

m's

más
seguridad
para todos

Marzo 2018 / Año 11 / No. 84

México y América Latina

Precio \$50.00 www.revistamasseguridad.com.mx

Protección integral en Aeropuertos



ESPECIAL

**Instalaciones e infraestructuras
estratégicas**
2da parte

Publicación de:



**PLAY
TO WIN**
**REFUSE
TO LOSE**



Certificado en protección profesional

Inicia: 12 de marzo

CERTIFÍCATE

CON

NOSOTROS



Inicia: 21 de mayo



Inicia: 02 de abril

Acércate a nuestra
área de atención a
socios para más
información.

**POR ÚNICA OCASIÓN
¡NOS CAMBIAMOS!**

Modificamos la sede y fecha de la **Reunión Mensual de abril** para que inicies tu jornada en el marco **Expo Seguridad 2018**.



¡ASISte!

24 de abril

Salón Montejo



**24-26 ABRIL
2018** Ciudad de México
Centro CitiBanamex

ASISte, atiende a las conferencias
que **ASIS** tiene programadas.
Visítanos en el **stand #1053** y
recibe grandes sorpresas.

exposeguridadmexico.com



+52 (55) 5251 0889 ext.14



socios@asis.org.mx



info@asis.org.mx



HUMBERTO MEJÍA HERNÁNDEZ, DSE
DIRECCIÓN GENERAL
humberto@revistamasseguridad.com.mx

MARÍA ANTONIETA JUÁREZ CARREÑO
DIRECCIÓN COMERCIAL Y RELACIONES PÚBLICAS
marieclaire@revistamasseguridad.com.mx

BLANCA L. ARGUETA PALACIOS
COORDINACIÓN DE DISEÑO
diseno@revistamasseguridad.com.mx

LUIS ALONSO NÁJERA GARCÍA
edicion@revistamasseguridad.com.mx

GENARO JUÁREZ
informacion@revistamasseguridad.com.mx
INFORMACIÓN

JOCELYN MEJÍA AGUILAR
PUBLICIDAD
comercial@revistamasseguridad.com.mx

ANDREA SAYURI MEJÍA JUÁREZ
ASISTENCIA A CLIENTES
asistencia@revistamasseguridad.com.mx

ARTURO GARCÍA "EL PROFE"
COLUMNISTA

OSCAR TENORIO COLÓN
ADMINISTRACIÓN Y CONTABILIDAD

NANCY LARA
ALFREDO YUNCOZA
FEDERICO PONCE
PEDRO VENEGAS
GUILLERMO ESPINOSA
ARTICULISTAS INVITADOS

YASSER MARTÍNEZ & GARCÉS ECHEVERRÍA
JURÍDICO

CONTACTO:
Tel/Fax: (52-55) 5527-2279 / 2873-2719
WhatsApp: 551894-7067
asistencia@revistamasseguridad.com.mx
atencion@mhccorporativo.com.mx

SÍGUENOS EN:



Más Seguridad Para Todos. Año 11, No. 84, Marzo 2018. Publicación mensual con domicilio en Poniente 62, número 3710, oficina 5, colonia Obrero Popular, delegación Azcapotzalco, C.P. 02840, México D.F., Tel/Fax: 5527-2279 / 2873-2719. **Editor responsable: Humberto Mejía Hernández.** Certificado de Reserva No.04-2013-090311420000-102 otorgado por el Instituto Nacional del Derecho de Autor. Certificado de Licitud de contenido No.11483 y Certificado de Licitud de Título No.13910, otorgados por la Comisión Calificadora de Publicaciones y Revistas Ilustradas de la Secretaría de Gobernación. Autorización del Registro Postal: PP15-5134 otorgado por Sepomex. Se autoriza la reproducción citando al medio y autor del texto, previo acuerdo por escrito con el editor. Impresa en: **Grupo Mejía Impresores**, calle La Poza No.72, Col. San Lorenzo Totolinga, Naucalpan de Juárez, Estado de México, Tel. (55) 2166-3555.

Aeropuertos más seguros

Al pensar en aeropuertos seguros, probablemente en la memoria del usuario exista un concepto negativo de la gestión y seguridad que se ha implementado en las terminales aéreas de México, esto debido al contexto político – social en el que estamos inmersos, a las fallas estructurales y crímenes cometidos en las inmediaciones de los mismos en los últimos años; esto sin duda envía un mensaje de alerta tanto a las autoridades federales, empresas de seguridad privada y población en general.

Es necesario ser conscientes que un aeropuerto, por sus características y condición de instalación estratégica, representa un riesgo nacional e internacional. No es casualidad que el crimen organizado busque vulnerar la seguridad valiéndose de armas de fuego y el uso negativo de la tecnología.

En el sector aeroportuario nacional, adicionalmente a las obligaciones con la Secretaría de Gobernación que tienen las empresas de seguridad privada, existe el requisito legal por parte de la SCT, que a través de la Dirección General de Aeronáutica Civil (DGAC) regula el cumplimiento de los requisitos nacionales e internacionales para la prestación de servicios complementarios y aeroportuarios de seguridad.

Sin embargo, las empresas de protección intramuros, fabricantes y distribuidores de tecnología, autoridades gubernamentales y miles de personas que dedican su vida al resguardo, avocan su tiempo y esfuerzo a la protección, así como prevención de incidentes a estas inmediaciones con diversas soluciones y procesos.

Para esta labor, la seguridad privada en México tiene estándares de calidad muy elevados, se necesita personal altamente capacitado. Actualmente, en el país existe un enorme porcentaje de elementos de protección intramuros, puede ser incluso más grande que los elementos de seguridad pública.

Por ejemplo, el Aeropuerto Internacional de la Ciudad de México (AICM) registra un flujo de pasajeros que asciende a 41.7 millones cada año, cifra que probablemente crecerá debido a la necesidad de innovación que le corresponde a esta, instalación vital. Otra prueba de ello es el aeropuerto de Cancún, que es el segundo más concurrido de nuestro país, solo después del AICM, inmueble que rápidamente pasó de tener un flujo de usuarios de 7 millones en 1999 a aproximadamente 23 millones anualmente. Para manejar el creciente número de pasajeros, otra terminal se puso en operación este 2018, lo que lo convirtió en la única instalación aérea del territorio mexicano con cuatro terminales.

