número de personas que hay en cada zona.
- Valorar visualmente situaciones de emergencia.
- Realizar seguimiento y ofrecer soporte a equipos de rescate.
- Verificar el correcto y oportuno uso de equipos de protección y seguridad, conductas adecuadas en el entorno laboral y dar seguimiento de procedimientos y procesos.

Los equipos que incorporan funciones de alarmas por lesiones y detección de cascos de seguridad ayuda a las organizaciones a tener un mejor control y hacer cumplir las normativas de protección. Estas mismas aplicaciones también se utilizan para recopilar datos útiles sobre cumplimiento de los reglamentos de seguridad, donde es posible emplear los componentes de audio en red para comunicarse con las personas que no lleven a cabo las reglas establecidas.

Por último, las soluciones de vigilancia en red pueden ofrecer resultados asombrosos en situaciones de emergencia. El control de acceso integrado y las cámaras permiten a los operadores realizar el seguimiento de la cantidad de trabajadores presentes en cada área de una instalación en un momento determinado. Los equipos se emplean para ayudar a evaluar el tipo, alcance y gravedad de una emergencia, además sirven de ayuda para llevar a cabo una evacuación eficiente de las instalaciones mediante la detección de humo, la evolución de un incidente, monitoreando el flujo del desalojo y ofreciendo apoyo a los equipos de rescate y ofrecen importante información para posibles investigaciones, así como para la capacitación de nuevo personal. **AS**



## **POR ACCIDENTES LABORALES**

# **se pierde el 4% del Producto Interno Bruto (BIP) Mundial**

*Una de las mayores causas de accidentes y fatalidades es la distracción. El error humano va más allá de la seguridad, Karina Ojeda, empresa SafeStart*



Según la Organización Internacional del Trabajo, 374 millones de personas sufren de lesiones o enfermedades causadas por accidentes relacionados al trabajo, se calcula que los días perdidos de trabajo representan el 4 por ciento del Producto Interno Bruto (PIB) Mundial y en algunos países hasta el 6 por ciento.

Karina Ojeda, de la empresa SafeStart habló en una presentación online para América Latina de este programa, enfocado a la disminución de accidentes laborales y las consecuencias que enfrentan las empresas cuando el error humano toca la puerta.

“Recuerdo el caso de una aerolínea donde el piloto en plena pista contesta una llamada telefónica y durante esta distracción provoca una avería en un ala del avión, causando una pérdida económica de 7 millones de dólares para la aerolínea, aunado al tiempo que el avión se mantuvo en el taller en reparación, las empresas no deben permitir que un área de riesgo utilice celular”, destacó.


“Una de las mayores causas de accidentes y fatalidades es la distracción. El error humano va más allá de la seguridad”. La especialista informó que “en América Latina, el 90 por ciento de los conductores usan celular mientras conducen, provocando severos accidentes”.

“A pesar de las reglas de seguridad en las organizaciones, los trabajadores se siguen accidentando, la mayoría de las organizaciones utilizan el programa de observación, para que hagan recorridos internos, pero estas medidas no son suficientes”, dijo Karina Ojeda.

SafeStart trabaja el lado humano, proporcionando habilidades para que las personas aprendan a cuidarse a sí mismas, disminuyendo entre un 30 a 70 por ciento los errores y accidentes.

Según análisis realizados por SafeStart entre el 85 y 95 por ciento de los accidentes son ocasionados por las decisiones de las personas que en la mayoría de las veces no son conscientes. El autor de este programa Larry Wilson, descubrió que cuatro estados mentales provocan accidentes: Prisa, Frustración, Fatiga y Complacencia.

Una persona cansada físicamente no rinde, hay operarios de máquinas que trabajan con cansancio, por lo que tarde o temprano esta condición humana pasa la factura.

SafeStart es un programa canadiense que atiende a más de 3 mil empresas en 60 países en 30 idiomas – en México su oficina principal está ubicada en Monterrey - “su principal beneficio es su presencia mundial, el error humano es igual en todas partes del mundo, los seres humanos nos distraemos de la misma forma”. 





# FUJITSU

## Desarrolla la tecnología de Mitigación de Desastres de IA para predecir inundaciones de ríos

Fujitsu Limited y Fujitsu Laboratories Ltd. anuncian el desarrollo de una tecnología que se basa en modelos matemáticos contruidos con datos limitados sobre los niveles de lluvia y agua, para crear predicciones de inundaciones de los ríos. La solución aprovecha Fujitsu Human Centric AI Zinrai, un portafolio integral que abarca la amplia gama de tecnologías y técnicas de Inteligencia Artificial (IA) de Fujitsu, y utiliza un modelo que incorpora los conocimientos de la hidrología para producir una IA que logre predicciones con mayor precisión.

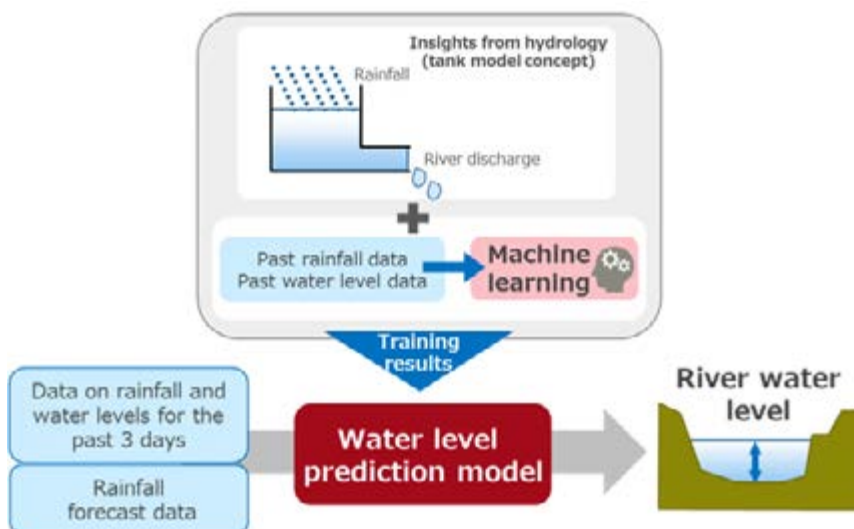
La nueva tecnología es efectiva incluso para ríos más pequeños con datos de medición limitados o para áreas donde los sensores de nivel de agua se han instalado recientemente y aún no han acumulado suficientes datos. Estas predicciones ofrecerán a las autoridades una herramienta vital para ofrecer tiempos de respuesta más rápidos y mitigar los daños por inundaciones en caso de un desastre natural, incluido el envío de personal a las áreas

afectadas y el apoyo a la toma de decisiones apropiadas al emitir avisos de evacuación.

Fujitsu y Fujitsu Laboratories continuarán trabajando para perfeccionar aún más esta tecnología a través de una prueba de campo con gobiernos locales en todo Japón, con el objetivo de ofrecer una solución comercial durante el año fiscal 2019. Así, la multinacional demuestra cómo esta y otras tecnologías de IA desempeñan un papel importante para combatir los efectos del cambio climático y contribuir al logro de una mayor sostenibilidad en la sociedad.