Nuestro deber como ciudadanos es estar al tanto de la tecnología, fenómeno que ha crecido debido a la búsqueda de la delincuencia por encontrar nuevas formas para atentar contra la seguridad. Es relevante esto en materia aeroportuaria, ya que la ciberseguridad es un de los puntos débiles que no se han atendido del todo cuando se trata de aeropuertos.

En el siguiente trabajo, titulado "Protección integral en aeropuertos", se profundiza en el tema de riesgo en aeropuertos e instalaciones estratégicas en general, brindando información sobre qué necesita el personal para capacitarse, que recursos tecnológicos y con qué empresas se puede recurrir para el resguardo de las mismas, así como la normatividad en el marco jurídico de los requisitos y necesidades para el correcto resguardo de estas instalaciones vitales. **m's**

7 Software
Axis Device
Manager

8 VIOTEC de
Bosch recibe
reconocimiento

10 Nueva
pantalla táctil
TST-100



14 El gran vacío
de México
instalaciones e
infraestructuras
estratégicas
(2da parte)

20 Se elevan
costos de
ciberataques
financieros

24
Protección integral
en aeropuertos

30 Reducción
del 29.5%
en robo al
transporte



38 Cumple FAM 103 años
de existencia

El día que Marco Antonio Sánchez Flores

hizo temblar al gobierno de la CDMX



Hace unos días se dio a conocer el nombre de Marco Antonio Sánchez, pero ¿quién es y qué fue lo que le ocurrió que originó la movilización única de los funcionarios de la Ciudad de México?

23 de enero de 2018 Marco Antonio Sánchez, estudiante de la preparatoria 8, de 17 años de edad, tomaba fotos de un mural en las inmediaciones del Metro Rosario, cuando fue detenido arbitrariamente por cuatro policías que lo acusaron de robo. A partir de ahí comenzó esta terrible historia que ha dado lugar no sólo a una constante indignación social por el actuar de las autoridades involucradas, sino un enfrentamiento y pronunciamiento de estudiantes, padres de familia y organizaciones civiles que exigen un esclarecimiento de los hechos.

La versión de los policías que detuvieron al joven ha sido cambiada constantemente, cosa que no sorprende; las contradicciones y actuaciones policiales dejan mucho que desear y además dejan al descubierto que a pesar de los esfuerzos realizados para mejorar; es decir, capacitar y humanizar a los policías ha sido en balde.

Por otro lado para fortuna de ellos, los videos que deberían proporcionar información clave acerca del caso, en esta ocasión y como suele suceder en estas situaciones, no muestran gran información. Miguel Ángel Mancera, jefe de gobierno de la Ciudad de México salió a confrontarse con los medios de comunicación y a decir que no debería existir manipulación de los videos.

La realidad del caso es que la sociedad mexicana debe quitarse la apatía y en verdad exigir respuestas y un proceso limpio de investigación. Las personas que conocen a Marco Antonio lo describen

como un joven estudiante, simpático, con buenas calificaciones, alejado de problemas; su padre menciona que es un joven normal, cariñoso, que se besan y abrazan, recuerda que daba clases de matemáticas e inglés en su colonia y que había luchado por integrarse a las filas de la máxima casa de estudios en una de sus preparatorias.

Y de pronto, un día normal, de escuela, en la que Marco sale de su casa se despide de sus padres y piensan que se verán por la noche al término de las actividades de cada uno, las cosas cambian drásticamente.

Los padres se despiden de su hijo en condiciones normales, quizá con alegría, quizá con prisa y cuando llega la noche también les llega la angustia de no tener noticias de su vástago, para enterarse después de que fue detenido, pero no llevado a ninguna agencia ministerial, que no les quieren levantar ninguna denuncia hasta que pasen 48 horas y que ese lapso es crucial para poder encontrarlo con vida.

Transcurren los días y no saben si está vivo o muerto; finalmente gracias a la movilización de sus padres y amigos en redes sociales y medios de comunicación, de pronto aparece Marco, en condiciones muy distintas a las que lo recuerdan aparece golpeado, con movimientos torpes, desorientado, en una agencia del Ministerio Público del Estado de México.

El día de hoy es diagnosticado con delirium mixto; según la valoración médica y psicológica que se llevó a cabo en el hospital psiquiátrico infantil, describen a Marco como alguien que no tenía antecedentes quirúrgicos, traumáticos, transfusionales, alérgicos o de toxicomanía; además de haber tenido un desarrollo adecuado en sus entornos familiares, escolares y sociales.

Según sus médicos evaluadores el delirium mixto, es caracterizado por una desorientación en tiempo y espacio, acompañado de ilusiones ópticas y cognitivas, los pacientes pueden confundir la realidad y pensar que tienen alucinaciones.

La angustia que viven sus padres en estos momentos al pensar si su hijo volverá a recuperarse e integrarse a sus acti-



vidades cotidianas, debe ser extenuante; las declaraciones que deben dar constantemente a los medios de comunicación, su lucha continua ante las autoridades de la Ciudad de México, para exigir justicia y cuentas claras del actuar policial, el desgaste físico y emocional de estar de un lado a otro y con guardias en el hospital para el cuidado de su hijo, escuchar una y otra vez las declaraciones de funcionarios del gobierno que dicen: “hicimos lo que está en nuestras manos, estamos haciendo lo mejor, no debería de haber manipulación de videos”, una y otra justificación, historias inventadas y poco creíbles deber ser el motor que sacuda a la sociedad.

No es posible que los jóvenes salgan un día normal a sus actividades y de la nada les cambie su vida, no podemos seguir permitiendo explicaciones de fábulas por parte de funcionarios en los que recae la responsabilidad del actuar de los servidores públicos bajo su mando.

Hace tiempo se “perdieron” 43 estudiantes, de los que nadie ha dado cuenta; marchas, manifestaciones, posturas internacionales, recomendaciones de derechos humanos y un grupo de padres de familia manteniendo un poco de esperanza por su justicia; es lo que resta de ese lamentable caso, lo preocupante e intimidante es la apatía social y gubernamental.

Dejemos de normalizar lo que está ocurriendo en nuestro país, es época de procesos electorales y no exigimos justicia o propuestas tangibles, sino que evaluamos los “spots” publicitarios, quién tiene la mejor canción, hacemos memes de lo que ocurre, bromeamos con las ideologías partidistas, pero ya es tiempo de ocuparnos en mejorar nuestro país. ¿Qué nos hace falta para comenzar?, ¿Qué tal si te reto a cambiar tu entorno?, ¿Qué tal si hoy salimos de nuestra zona de confort?, ¿te atreverías o seguirás no haciendo nada y quejándote de todo? **m's**



*** Nancy Lara / México**

Maestra en Política Criminal. Directora de asesoría y capacitación en CIIS México. Docente en el Diplomado de policías acreditables en el D.F. Coordinadora de Plataforma México en la Coordinación de investigación de campo de la división de investigación de la Policía Federal México. -Asistente del Director General de Secuestros y Extorsiones de Policía Federal México. Productora y conductora programa CIIS a través de www.gooradio.com.mx

m's

Síguenos...



revistamasseguridad



@revmasseguridad



revmasseguridad



Revista Más Seguridad



Revista Más Seguridad



Revista Más Seguridad

www.revistamasseguridad.com.mx

Newsletter **Redes**
semanal **Sociales**

Meade, reto a la incredulidad ciudadana

El hombre sabio no debe abstenerse de participar en el gobierno del Estado, pues es un delito renunciar a ser útil a los necesitados y una cobardía ceder el paso a los indignos. Epicteto

La liturgia seguida en el destape de José Antonio Meade, a la vieja usanza, no dejaba lugar a dudas que lo que buscaba el partido en el poder era apostarle a la mejor carta posible, aun tratándose de un externo.

Lo que vino después de su renuncia como Secretario de Hacienda fueron meros formulismos que a nadie sorprendieron. Inmediatamente después de presentar su renuncia, Meade se reunió con los líderes de la Confederación de Trabajadores de México (CTM), encabezada por Carlos Aceves del Olmo, quien dijo que Meade Kuribreña es “el candidato de la esperanza”; después recibió el respaldo de la Confederación Nacional Campesina (CNC) del PRI acompañado de sus líderes históricos donde hizo un llamado a los agraristas a sembrar la semilla del desarrollo de la paz; el líder de la central campesina del PRI aseguró que los campesinos darán su respaldo a su “amigo” Meade; por último, Arturo Zamora, de la Confederación Nacional de Organizaciones Populares (CNOP), aseguró que el exsecretario de Hacienda “escucha y abandera las causas populares de trabajadores, profesionistas, movimientos, mujeres y jóvenes a los que representa la confederación”.

El cobijo del PRI continuará con la autorización para que se registre en el proceso interno de ese partido y obtenga la candidatura a la Presidencia, ya que cumplió con todos los requisitos. Resulta por demás interesante ver por primera vez al Revolucionario Institucional recibir a un no militante que podría considerarse como independiente, con una trayectoria administrativa de servicio a dos partidos en el poder (PAN y PRI) lo que ya de entrada se ha reflejado en un apoyo singular por parte de panistas y que en el momento de sufragar le sumarán votos.

La reacción de dirigentes políticos no se hizo esperar, AMLO, con su ironía y sarcasmo tradicional, expresó calificativos meramente subjetivos refiriéndose “al regreso de dedazo en su máximo esplendor. El ritual del tapado nos retrasa 25 años en el tiempo. En pleno siglo XXI eso es una vergüenza”.

Margarita Zavala, más mesurada, también se refirió al dedazo como un hecho propio del viejo PRI.

Anaya, en sus desplantes triunfalistas, quiso demostrar que la designación de Meade no era importante para el PAN, a quien da por seguro triunfador en las próximas elecciones con o sin Frente.

No podemos soslayar que los vicios



en las recientes elecciones en el Estado de México y Coahuila fomentaron mayor incredulidad y desazón en la sociedad civil, en ésta última los intentos fallidos de Anaya por anular los comicios en Coahuila, al final fueron su gran derrota, y la postura de Lorenzo Córdova (presidente del Consejo General del INE) apostándole a esa nulidad, generaron mayor desconfianza, la que al final fue resuelta por el Tribunal Electoral del Poder Judicial de la Federación.

Meade, un hombre dedicado a las tareas públicas por más de 20 años, se ha consolidado como un eficiente operador de las finanzas públicas, de las relaciones internacionales y del quehacer administrativo que ha fortalecido la estructura macroeconómica de nuestro país.

El reto es enorme, la ausencia de posiciones de elección popular no será óbice para que en su caso, Meade entienda que las asignaturas pendientes son muchas, pero que, desgraciadamente, desembocan mayormente en los cauces de la seguridad pública y nacional.

Meade precisa de operadores políticos de gran experiencia para enfrentar 18 años de campaña del único político que encabeza las preferencias, según las encuestas actuales, no es para menos, tantos años en campaña lo han formado como un político también a la vieja usanza, me refiero a López Obrador, quien ha sabido aprovechar la ceguera del INE a las violaciones cometidas por Morena, lo que hace suponer que el instituto está en contra del PRI; sería terrible que en las próximas elecciones en julio de 2018 apareciera el fantasma de la anulación.

El Frente al parecer se desmorona. Todavía no está claro quién va a las disputas entre los contendientes y las distancias más que ideológicas se ensanchan a cada momento, PRD en su caso cobijaría a Mancera y supuestamente el PAN a Anaya.