### Antecedentes

En los últimos años, los gobiernos locales en Japón se han enfrentado a los desafíos de la gestión de los ríos que causan graves daños por inundaciones a raíz de las frecuentes fuertes lluvias. Los ríos más pequeños que fluyen a través de áreas urbanas, a menudo experimentan un aumento repentino del nivel del agua debido al impacto de tormentas de lluvia y tifones impredecibles, pero poderosos. Año tras año, el riesgo de que ocurran daños importantes muy rápidamente por inundaciones representa una



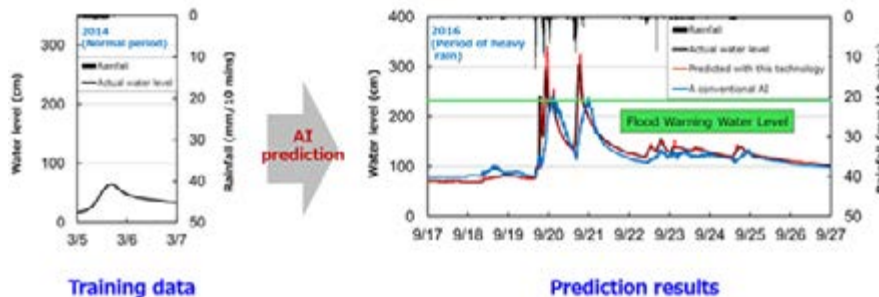
amenaza esporádica, pero cada vez más grave, lo que subraya la necesidad urgente de mejorar las medidas frente a la inundación. Como parte de estas, se han realizado predicciones del nivel del agua para grandes ríos designados como riesgo de inundación. Sin embargo, para ríos más pequeños o áreas donde se han instalado sensores de nivel de agua recientemente, hacer predicciones precisas ha resultado difícil hasta ahora, debido a la falta de datos suficientes, sobre el nivel de agua y los últimos resultados de observación de la tasa de flujo.

Para abordar esto, Fujitsu y Fujitsu Laboratories han desarrollado una nueva tecnología que predice con precisión los niveles de agua, incluso para ríos con datos de medición limitados, permitiendo al personal de prevención de desastres tomar medidas tempranas para mitigar los daños.

### Acerca de la tecnología recientemente desarrollada

Fujitsu y Fujitsu Laboratories han desarrollado un modelo matemático que puede encontrar parámetros óptimos cuando el aprendizaje automático se usa para conocer el modelo con datos de lluvia y del nivel de agua pasados, creando funciones basadas en el concepto de modelo de tanque, que expresa la descarga de agua de una cuenca fluvial dentro de la hidrología.


Usando este modelo, la IA predice los niveles de agua futuros en función de la información recopilada para presentar los datos sobre las precipitaciones y el nivel de agua, junto con los pronósticos para las próximas horas transmitidos a los gobiernos locales por varias organizaciones meteorológicas. El modelo de predicción también se puede optimizar muy

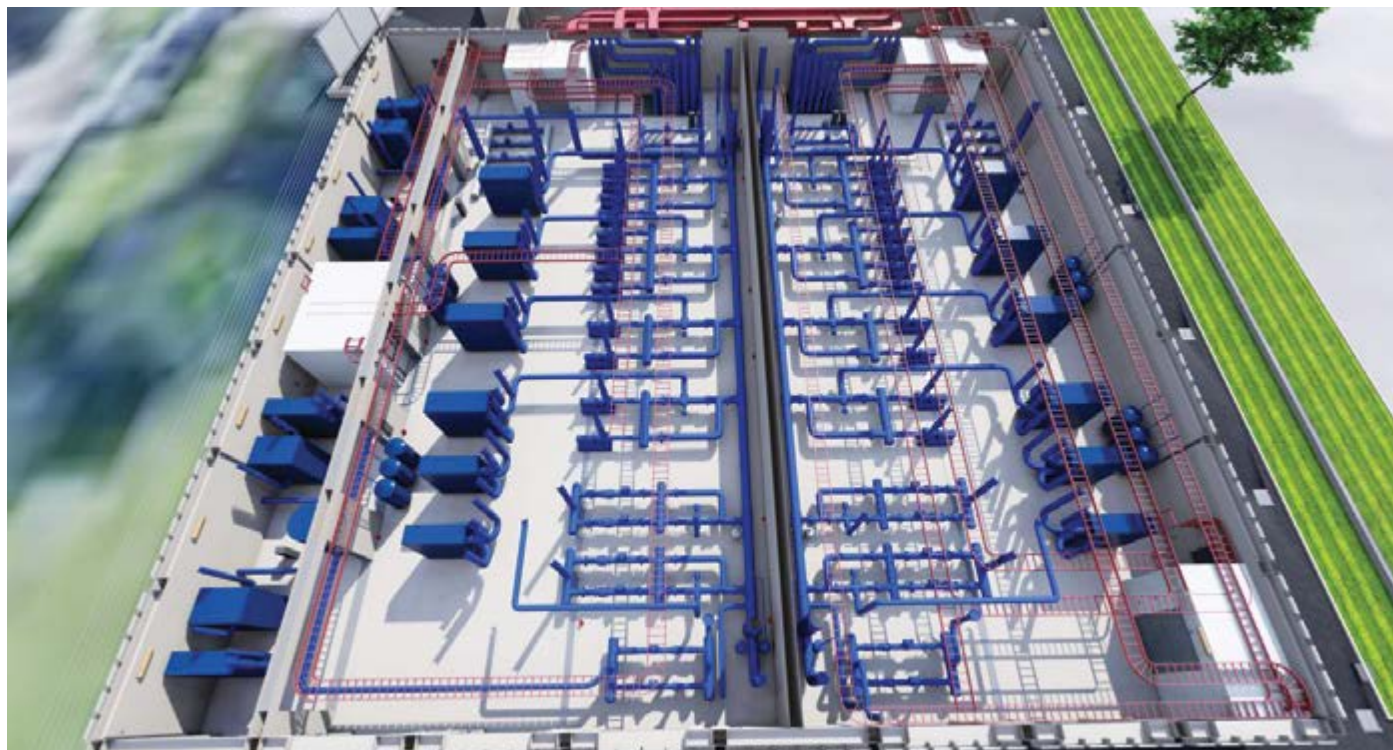


rápidamente, incluso después de los cambios en el entorno del río o la introducción de nueva infraestructura. En casos como este, el modelo simplemente se puede re-entrenar utilizando datos de lluvia y del nivel de agua tomados después de cualquier cambio.

Cuando se realizó una prueba que evaluaba la precisión del nuevo modelo aplicando esta tecnología a datos anteriores de ríos más pequeños administrados por un gobierno local, se verificó que cuando se trabajaba con datos de sólo un aumento de nivel de agua de lluvia podía predecirse con una precisión consistente (Figura 2). Además, Fujitsu y Fujitsu Laboratories han llevado a cabo una evaluación que compara esta tecnología con los métodos estándar de predicción del nivel del agua, que utilizan datos como observaciones de caudal. La evaluación, realizada con la asistencia del profesor Akira Kawamura de la Universidad Metropolitana de Tokio, confirmó con éxito que esta tecnología puede ofrecer una precisión equivalente o mejor.

### Perspectivas de futuro

Fujitsu anticipa que esta tecnología también se puede aplicar para ayudar a controlar las inundaciones en ríos fuera de Japón y está llevando a cabo una variedad de pruebas con clientes con el objetivo de ponerla a disposición como solución comercial en el año fiscal 2019. Fujitsu Laboratories está trabajando para mejorar aún más la precisión de esta tecnología, haciéndola parte de un conjunto de tecnologías predictivas y de diagnóstico para proteger los activos de los clientes, incluyendo las instalaciones y la infraestructura social cerca de los ríos, contribuyendo así a la creación de pueblos y ciudades resistentes a los desastres gracias al uso de tecnología digital. 





# DIRECTORIO DE SEGURIDAD



**ABASTECEDOR PRINCIPAL NACIONAL, S.A. DE C.V.**

No. de Autorización. DGSP/020-11/1687  
La Rioja Número 2979, Col. Providencia  
1ra. 2da. y 3ra. Secc., C.P. 44630,  
Guadalajara, Jalisco.

Tel. (33) 36425110 / 36412350 / 36415684  
ventas@aprinna.net / www.aprinna.net



**GRUPO LK**  
SEGURIDAD PRIVADA

**LK SEGURIDAD PRIVADA, S.A. DE C.V.**

No. de Autorización. DGSP/119-07/926  
Hacienda de Tepalcates No.57,  
Col. Hacienda el Rosario, C.P. 02420,  
Alcaldía Azcapotzalco, Ciudad de México.

Tel. (55) 8848 8264  
grupolk2020@gmail.com



**Multiproseg**  
Agrupación de  
MULTIPRODUCTOS DE SEGURIDAD PRIVADA S.A. DE C.V.  
SERVICIOS DE SEGURIDAD PRIVADA

**MULTIPROSEG, S.A. DE C.V.**

No. de Autorización DGSP/090-16/3023  
Av. Armada de México No. 1500,  
Residencial Cafetales, C.P. 80220,  
Alcaldía Coyoacán, Ciudad de México.

Tel. 01(55) 5594 5513  
info@multiproseg.com / www.multiproseg.com



**IPS**

**INTERNATIONAL PRIVATE SECURITY DE MEXICO, S.A. DE C.V.**

No. de Autorización DGSP/008-12/1940  
General Ignacio Zaragoza Número 768,  
Col. Aviación Civil, C.P. 15740,  
Alcaldía Venustiano Carranza, Ciudad de México.

Tel. (55) 63786621  
www.grupoipsmexico.com



**INALARM**  
CORPORATIVO

**CORPORATIVO INALARM, S.A. DE C.V.**

No. de Autorización DGSP/115/11/1751  
Rey Maxtla No. 213, Col. San Francisco  
Tetecala, C.P. 02730, Alcaldía Azcapotzalco,  
Ciudad de México.

Tel. (55) 5354 5670  
www.inalarm.mx



**SEPSISA**  
SEGURIDAD PRIVADA

**SERVICIOS ESPECIALIZADOS EN SEGURIDAD PRIVADA SEPSISA, S.A. DE C.V.**

No. de Autorización DGSP/277-12/2152  
Calzada de Las Bombas No. 121,  
Col. Ex-Hacienda, Coapa, C.P. 04980,  
Alcaldía Coyoacán, Ciudad de México.

Tel. (55) 5662 6284 (55) 5662 6039, (33) 1562 6604 y (33) 3658 4548  
www.sepsisa.com.mx



**ICP RANGER SWAT MEXICO**

**ICP RANGER SWAT MEXICO, S.A. DE C.V.**

No. de Autorización. DGSP/250-17/3397  
Av. Invierno Número 11, Col. Ángel Zimbron,  
C.P. 02099, Alcaldía Azcapotzalco,  
Ciudad de México.

Tel. (55) 5561535  
contacto@rangerswat.com.mx / www.rangerswat.com.mx



**GRUPO EMPRESARIAL CASA**

**GRUPO EMPRESARIAL CASA, S.A. DE C.V.**

No. de Autorización DGSP/144-05/669  
Limoneros No. 9-A, Fraccionamiento  
Valle de San Mateo, C.P. 53240, Naucalpan,  
Estado de México.

Tel. 5373 1761 y 5363 2868  
ventas@gecsa.com.mx / www.gecsa.com.mx



# Las 10 normas más importantes sobre **SEGURIDAD INDUSTRIAL**

## 1.- Condiciones de seguridad para la prevención y protección contra incendios

Esta norma establece las condiciones de seguridad para la prevención contra incendios. Se aplica en aquellos lugares donde las mercancías, materias primas, productos o subproductos que se manejan en los procesos, operaciones y actividades que impliquen riesgos de incendio.

(Nom-002-STPS-1993. de las Normas Oficiales Mexicanas).

## 2.- Sistemas de protección y dispositivos de seguridad en maquinaria, equipos y accesorios

Esta norma tiene por objetivo prevenir y proteger a los trabajadores contra los riesgos de trabajo. Se aplica donde por la naturaleza de los procesos se emplee maquinaria, equipo y accesorios para la transmisión de energía mecánica.

(Nom-004-STPS-1994. de las Normas Oficiales Mexicanas).

## 3.- Condiciones de seguridad para el almacenamiento, transporte y manejo de sustancias inflamables y combustibles

Esta norma tiene por objetivo prevenir y proteger a los trabajadores contra riesgos de trabajo e incendio. Se aplica donde se almacenen, transporten o manejen sustancias inflamables y combustibles.

(Nom-005-STPS-1993. de las Normas Oficiales Mexicanas).

## 4.- Seguridad e Higiene para el almacenamiento, transporte y manejo de sustancias corrosivas, irritantes y tóxicas

Su objetivo es prevenir y proteger a los trabajadores contra los riesgos de quemaduras, irritaciones o intoxicaciones. Se aplica donde se almacenen, transporten o manejen sustancias corrosivas, irritantes o tóxicas.

(Nom-009-STPS-1994. de las Normas Oficiales Mexicanas).

## 5.- Seguridad e higiene en los centros de trabajo donde se produzcan, almacenen o manejen sustancias químicas capaces de generar contaminación en el medio ambiente laboral

Su objetivo es prevenir y proteger la salud de los trabajadores y mejorar las condiciones de seguridad e higiene donde se produzcan, almacenen o manejen sustancias químicas que por sus propiedades, niveles de concentración y tiempo de acción sean capaces de contaminar el medio ambiente laboral y alterar la salud de los trabajadores, así como los niveles máximos permisibles de concentración de dichas sustancias, de acuerdo al tipo de exposición. Se aplica donde se produzcan, almacenen o manejen sustancias químicas capaces de generar contaminación en el ambiente laboral.

(Nom-010-STPS-1994. de las Normas Oficiales Mexicanas).



## 6.- Seguridad e higiene en los centros de trabajo donde se produzcan, usen, manejen, almacenen o transporten fuentes generadoras o emisoras de radiaciones ionizantes

Su objetivo es implantar las medidas preventivas y de control a fin de que los trabajadores expuestos a radiaciones ionizantes, no reciban por este motivo dosis que rebasen los límites establecidos en la presente norma. Se aplica donde se produzcan, usen, manejen, almacene o transporten fuentes generadoras o emisoras de radiaciones ionizantes.