Por otro lado, la aprobación muy dividida de la Ley de Seguridad Interior (proceso legislativo que también vuelve a dividir al PAN) fue turnada con premura desafortunada al Senado después de haber estado en la reserva de las prioridades legislativas por mucho tiempo, a saber, que resultará cuando la ley se apruebe.

En este escenario los grandes perdedores son los partidos, pero más allá de este enredo político la sociedad civil que sigue padeciendo una infame violencia y un crecimiento galopante de la criminalidad. Lo dicho, Meade o quien gane las elecciones, tendrían el gran reto de vencer la “incredulidad ciudadana”, inseguridad, pobreza y liberar a la sociedad de corrupción, impunidad y delincuencia; son tareas ingentes que no caben en los discursos políticos y las ofertas de campaña, acciones contundentes e inmediatas impostergables. **más**



*** Dr. Federico Ponce México**

Ex subprocurador General de la República, catedrático de la Universidad Anáhuac, México-Norte y vicepresidente de la Academia Mexicana de Derecho Internacional.
fpr_online@hotmail.com
@fpr_online

EXP[®] SEGURIDAD M É X I C O

Los países de nuestra región necesitan encaminar de nuevo sus estrategias de seguridad para proteger a sus ciudadanos. Los índices de inseguridad durante el último año son preocupantes, y países que hace poco eran ejemplo de proyectos exitosos de seguridad ciudadana, ahora se han visto lastimados de nuevo por el fenómeno de la violencia.

Para hablar de cifras, cito por ejemplo a Colin Mathers, coordinador de Análisis sobre Salud y Mortalidad en la Organización Mundial de la Salud (OMS), quien el año pasado declaró que América Latina tiene la tasa de homicidios más alta del mundo (hasta 18,6 víctimas por cada 100 mil habitantes), de hecho, según los datos de la OMS analizados en 2017, los 10 países con las tasas más altas de homicidios en el mundo están en Latinoamérica y el Caribe.

Lamentablemente el 2018 no lo empezamos de la mejor manera, los recientes atentados contra policías en Ecuador y Colombia; las inquietantes cifras de homicidios en México y Costa Rica y la floja política contra el crimen de países importantes en la región como Brasil y Argentina son para preocuparse.

Son varios los determinantes que explican la situación de inseguridad en la región: elevados índices de criminalidad, existencia de grupos armados, violaciones a los derechos humanos, impunidad, insuficiencias en el marco jurídico, sistemas penitenciarios inoperantes, ineficacia de las instituciones policiales, corrupción, desconfianza ciudadana, ausencia de la cultura de la legalidad, la delincuencia organizada y la ciberdelincuencia.

Además, a este escenario debemos sumarle la situación contextual de Latinoamérica: una región en la que existe una alta concentración de personas de bajos recursos en zonas urbanas, con pocas oportunidades de empleo bien remunerado y altos niveles de inequidad que deterioran la calidad de vida y mantienen altas las tasas de criminalidad, victimización y violencia.

Para hacer frente a este panorama se necesita una visión más amplia que incluya objetivos concretos, aplicación e inversión inteligente de los recursos en seguridad, es decir, orientar mejor el gasto, imponer controles, objetivos e indicadores, eliminar despilfarros y sobre todo, atacar la corrupción.

Por ejemplo, la integración tecnológica supone uno de los mayores retos en la industria de la seguridad en América Latina. El 2017 fue un buen año en materia de fortalecimiento de los equipos humanos de seguridad privada y fuerza pública,

así como en adopción de nuevas tecnologías de vigilancia urbana. No obstante, siguen siendo incipientes o marginales las propuestas, privadas o públicas, que se basen en la integración de nuevas tecnologías.

En México, particularmente, si bien existe una Ley de Seguridad Privada en el contexto federal, no existe una ley general con alcance nacional. Es decir,



Mario Arroyo Juárez, rector del Instituto Iberoamericano de Liderazgo en Seguridad

Reemprender el camino de la seguridad, la tarea de América Latina para 2018



existen 32 legislaciones locales que le restan competitividad al sector y carecemos de estándares o normas que guíen los diferentes ámbitos de la seguridad. Apenas en 2017 el país emitió una normatividad para videovigilancia urbana que, además de operar con presupuesto público, ha dado un impulso a la industria gracias a las iniciativas que emergen a partir de dicha normatividad: mayor inversión, aumento en el número de cámaras instaladas, entre otras propuestas.

Si bien es cierto que existen condiciones y proyectos en curso que pretenden incorporar diversos sistemas de comunicación existentes, tecnologías inminentes y emergentes, es fundamental que quienes trabajamos por la industria de la seguridad en América Latina asumamos desafíos esenciales que contribuyan al crecimiento y el fortalecimiento de la misma.

Un buen ejemplo en esta materia es Ecuador, cuyo Plan Cuadrante, que sumado a la inversión en equipos tanto de seguridad física como electrónica, han reducido su tasa de homicidios, la cual lleva varios años a la baja; además, cabe mencionar su Servicio Integrado de Seguridad ECU 911, el cual ganó el Premio ALAS a la seguridad en 2017 por ser un sistema integrado de vigilancia ejemplar para la región.

En definitiva, proponemos los siguientes retos, pero los invitamos a nutrir la discusión y a ofrecer nuevas miradas sobre la mejor forma de impulsar la industria: gestionar la seguridad urbana a través de la cooperación entre el gobierno, el sector privado y la sociedad civil; crear una cultura de prevención y ambiente seguro para todos los habitantes por medio del apoyo a las autoridades locales y contar con plataformas de tecnologías de la información y comunicación que se conviertan en el soporte material para el despliegue de estrategias, programas y acciones.

Como vocero responsable de relaciones públicas con el gobierno (México) de Expo Seguridad México y Expo Seguridad Industrial, los invito a participar de estos espacios, los cuales considero son la mejor plataforma para aprender las mejores prácticas y experiencias, buenas o malas, además de las mejores soluciones, allí encontrarán a los profesionales que tienen el conocimiento de vanguardia de todo el planeta, tanto para la esfera pública como en el sector privado.