(Nom-012-STPS-1994. de las Normas Oficiales Mexicanas).

## 7.- Protección personal para los trabajadores en los centros de trabajo

El objetivo de esta norma es establecer los requerimientos de la selección y uso del equipo de protección personal para proteger al trabajador de los agentes del medio ambiente de trabajo que puedan alterar su salud y vida. Se aplica en todos los centros de trabajo como medida de control personal en aquellas actividades laborales que por su naturaleza, los trabajadores estén expuestos a riesgos específicos.

(Nom-015-STPS-1994. de las Normas Oficiales Mexicanas).

## 8.- Condiciones de seguridad en donde la electricidad estática represente un riesgo

Su objetivo es establecer las medidas de seguridad para evitar

los riesgos que se derivan por generación de la electricidad estática. Se aplica en los centros de trabajo donde por la naturaleza de los procedimientos se empleen materiales, sustancias y equipo capaz de almacenar cargas eléctricas estáticas.

(Nom-022-STPS-1993. de las Normas Oficiales Mexicanas).

## 9.- Señales y avisos de seguridad e higiene

Establece el código para elaborar señales y avisos de seguridad e higiene; así como las características y especificaciones que éstas deben cumplir. Las señales y avisos de seguridad e higiene que deben emplearse en los centros de trabajo, de acuerdo con los casos que establece el Reglamento General de Seguridad e Higiene en el Trabajo, y no es aplicables a señales o avisos con iluminación propia. Por lo tanto se aplica en todos los centros de trabajo.

(Nom-027-STPS-1994. de las Normas Oficiales Mexicanas).

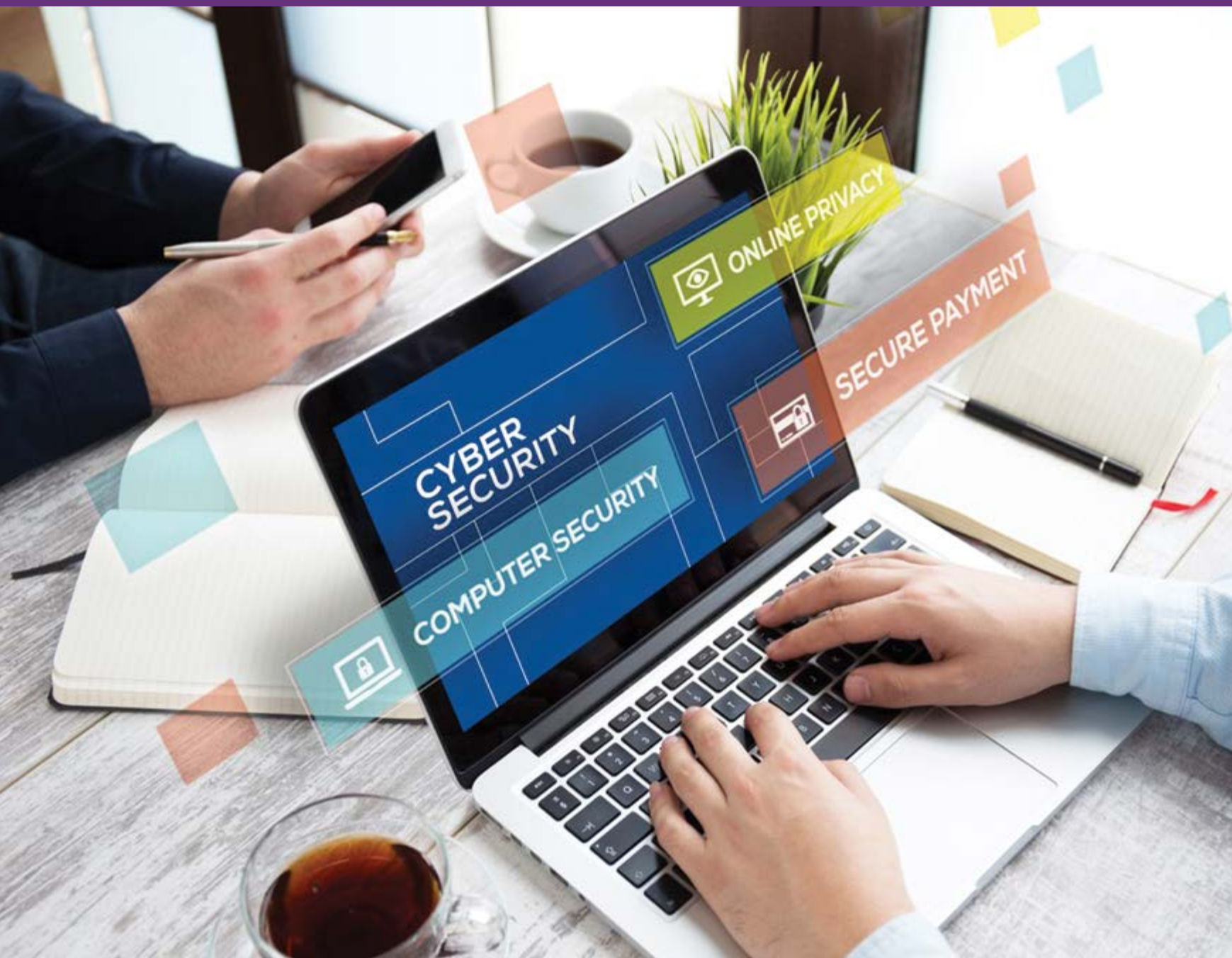
## 10.- Medicamentos, materiales de curación y personal que presta los primeros auxilios

Establece las condiciones para brindarlos primeros auxilios oportunos y eficazmente. Se aplica en todos los centros de trabajo, para organizar y prestar los primeros auxilios.

(Nom-020-STPS-1994. de las Normas Oficiales Mexicanas).



# CIBERSEGURIDADMX



REVISTA DIGITAL  
ESPECIALIZADA EN CIBERSEGURIDAD

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



# 4 formas en que la Inteligencia Artificial ayuda a las empresas a vender más:

## AGENCIA B12

- *La IA se ha abierto paso por los procesos empresariales al conocer mejor a los clientes y productos, lo que da como resultado mayor productividad.*
- *Está en la automatización de procesos, en el análisis de datos, en el apoyo al trabajador humano y sobre todo en la atención al cliente.*



**S**i se adoptan tecnologías asociadas a IA, en los próximos 10 años, el ritmo de crecimiento económico podría acelerarse en más de un punto porcentual por año, de acuerdo con el estudio Inteligencia Artificial y Crecimiento Económico. Oportunidades y Desafíos para México, elaborado por el Centro de Implementación de Políticas Públicas para la Equidad y el Crecimiento (CIPPEC).

David Pérez, Country Manager de Agencia B12 México, comenta sobre este tema: “La IA se va abriendo paso por los procesos empresariales al conocer mejor los clientes y productos, lo que da como resultado mayor productividad”. Veamos 4 formas de cómo la IA impacta a las empresas:

### 1. Automatización de procesos

Cuando los procesos son rutinarios y se hacen de forma manual son susceptibles de automatizarlos a través de máquinas inteligentes de IA, para ayudar a las empresas a ser más ágiles al operar más rápido y con menos recursos. Esta automatización se está dando en diversos sectores del país, desde robots en una fábrica automatizada, hasta en procesos de trámites en una aseguradora.