Si quieres conocer todas las soluciones y productos de seguridad y seguridad industrial que ofrece Expo Seguridad México y Expo Seguridad Industrial, regístrate sin costo para asistir a nuestras versiones 2018. **m's**

Registro ESM

<https://exposeguridad.infoexpo.com.mx/2018/ae/web/codigo/FXDG58087>

Registro ESI

<https://esi.infoexpo.com.mx/2018/ae/web/codigo/KHYO91249>



Device Manager

La amplia gama de funciones de administración de equipos incluye:

- Asignación automática de direcciones IP
- Instalación, configuración, reemplazo y actualización de cualquier dispositivo
- Copiar configuraciones entre miles de dispositivos
- Conexión a múltiples servidores/sistemas
- Puntos de restauración y configuración de fábrica pre-determinada
- Actualización del firmware del dispositivo
- Administración y actualización de cuentas de usuario y contraseñas
- Implementación, gestión y renovación de certificados HTTPS e IEEE 802.1x

Ciberseguridad proactiva

AXIS Device Manager ofrece mejoras significativas en la seguridad de los dispositivos al permitir la administración centralizada de cuentas, contraseñas y certificados, así como el refuerzo a los dispositivos de acuerdo con la guía de Axis. Esto permite que sea más sencillo y rentable para los instaladores y administradores de sistemas gestionar e implementar proactivamente características. **ms**

Axis Communications anuncia el lanzamiento de este software integral de administración, que ofrece una forma sencilla, rentable y segura de gestionar todas las tareas principales de instalación y administración de dispositivos operativos. Facilita la protección proactiva de dispositivos y redes. Su uso es adecuado para administrar el robusto portafolio de cámaras de red Axis, controles de acceso y dispositivos de audio en un mismo sitio, o diferentes equipos localizados en diversos espacios.

El nuevo desarrollo de la plataforma de software AXIS Camera Management, ahora AXIS Device Manager, demuestra el compromiso de la empresa de ayudar a sus clientes a lograr operaciones sencillas y rentables de instalación, así como a proteger proactivamente sus dispositivos y redes contra riesgos de ciberseguridad.

Nueva función Wisenet extraLUX permite capturar imágenes nocturnas a color

Hanwha Techwin, anunció que extraLUX, una función referente en la industria para entornos con muy poca luz, ahora estará disponible en toda la gama de cámaras de su popular serie X. Gracias al potente circuito integrado auxiliar Wisenet 5 y a la tecnología de procesamiento, las cámaras que tienen la función extraLUX capturan imágenes nítidas y de colores naturales en condiciones de poca luz sin ledes IR, en cualquier entorno y hora del día.

Usando objetivos varifocales motorizados Hanwha con un paso (f-stop) de .94 y un sensor CMOS de 1/2", la función extraLUX permite captar imágenes más nítidas y claras que nunca.

Las cámaras de las series X XNB-6005, XNO-6085R (tipo bala), XNV-6085 (domo para exteriores) y XND-6085 (domo para interiores) ya cuentan con la función extraLUX. Estas cámaras tienen objetivos varifocales motorizados (4.1 mm ~ 16.4 mm) que permitirán al usuario hacer acercamientos/alejamientos y enfoques de forma remota. Los productos de las series XND-6085 y XNV-6085 cuentan con la función PTRZ completa (movimiento horizontal, vertical, zoom y rotación), la cual permite mejorar su control y posicionamiento.

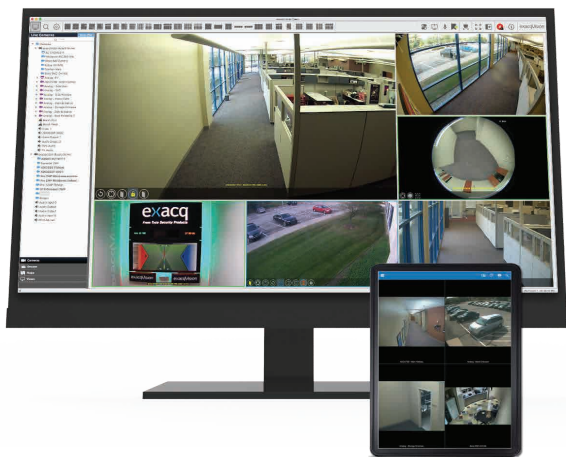


Imágenes a más claras y nítidas en situaciones de muy poca luz

La cámara tipo caja XNB-6005 también cuenta con un sensor de 1/2" y una amplia selección de configuraciones de objetivos, entre otros, objetivos inteligentes CS (I-CS) que comunican su posición, la apertura de su iris y su enfoque directamente a la cámara para obtener ajustes de imagen más precisos y rápidos.

Además, las cámaras XNO-6085R, XNV-6085, XND-6085 y XNB-6005 tienen un sensor giroscópico incorporado para la estabilización de la imagen digital que permite obtener imágenes estables y más precisas cuando las cámaras se ponen en funcionamiento en un entorno que provoque que la cámara se sacuda. Para iluminar objetos distantes, la XNO-6085R tiene un infrarrojo incorporado con un alcance de 229 pies (70 m).

Las cámaras de la serie Wisenet X cuentan con la tecnología Wisenet 5 que ofrece 150dB de amplio rango dinámico (WDR), un completo paquete de herramientas de análisis que no requieren licencia, aumento de la seguridad del dispositivo y mejor compresión y transferencia de datos gracias a la tecnología de compresión Wi-seStream II de Hanwha y al estándar de codificación H.265 de alta eficiencia. **ms**



exacqVision ofrece combinación superior

Johnson Controls presentó la reciente versión del sistema de gestión de video (VMS) exacqVision (9.0), la cual incorpora importantes características que contribuyen a garantizar la integridad general del entorno de seguridad del cliente, además de ofrecer herramientas que facilitan la mitigación de eventos de seguridad.

exacqVision es reconocido por su capacidad de ofrecer información crítica sobre la salud y el desempeño del VMS. Proporciona ese mismo enfoque para los paneles de control de acceso e intrusión, ya que incorpora alarmas de integridad que informan al usuario ante potenciales problemas para garantizar que el sistema mantenga un alto nivel de desempeño.

Con las nuevas integraciones con las cámaras Illustra Pro con funcionalidades analíticas, los usuarios pueden monitorear grandes áreas basándose en determinados comportamientos (como la presencia de merodeadores), mientras que las potentes herramientas de búsqueda permiten buscar fácilmente eventos importantes a partir de metadatos.

Además, los administradores ahora pueden definir mejor los privilegios de visualización en tiempo real y de búsqueda de videos para garantizar que solo los usuarios adecuados tengan acceso a los videos de vigilancia. Por ejemplo, a un usuario se le puede otorgar acceso al video en vivo de una cámara específica, pero restringir el acceso al video grabado.

También se realizaron mejoras en los grupos de usuarios de Enterprise System Manager 5.4, que saldrá al mercado junto con exacqVision 9.0, que permiten asignar a los usuarios a múltiples grupos, cada uno con diferentes privilegios. De esta forma, se busca cumplir con las demandas de grandes organizaciones que necesitan asignar usuarios a múltiples grupos en servidores distintos.

Por último, exacqVision 9.0 simplifica el proceso de configuración agregando campos de información adicionales a la página de entradas y salidas de audio, alarmas y activadores. **m's**

AVIOTEC de Bosch

recibe primer reconocimiento VdS a nivel mundial

La solución de detección de incendios mediante video AVIOTEC de Bosch, recibió el primer reconocimiento mundial VdS Damage Prevention GmbH (VdS) como cámara de video automática para la vigilancia visual de incendios, con el número G217090. La VdS es una renombrada institución independiente en el ámbito de la seguridad y la protección empresarial, y un organismo alineado con los estándares internacionales de seguridad. El sello de calidad VdS se considera un criterio de inversión importante y a menudo sirve como base para una posterior estandarización EN.

VdS ha desarrollado un sofisticado procedimiento de prueba para la detección de incendios mediante video que incorpora las directrices establecidas VdS 2203, los "Requisitos para el software de protección contra incendios" y los "Requisitos para la prueba de detectores de llama". AVIOTEC IP starlight 8000 es el primer producto a nivel mundial que ha pasado estas pruebas. No solo se puso a prueba su inmunidad frente a falsas alarmas, sino también su funcionalidad a largo plazo en lo referido a seguridad y fiabilidad bajo condiciones ambientales desafiantes, así como las influencias mecánicas operacionales.

La luz es más rápida que el humo

La ventaja decisiva de la detección de incendios mediante video es su velocidad. Detecta visualmente los incendios directamente en la fuente, independientemente de la migración del humo al detector. Philipp Mondrik, director de proyecto de VdS, también subraya su velocidad de detección: "En general, nuestras pruebas mostraron que esta solución de detección de incendios mediante video, en condiciones ideales se puede definir como la "detección de incendios más rápida".

Bosch supera el importante criterio de prueba de inmunidad contra falsas alarmas con nota, ya que los algoritmos de detección de incendios desarrollados sobre la base de un modelo físico de humo y llama, definen con precisión propiedades específicas del fuego y las distinguen claramente de posibles valores de perturbación. Por lo tanto, AVIOTEC no solo ofrece una solución muy rápida, sino también fiable y robusta para la detección de incendios mediante video, y desde el 16 de noviembre de 2017 cuenta también con la aprobación VdS. **m's**





24-26 ABRIL
2018 Ciudad de México
Centro Citibanamex

Asiste sin ningún costo. Regístrate hoy en: www.exposeguridadmexico.com

*Registro sin costo hasta el 20 de abril. No incluye conferencias



ENCUENTRA



La mayor oferta de productos y soluciones de seguridad.



INTERÁCTUA



Más de 350 expositores y 11,500 m2 de exhibición



DESARRÓLLATE



Conferencias especializadas en materia de seguridad

Descarga nuestra APP móvil

Mantente informado sobre nuestros ciclos de conferencias, actividades, nuevos expositores, productos y más.

Expo Seguridad



Visita nuestro blog

Conoce las últimas tendencias del mercado, nuevos productos y novedades de la expo.

blog.exposeguridadmexico.com

Patrocinadores Corporativos



Patrocinadores Fundadores



www.exposeguridadmexico.com

Powered by



Organizado por



Reed Exhibitions®

El logotipo de Expo Seguridad México es una marca de RELX Intellectual Properties SA, objeto de uso bajo licencia.



TelepathyTM,

software de mapeo
gráfico y edición

La empresa especialista en el control de acceso, Keri Systems, presentó su potente y nuevo cliente de mapeo, comando y control gráfico que será proporcionado de forma gratuita con la compra de Doors.NETTM. Telepathy, permite a los usuarios trazar gráficamente en una representación "tipo-mapa" de su instalación tanto accesos, puntos de alarma, salidas y equipamientos de control.

Los iconos personalizables pueden adaptarse a sus mapas de accesos para representar su ubicación física. Una vez vinculados al hardware, se pueden activar con un clic del mouse para interactuar con una variedad de amenazas e incorporar alertas de sonido para garantizar que nunca pueda perder un evento.

Características principales:

- Proporciona una visualización de vistas aéreas, exteriores o transversales de sus edificios junto con planos de cada piso para proporcionar una visualización completa del sistema.
- Los iconos de estado interactivos notifican a los operadores sobre importantes condiciones de alertas predefinidas.
- Control de hardware a través de iconos que están vinculados a puertas, entradas etc.