### 2. Análisis de datos

Datos hay en todas partes, procesarlos significa convertirlos en información para darles sentido y valor. El crecimiento de Big Data se hace presente cuando se trata de manejar grandes cantidades de datos a través de la administración y análisis, para darles esa estructura

que los transforma en información. Tal es el caso, por ejemplo, cuando se usa para conocer mejor a los clientes en cualquier tipo de negocio.

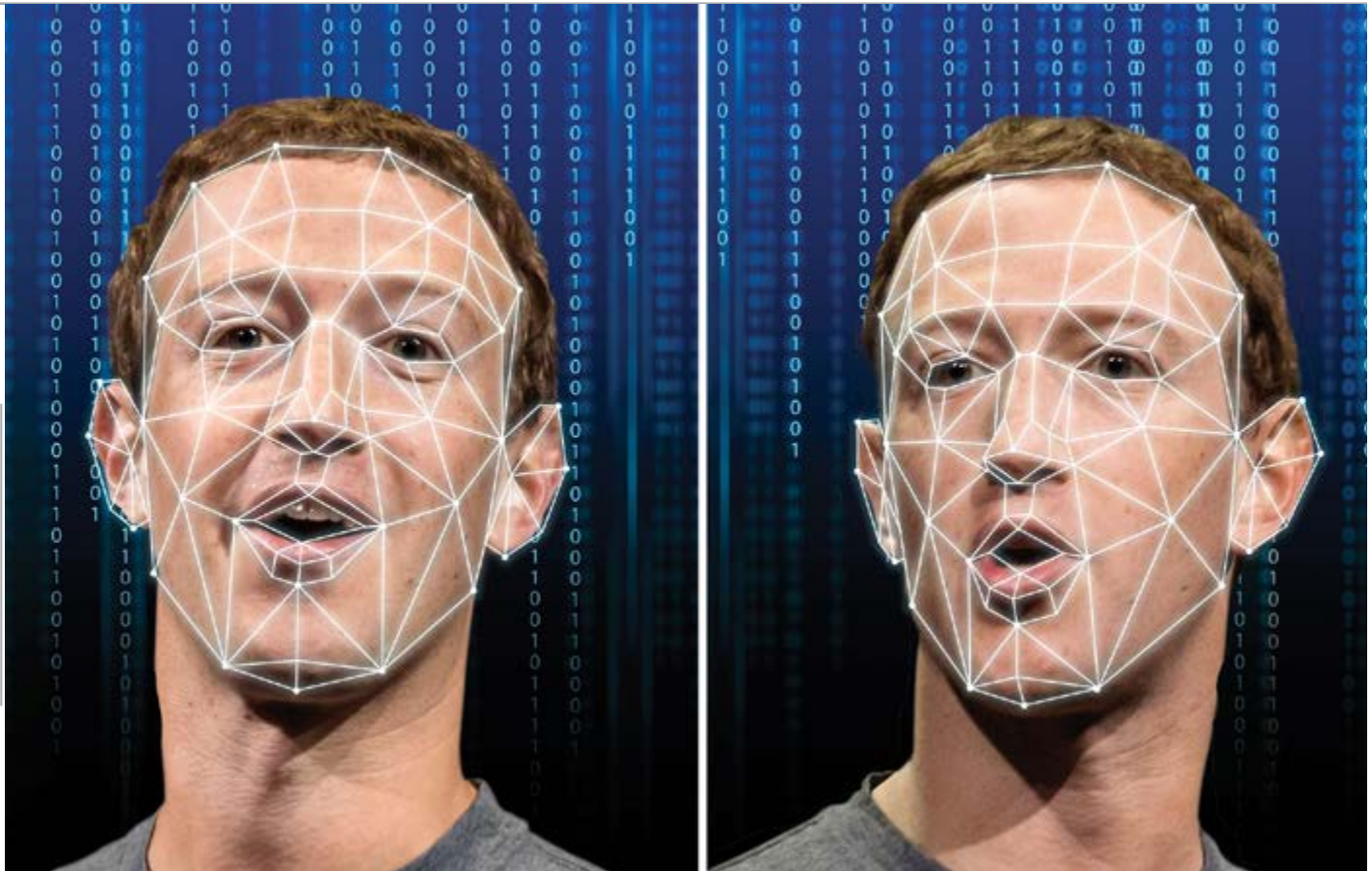
### 3. Apoyo al equipo humano

Mucho se ha hablado de que la IA reemplazará al ser humano, pero lo cierto es que más bien ayuda a los trabajadores en su seguridad, en su desempeño diario y al predecir perfiles de clientes o futuros clientes, lo que trae evidentes beneficios a las compañías que se apoyan en la IA para sus tareas fáciles o complicadas a fin de ser más productivos, lo que definitivamente retribuye en más ventas.

### 4. Atención al cliente

Con el objetivo de atender mejor al cliente 24x7, las compañías de comercio electrónico han integrado Chatbots en sus sitios Web para apoyar a su cliente en tiempo real. Esta asistencia es completa gracias a las soluciones de IA que agilizan el servicio y facilitan el perfeccionamiento de las herramientas digitales para ser más eficaces y lograr mayores ventas.

David Pérez afirma que la IA constantemente va tomando relevancia en el mundo empresarial, tanto en procesos internos, como en manufactura y hasta en el reconocimiento del habla y del lenguaje natural. La IA está presente en varias de las empresas más potentes del mundo. La emplean para fines tan diversos como mejorar la experiencia de usuario, perfeccionar sus productos y ofrecer un buen servicio posventa. Se trata de empresas como Apple, Facebook, Tesla, y Google, entre otras. 



# DEEPFAKES

## ¿Estamos preparados para su impacto?

Por Jake Moore

*Las deepfakes están comenzando a crearse con mayor facilidad y rapidez, y están abriendo una puerta a una nueva forma de delito cibernético. Aunque los videos falsos todavía se consideran como relativamente dañinos o incluso como graciosos, este fenómeno podría dar un giro más siniestro en el futuro y ser el centro de escándalos políticos, delitos cibernéticos o incluso escenarios inimaginables que involucran videos falsos, y no solo dirigidos a figuras públicas.*

Se conoce como deepfake a la técnica de síntesis de imágenes humanas basada en inteligencia artificial que se utiliza para crear contenido falso, ya sea desde cero o usando un video existente con el objetivo de replicar la apariencia y el sonido de un humano real. Tales videos pueden parecer increíblemente reales y actualmente muchos de estos involucran a celebridades o figuras públicas que dicen algo escandaloso o falso.

Una reciente investigación muestra un gran aumento en la creación de videos que hacen uso de esta técnica, casi duplicándose el número de estos videos solo en los últimos nueve meses. Los deepfakes también están creciendo en calidad a un ritmo acelerado. Al buscar en YouTube el término 'deepfake', te darás cuenta de que estamos viendo la punta del iceberg de lo que está por venir.