- Capaz de iniciar acciones pre-configuradas con el administrador de situaciones como desbloqueo global o cierre de emergencia.
- Interfaces con control de acceso, pasar lista de personal y alistamiento, video, intrusiones, y sistemas de extinción.
- Administración de varios sitios desde un mismo software.
- Visualización e interacción sobre alertas actuales.
- Ver información histórica de un evento.
- Iconos de sensores dinámicos personalizables.
- Alertas animadas con sonido para garantizar que no se pierda un evento, y es posible configuración para requerir una contraseña.
- Planos de piso interactivos.
- Interfaz con lectores de asistencia.
- Ventanas acoplables para uso de monitores múltiples.

TelepathyTM será un gran éxito con aquellas instancias que controlan un gran número de instalaciones y requieren controlar los accesos, como instancias gubernamentales, penitenciarios o de educación. **m's**



Nueva pantalla táctil TST-100

Johnson Controls presentó su terminal multifuncional de pantalla táctil TST-100 de Software House, proporcionando al usuario final una mejor experiencia de control en los puntos de acceso. Con una interfaz de usuario intuitiva con pantalla táctil, su funcionalidad de intrusión nativa, la compatibilidad con controladores de acceso tradicionales y los nuevos modelos IP de Software House, le agrega valor al sistema de control de acceso al permitirles a sus usuarios tener más flexibilidad y control al nivel de la lectora.

Cuenta con una pantalla táctil LCD de 4.3" que muestra una variedad de íconos a color y menús de comando personalizados. Esto les proporciona una respuesta rápida y fácil a los usuarios finales, y permite que los guardias y otras personas puedan armar y desarmar las zonas de intrusión, y dar comandos personalizados directamente en la puerta.

Como incluye el minicabezal de lectura multitecnología 5127 de HID Global, la terminal de pantalla táctil admite una variedad de tecnologías de tarjetas inteligentes de alta seguridad, como HID iCLASS SE y iCLASS Seos, entre otras. También utiliza el protocolo RS485 encriptado de alta velocidad para entablar comunicaciones seguras con un controlador IP. Esto hace que la terminal sea ideal para instalaciones sanitarias, instituciones educativas, aeropuertos y otros entornos críticos de seguridad donde no se permite la conectividad de red directamente con una lectora en el lado no seguro.

Encriptado de alta velocidad para entablar comunicaciones seguras con un controlador IP. Esto hace que la terminal sea ideal para instalaciones sanitarias, instituciones educativas, aeropuertos y otros entornos críticos de seguridad donde no se permite la conectividad de red directamente con una lectora en el lado no seguro.

La terminal de pantalla táctil TST-100 también ofrece características de control de intrusión en la puerta sin la necesidad de incorporar una interfaz dedicada, lo que les permite a los usuarios finales visualizar el armado y desarmado de las zonas de intrusión en el dispositivo. Un menú de comando también permite que los usuarios finales generen comandos de teclas personalizadas para el sistema de intrusión. La programación de la lectora incluye el protocolo de mensajería confiable (RM) de Johnson Controls que facilita la compatibilidad con cualquier controlador de acceso iSTAR. Esta terminal se puede incorporar a cualquier plataforma de Software House —tanto al sistema de administración de seguridad y eventos C•CURE 9000— como al cliente unificado victor.

La terminal de pantalla táctil TST-100 incluye el módulo IP-ACM, el módulo de control de acceso Ethernet basado en IP de Software House, que, cuando está instalado cerca de la

EVOLUCIÓN, SEGURIDAD Y CULTURA DE LA PROTECCIÓN



15 DE MARZO



Mtro. Raúl Sánchez Jiménez
FISCAL GENERAL DEL ESTADO DE JALISCO



Lic. Joel Juárez Blanco
DIRECTOR GENERAL GSI SEGURIDAD PRIVADA
"Conocer Normas de Competencia"



María Teresa Septien, DSE
DIRECTORA EJECUTIVA AFIMAC LATINOAMERICA
"Factor humano como elemento clave en la evolución y cultura de la seguridad"



Mtro. Bernardo Gómez del Campo Díaz Barreiro
DIRECTOR DE SERVICIOS ESPECIALES DE SEGURIDAD PARA PROTECCIÓN DE TESTIGOS DE LA POLICÍA FEDERAL MISTERIAL DE LA PGR
"Seguridad Humana, ¿El último escalón para la paz en México?"



Mtro. Carlos Seoane Noroña
SOCIO DIRECTOR DE SEOANE CONSULTING GROUP
"Entendiendo el fenómeno del tirador activo: una amenaza creciente"

16 DE MARZO



Ing. Alberto Friedmann R.
CEO CODECO MÉXICO / DIRECTOR GRAL. ADJUNTO PROSA
"Ciberseguridad, la protección actual"



Saúl Mendoza Hernández
MEDALLISTA PARALÍMPICO
"Más allá de los límites"



Eduardo Hernández Ruiz
GENERAL MANAGER SUPPLY CHAIN SECURITY COUNCIL
"El estándar ISO 28000: Supply Chain Security Management en la protección a ciclos productivos"



Ing. Martha Beatriz Manrique Gómez
ASESORÍA BLINDAJE DE VEHÍCULOS Y MATERIALES ANTIBALA
"Cómo adquirir correctamente un vehículo blindado"

PATROCINADORES



ORGANISMOS DE APOYO



15 MARZO 16 EXPO GUADALAJARA

¡YA
FALTA POCO
REGÍSTRATE
EN LÍNEA!

www.expoproteccion.com

.....

**COSTO DE
CONGRESO \$5,500 + IVA**
(Acceso a todas las conferencias, material, comidas,
coffee break, constancia con valor curricular)

.....

SOCIOS
COPARMEX, CANACO, ASIS, CNSP

25% DE DESCUENTO



**EXPO[®]
PROTECCIÓN**
2018

direccion@expoproteccion.com
ventas@expoproteccion.com

.....