De hecho, ya se han registrado casos en los que se utiliza esta tecnología para el fraude, donde, según los informes, se utilizó una voz falsa para estafar a un CEO con una gran suma de dinero. Se cree que el CEO de una firma británica no identificada pensó que estaba hablando por teléfono con el CEO de la empresa matriz alemana y fue convencido para transferir, de forma inmediatamente, € 220,000 (aproximadamente US\$ 244,000) a la cuenta bancaria de un supuesto proveedor húngaro. Si fue tan fácil influir en alguien simplemente pidiendo que lo haga mediante una llamada telefónica, entonces seguramente necesitaremos una mejor seguridad para mitigar esta amenaza.

### Engañando el ojo

También hemos visto aplicaciones que hacen que los deepnudes conviertan en segundos las fotos de cualquier persona vestida en una foto en topless. Si



bien, afortunadamente, una aplicación en particular, DeepNude, fue dada de baja, ¿qué sucedería si la misma regresa bajo otra forma y es capaz de crear videos convincentemente de apariencia auténtica?

También hay evidencia de que la producción de estos videos se está convirtiendo en un negocio lucrativo, especialmente en la industria de la pornografía. La BBC dice que “el 96% de estos videos son de celebridades femeninas cuyas imágenes fueron utilizadas para crear videos sexuales sin su conocimiento o consentimiento”.

Un proyecto de ley reciente en California ha dado un salto de fe y ha hecho ilegal crear una deepfake pornográfica de alguien sin su consentimiento, multando al responsable con hasta \$150,000. Pero es muy probable que ninguna legislación sea suficiente para disuadir a algunas personas de crear esta clase de videos.

Para estar seguros, un artículo de The Economist discute que para hacer una deepfake lo suficientemente convincente se necesitaría una gran cantidad de material en video y/o grabaciones de voz para hacer incluso una breve deepfake. Quería desesperadamente crear una deepfake de mí mismo, pero lamentablemente, al no contar con muchas horas de video, no pude hacer una deepfake de mi rostro.

Habiendo dicho eso, en un futuro no muy lejano, puede ser completamente posible que a partir de solo unas pocas “historias” de Instagram se pueda crear una deepfake convincente para la mayoría de los seguidores. Adicionalmente, las deepfakes también pueden ser utilizadas para hacer bullying en las escuelas, la oficina o incluso en otros terrenos.

Además, los ciberdelincuentes definitivamente utilizarán más esta tecnología para generar víctimas.

### Enfrentando una amenaza muy real

Entonces, ¿qué se puede hacer para prepararnos ante esta amenaza? Primero, necesitamos educar mejor a las personas sobre la existencia de las deepfakes,

*Las deepfakes se están volviendo más fáciles de crear y se vuelven casi imposibles de detectar para el ojo humano. Como resultado, toda esa falsificación podría contaminar el agua que separa la realidad de la ficción, lo que a su vez podría llevarnos a no confiar en nada, incluso cuando se nos presenta algo que nuestros sentidos nos dicen que es real.*

cómo funcionan y el daño potencial que pueden causar. Todos tendremos que aprender a ser conscientes de que incluso los videos más realistas que vemos podrían tratarse de piezas fabricadas.

En segundo lugar, la tecnología necesita desesperadamente desarrollar una mejor detección de las deepfakes. Aunque el machine learning es una pieza central en la creación de estos contenidos falsos, deberá crearse algo que actúe como el antídoto capaz de detectarlos sin depender únicamente del ojo humano.

Finalmente, las plataformas sociales deben darse cuenta de que existe una amenaza importante y que puede tener un impacto muy grande, porque cuando se combina un video impactante con las redes sociales, el resultado suele ser una propagación muy rápida, lo cual podría tener un impacto negativo en la sociedad.

No me malinterpretes; disfruto enormemente el desarrollo de la tecnología y ver cómo se desarrolla frente a mis propios ojos. Sin embargo, debemos ser conscientes de cómo la tecnología a veces puede afectarnos negativamente, especialmente cuando el machine learning está madurando a un ritmo más rápido que nunca. De lo contrario, pronto veremos que las deepfakes se convertirán en la norma y esto tendrá efectos de largo alcance. **MS**





## PROFESIONALES EN SEGURIDAD INFORMÁTICA: Entre la formación académica y la autodidacta

Por Juan Manuel Harán

Según un informe reciente de Cybersecurity Ventures, el crecimiento de las vacantes en el sector de la ciberseguridad se espera que crezca en un 350% para el 2021. Sin embargo, la escasez de profesionales con las habilidades suficientes para cubrir esa demanda se estima que generará, para ese mismo año, tres millones y medio de vacantes a lo largo del mundo que no serán cubiertas.

### ¿Una formación que se adquiere de manera autodidacta?

Si bien cada vez más universidades alrededor del mundo ofrecen carreras de grado en seguridad informática, aún no es una titulación que pueda encontrarse en todas las instituciones. Muchos profesionales que se desempeñan en este campo adquirieron sus habilidades a través de certificaciones y de manera autodidacta. Sin embargo, si bien no están lo suficientemente difundidas como deberían si consideramos la demanda, la realidad es que la oferta se está incrementando, aseguran especialistas.

Según nos explica el reconocido investigador de ESET, Aryeh Goretsky, quien comenzó a trabajar en la industria a fines de

los años 80, al principio no había cursos ni certificaciones sobre ciberseguridad. “Si bien nos enseñaron seguridad informática, el foco estaba centrado en modelos de control de acceso y en el concepto de asegurar sistemas informáticos para múltiples usuarios; pero no desde una perspectiva más amplia o como un sistema interconectado a nivel global. Por lo tanto, quienes estaban interesados en el concepto de ciberseguridad teniendo en cuenta el comportamiento de computadoras y redes interconectadas comunicadas entre sí, debían aprenderlo por cuenta propia a partir de libros y de la propia experimentación práctica”, explica.

Por su parte, el investigador de malware del laboratorio de ESET de Canadá, Marc Etienne Léveillé, quien estudió desarrollo de software e ingeniería informática, explica que “varias de las cosas que aprendí en la universidad no aplicaban en mi posición como investigador, lo que me llevó a tener que leer y aprender acerca de muchos aspectos de seguridad por cuenta propia”.

Sin dudas que en la actualidad el escenario contribuye enormemente al aprendizaje autodidacta. Esto lo comprobamos con la oferta educativa y de calidad que ofrecen plataformas que ofrecen cursos online masivos y abiertos (MOOC, por sus siglas en inglés) como Coursera, con la posibilidad que ofrecen redes sociales como Twitter para compartir información constantemente y en la que se conectan grandes profesionales con personas deseosas de aprender; además de la cantidad de recursos disponibles en YouTube, sitios web y demás repositorios. “Si bien el aprendizaje por cuenta propia es un camino posible y muchos profesionales en esta industria se formaron de esta manera, no se trata de la

*El crecimiento de los ciberataques a lo largo de los años provocó un aumento de la demanda de profesionales en el campo de la seguridad de la información a figuras públicas.*



única opción”, explica el investigador de ESET Brasil, Daniel Cunha Barbosa. “También es cierto que la comunidad de tecnología y seguridad es cada vez mayor y a un gran porcentaje de la misma le gusta compartir sus conocimientos, lo que permite que los profesionales que recién comienzan consigan tener el apoyo de otros profesionales”, añade.

Sin embargo, pese a la necesidad muchas veces de aprender por cuenta propia muchos aspectos que forman parte de la seguridad y de la labor diaria de los investigadores, varios coinciden en el valor de la formación académica. “Si tuviera que decidir nuevamente qué camino seguir volvería a elegir la universidad, ya que me dio la oportunidad de conocer muchas personas y de participar en distintas actividades extra curriculares”, dice Marc Etienne.

### Creció la oferta académica en el campo de la seguridad informática

Dado que los incidentes de seguridad han incrementado con el correr de los años, también el deseo de estandarizar los aspectos pedagógicos de quienes desean formarse en este sector, opina Goretsky. “En general creo que es positiva la amplia oferta educativa que existe actualmente en todos los niveles que hacen a la ciberseguridad, pero también me preocupa la calidad de la educación que se ofrece”, explica. “Necesitamos tanto de profesionales que cuenten con conocimientos teóricos como de perfiles operativos, y necesitamos que todos ellos cuenten con sólidos conocimientos acerca de la construcción de bloques de sistemas complejos. Si bien mucho de esto puede aprenderse, aún es necesario el aprendizaje por cuenta propia para llevar los conocimientos adquiridos a la construcción de estructuras complejas y al desarrollo de ideas, pero no sé si la oferta de posgrados y las certificaciones ofrecen un marco suficiente o limitado que permita obtener una base sólida de los conceptos en ciberseguridad”, añade.

En países como Canadá, la oferta de cursos universitarios en ciberseguridad ha incrementado, cuenta Léveillé. “Ahora hay titulaciones con especializaciones en seguridad informática, mientras que antes la única opción era hacer desarrollo de software o redes informáticas. Igualmente, aún existe una demanda creciente de profesionales que es necesario cubrir en nuestra industria. Quizás, con el esfuerzo de los programas educativos veremos en algunos años una situación más estable”, opina.

Para Cunha Barbosa, “es más positivo que existan programas de especialización y de posgrado que titulaciones en sí, ya que contar con una titulación que le brinda al futuro profesional una base más amplia le permitirá conocer aspectos tecnológicos que van más allá de la seguridad, y eso lo ayudará a convertirse en un profesional más preparado”.

### ¿Qué tan promocionadas son las carreras en ciberseguridad?

Muchas veces, los jóvenes se enfrentan a un difícil proceso cuando deben decidir qué carrera estudiar. Muchos finalizan la educación secundaria sin tener muy claro qué quieren hacer de sus vidas. Más allá de la multiplicidad de factores que entran en juego y que hacen que este proceso sea difícil, el hecho de no tener información sobre las carreras

menos tradicionales hace que los jóvenes no logren vincular sus intereses y gustos personales con un área de formación.

Varios especialistas coinciden en que la visibilidad de las carreras en seguridad es mayor ahora que hace unos años. “Antes era algo que debías descubrir por tu propia cuenta, pero ahora veo muchos más estudiantes interesados en seguridad informática que en mi época de estudiante. Ahora se nota que hay más empresas y escuelas que quieren despertar el interés en los estudiantes”, opina Léveillé.

Por otra parte, “los jóvenes muchas veces se hacen una imagen equivocada acerca de qué es la ciberseguridad y no logran darse cuenta del alcance”, comenta Aryeh Goretsky. Los jóvenes puede que vean como atractiva la imagen del prototipo de un hacker atacando computadoras y adquiriendo fama y dinero, pero lo que hace falta también es explicar que hace la ciberseguridad. “Creo que hay una falta de conciencia a nivel general, ya que la defensa de redes y equipos ante un ataque suele ser una tarea más difícil e intensa que la de atacar esas redes y computadoras. Sin embargo, lo que los medios de comunicación y la industria del entretenimiento transmiten es una imagen sesgada e idealizada del atacante y no de quienes trabajan del lado de la defensa, lo cual distorsiona la visión de lo que es la ciberseguridad”, opina.

### La seguridad por diseño: ¿un problema de la formación?

Consultados acerca de si consideran que los contenidos sobre seguridad que se ven durante el proceso de formación los futuros programadores y/o desarrolladores son suficientes para que cuando los profesionales den el salto al mercado laboral estén capacitados para brindar sistemas seguros, para Marc Etienne, “el desarrollo seguro está muy bien enseñado en la actualidad. El problema está en que los desarrolladores necesitan el incentivo para aplicar lo que aprendieron. Los problemas de seguridad en el código deben detectarse durante la revisión del código y deben ser resueltos antes de incluirse en el proyecto. Si los desarrolladores ven que sus códigos siempre son rechazados prestarán más atención y desarrollarán los reflejos apropiados”, opina.

El desarrollo de los profesionales en el campo de la seguridad informática debe ser constante debido a la continua evolución de las amenazas. Si bien en la actualidad existen muchas opciones para desarrollar habilidades suficientes para desempeñarse en este campo, como son las carreras, las especializaciones, las certificaciones e incluso los cursos y el material disponible para estudiar de manera independiente, está claro que no hay una única forma. **XS**



# PREDICCIONES DE SEGURIDAD

## en el año 2020



**A**ctualmente todos vivimos conectados, nuestro Smartphone contiene un montón de información sobre nosotros y, por si acaso, esta información también podemos encontrarla en nuestra Tablet. Además, desde hace tiempo, nuestros objetos electrónicos nos ofrecen nuevas posibilidades gracias al hecho de poder conectarse a internet. Cada vez dependemos más de la tecnología pero hay algo en lo que muchos de nosotros no hemos pensado: la ciberseguridad.

Seguro que muchos pensarán que esto les sucederá, que los ciberataques sólo se hacen a los ordenadores, pero no es cierto. Por ejemplo, ¿alguna vez habéis ido en autobús o has estado en un restaurante o un hotel y has usado la wifi gratuita para no gastar datos móviles? Si la respuesta es afirmativa, ya has puesto en riesgo tu Smartphone y has podido ser el punto de mira para un ciberataque.

La ciberseguridad es un aspecto que debería importarnos a todos, también a las empresas. Es importante empezar a concienciarnos y empezar a tomar medidas.

Presentamos una infografía con 10 predicciones que ha hecho Earl Perkins, vicepresidente de investigación de Gartner, para mejorar la ciberseguridad de las empresas en el futuro:

### 2019

- 1.- El 40% de las implementaciones de la Identidad como Servicio (IDaaS) reemplazarán las implementaciones de identidad y gestión de accesos (IAM) instaladas en las empresas, frente al 10% actual. Este hecho será debido a la dificultad y al coste de la infraestructura IAM.
- 2.- El uso de contraseñas y tokens (dispositivos de seguridad adicional para las transacciones en internet) en casos de riesgo medio se reducirá un 55% debido a la introducción de tecnologías de reconocimiento.

### 2020

- 3.- Hasta el 2020, el 99% de las vulnerabilidades explotadas seguirán siendo aquellas que los profesionales TIC y de seguridad ya conocen desde hace al menos 1 año. Las empresas deben prestar atención en las vulnerabilidades que tienen actualmente para evitar que sean el foco de ataque en un futuro.
- 4.- Un tercio de los ataques exitosos experimentados por las empresas será debido a los recursos TIC sombra. Éstos son los recursos TIC usados dentro de una empresa sin la aprobación o consentimiento del departamento TIC.
- 5.- El 40% de las empresas dedicadas a DevOps protegerán sus aplicaciones adoptando medidas de seguridad como las tecnologías de auto-test, auto-diagnóstico y auto-protección.
- 6.- El 80% de los nuevos contratos basados en los Agentes de Seguridad para el Acceso en la Nube (o CASB: Cloud Access Security Broker), vendrán empaquetados con Firewalls de red, puertas de enlace seguras y plataformas WAF para proteger las aplicaciones web.
- 7.- Más del 25% de los ataques identificados realizados a empresas, implicará al IoT. Según Perkins, los profesionales de seguridad y TIC deberán reservar entre el 5% y el 10% de su gasto para la vigilancia y protección de dispositivos IoT.

Estos 7 puntos ayudarán a que las empresas puedan mejorar su ciberseguridad, pero tienen que tener clara una cosa, tienen que actuar lo antes posible, si han pensado en retrasar la implementación de medidas de seguridad para no interrumpir el negocio, estarán cometiendo un error y puede ser que acaben perdiendo más dinero. **XS**



*La demanda de profesionales en ciberseguridad, uno de los temas con más relevancia para el país*

## Se anuncia la nueva fecha de **Infosecurity México 2020**, será 20 y 21 de mayo



**C**iudad de México.- Infosecurity México 2020, evento que mostrará lo último en conocimiento, tendencias y soluciones para proteger datos informáticos, anunció su próxima celebración que se llevará a cabo el miércoles 20 y el jueves 21 de mayo de este año, en las instalaciones del Centro Citibanamex, ubicado al poniente de la CDMX.

Juan Manuel Rodríguez Ospina, Show Director de Infosecurity México, comentó que este evento de ciberseguridad, se realiza en un entorno en el que existe una creciente cantidad de ataques a un mayor número de industrias o sectores económicos, los cuales resultan en pérdida de información, vulnerabilidad en equipos y sistemas, ataques de ransomware, robos de identidades, entre otros daños.

“Hace cinco años, cuando inició Infosecurity, se hablaba poco de ciberseguridad en el país, y aunque las industrias siguen siendo las mismas, los procesos industriales y de negocios se están digitalizando más, al tiempo que el comercio electrónico está aumentando. Esto implica un riesgo en la integridad de la información y de los equipos y, por ello, queremos reunir en Infosecurity México a las principales marcas del mercado, quienes presentarán sus soluciones y productos, además de que mostraremos tendencias, analizaremos casos y compartiremos conocimiento. Este es un evento para todas las empresas y para los profesionales que manejan datos e información”, explicó Rodríguez Ospina.

La importancia de este evento radica en que la ciberseguridad representa un riesgo para México si no es atendida por el sector público y por el privado. De acuerdo con especialistas, una de las amenazas que enfrentan los países es la creciente dependencia cibernética que aumenta la vulnerabilidad, debido a la posible interrupción de servicios críticos y afectaciones a la infraestructura de información (por ejemplo, internet, satélites, etc.) y redes, causando interrupción generalizada, además de la generación de ciberataques o malware a gran escala que provocarían grandes daños, tensiones geopolíticas o pérdida de confianza en internet, además de la extracción de datos privados u oficiales que tendría lugar a una escala sin precedentes.

Por tal motivo, según el show director de Infosecurity México, el evento busca reunir en un mismo espacio a expositores, visitantes y conferencistas, “Para que podamos seguir desarrollando la industria al tiempo de ofrecer acceso a

pláticas de muy alto nivel, para aprender qué es lo que ha pasado incluso en otras partes del mundo y qué podemos implementar en México”, sobre todo si se considera que el 83% de empresas mexicanas son víctimas de ciberataques por lo menos una vez al año, lo que ubica a nuestro país dentro los primeros diez con más ataques cibernéticos.

Cabe señalar que los organizadores de este evento, propiedad de Reed Exhibitions México, se han preocupado por considerar las experiencias de las ediciones anteriores, que han sido expresadas por sus visitantes, expositores y conferencistas donde, entre otros hallazgos, han encontrado que a nivel general hay una falta de personal especializado en ciberseguridad, debido en parte a que hay una fuerte exigencia por los cambios tan rápidos que suceden en el ámbito informático.

De hecho, según informes, la industria de la ciberseguridad se enfrenta a una crisis de empleo. Se calcula que tan solo la India requerirá dos millones más de profesionales en los próximos dos años, y la estimación mundial es de 3,5 millones para 2022, aunque los salarios se están alineando con estas demandas, con puestos de analista de nivel de posgrado en los Estados Unidos que alcanzan los 100 mil dólares por año, los más altos de todas las profesiones.

“Por ello es que en Infosecurity México queremos impulsar no solo al mercado, sino a la difusión del conocimiento y al apoyo en la formación de personal certificado. Sabemos que hay gente que se está desarrollando porque hay un campo profesional atractivo, pero se necesitan más profesionales para el monitoreo de redes, para los dispositivos móviles, para la infraestructura. Antes, las empresas tenían con un solo analista, hoy necesitan cinco o más”, expresó Juan Manuel Rodríguez, quien agregó que también están acercándose a la academia para complementar su concepto.

Para finalizar, el principal directivo del evento indicó que en la próxima edición buscarán llegar a 6,500 m2 de exposición. “Lo que representa un 20% más que la edición anterior y, aunque la industria crece entre 10% y 15% al año, nosotros buscamos ir más allá de ese porcentaje con base en la presencia de expositores de alto nivel, conferencistas reconocidos mundialmente y una serie de nuevas actividades que ya tenemos programadas y que daremos a conocer pronto”. **IS**

# ÍNDICE DE ANUNCIANTES

## UNIFORMES JR

Portada

## MULTIPROSEG

2da. Forros / Pág. 3

## COMEXA

Pág. 7

## CSCS

Pág. 22

## IP USERGROUP

Pág. 27

## ALAS

Pág. 30

## GECSA

Pág. 33

## GRUPO LK

Pág. 35

## UNIFORMES JR

Pág. 39

## ASIS

Pág. 41

## ZN CORPORATIVO

Pág. 45

## ASUME

Pág. 47

## APRINSA

Pág. 49

## IPS

Pág. 53

## EXPO SEGURIDAD

MÉXICO

Pág. 55

## ORIGINS

Pág. 61

## GEO GLOBAL NETWORK

Pág. 63

## XTREM SECURE

Pág. 71

## RANGER SWAT MÉXICO

Pág 88 -3ra. de Forros

## SEPSISA

Contraportada





# RANGER SWAT MÉXICO



Servicio de transporte a Ejecutivos



Servicio de Custodias



Servicio de GPS y Rastreo Satelital



Servicio de Escoltas



Servicio de Intramuros



# Detecto, Visualizo y Actúo

52 (55) 5347 2741  
[contacto@rangerswat.com.mx](mailto:contacto@rangerswat.com.mx)



Av. Invierno #11, Col. Ángel Zimbrón, Alcaldía Azcapotzalco, C.P. 02910.





*El camino a la excelencia comienza por la seguridad.\**