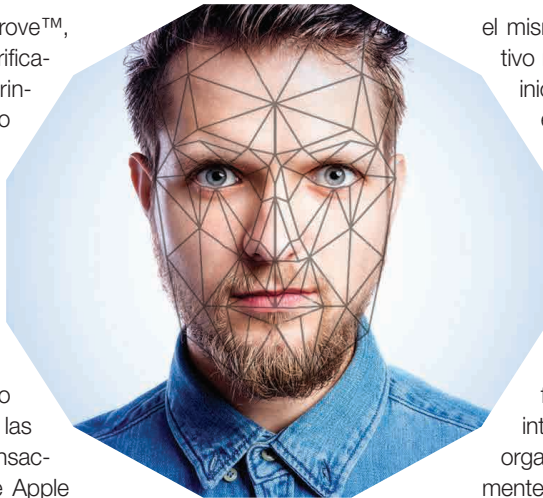
01 800 890 7414

HID Global brinda soporte al reconocimiento facial FaceID del iPhone X

HID Global®, anunció que HID Approve™, su plataforma de autenticación y verificación móvil de dos factores, ahora brinda soporte al sistema de reconocimiento facial Face ID, del iPhone X de Apple. La empresa espera que el reconocimiento facial desempeñe un papel cada vez más importante en sus ofertas de autenticación, junto con la detección de amenazas y fraudes.

El reconocimiento facial es una herramienta que ofrece el nuevo teléfono iPhone X de Apple para proteger el acceso a la banca en línea o a la banca móvil y las firmas digitales que se emplean en las transacciones bancarias. La función Face ID de Apple también se puede usar para proteger el acceso remoto a datos y aplicaciones de empleados. Ahora los clientes de HID Global pueden implementar Face ID de manera fácil, utilizando la plataforma de autenticación móvil de la compañía, ya sea como una aplicación integral o directamente incorporada a las aplicaciones corporativas existentes utilizando el kit de desarrollo de software de HID Approve (SDK).

Asimismo, la tecnología Face ID permite que, de forma segura, los usuarios del iPhone X puedan realizar pagos desde su teléfono celular y realizar desbloques y autenticaciones con



el mismo. Lo anterior significa que este dispositivo no cuenta con lector de huella ni botón de inicio, basta con la cara del usuario para que el equipo se desbloquee, toda vez que con su tecnología de reconocimiento facial es posible que, mirando la pantalla gracias a un sistema de cámara e infrarrojos, se reconozcan las facciones del usuario autorizado para manipular el celular.

HID Global tiene la capacidad de combinar la tecnología de reconocimiento facial con la detección de amenazas y otra inteligencia basada en riesgos para que las organizaciones puedan reconocer más rápidamente posibles fraudes o usos indebidos, al tiempo que mejoran y personalizan la experiencia de los usuarios. La compañía está desarrollando nuevas prestaciones que facilitan a las instituciones financieras la detección de cibercrimen tales como programas maliciosos, programas de secuestro, hacking de aplicaciones, transacciones y mensajes electrónicos fraudulentos. El reconocimiento facial desempeñará un papel fundamental en la implementación de estas prestaciones, pues permite obtener datos valiosos para ayudar a potenciar el análisis predictivo y otras funciones de inteligencia artificial (IA). **m's**

Arcos detectores de metales, solución en franca expansión



La empresa Global Protection, especializada en la implementación de dispositivos de seguridad en eventos masivos e instalaciones que requieren un estricto control de acceso, presenta al mercado mexicano una de sus más recientes incorporaciones a su importante portafolio, el modelo PD 6500i de la reconocida marca Garrett, especialista en productos de detección de metales de arco.

El Garrett PD 6500i es un arco multizona de detección exacta que identifica entre otras cosas si el objetivo está en el lado derecho, centro o izquierdo de la persona que lo atraviesa, además de la altura exacta en la que se encuentra el objeto; e incluso es capaz de discernir entre objetos no perjudiciales, como monedas o llaves.

Aunque su uso inicialmente fue pensado para instalaciones federales y en aeropuertos, los arcos detectores de metales se han requerido en cada vez más variedad de establecimientos como escuelas, sitios de espectáculos y edificios

corporativos. Este sistema de control de acceso también es usado en fábricas y bodegas con el fin de evitar mermas, y puede ser también utilizado en terminales de transportes colectivo como el metro de la Ciudad de México, salas de justicia, sitios históricos, y en eventos masivos como, estadios deportivos y conciertos.

La funcionalidad multizona del Garrett PD 6500i puede detectar si un individuo pasa por la entrada del detector con un arma escondida en sus tobillos. Pues el detector multizona podrá identificar la ubicación del objetivo, ya sea del lado izquierdo o derecho del individuo, pues puede indicar la ubicación específica, de pies a cabeza y del lado izquierdo o derecho. Cuenta con la capacidad de ser añadido a puntos de control existentes sin tener que sustituir otras unidades de terceros. Incluye múltiples canales y 2.300 frecuencias de operación seleccionables.

Su diseño le permite indicar la ubicación del objetivo rápidamente lo que es determinante para que el personal de seguridad pueda responder eficazmente ante grandes multitudes donde se requiere de una capacidad mayor de control de acceso inmediato. **m's**

OPTEX GROUP OF COMPANIES: YOUR IDEAL PARTNER IN PROVIDING ADVANCED SECURITY AND SAFETY SOLUTIONS FOR YOUR BUSINESS

Grupo Optex ofrece a sus clientes, líderes mundiales expertos en la protección perimetral, sensores por fibra óptica, detectores de intrusión, incluyendo tecnologías Infrarrojas, láser y radar, e iluminadores LED para CCTV.

Nuestras soluciones reflejan la más alta tecnología y calidad con diversas opciones de integración a sistemas cableados, sistemas inalámbricos y plataformas IP.

FUERA DEL PERIMETRO O EN AREAS VIRTUALES

Tecnologías Radar y Laser para detectar amenazas de intrusión en Aire, Tierra o Agua, antes de que lleguen a la primera línea de defensa
(incluye detección de drones)



REVEAL



REDSKAN

ILUMINACION LED DE ALTO RENDIMIENTO

Soluciones inteligentes de Iluminación para Seguridad y CCTV. Iluminación Infrarroja, Luz Blanca, PoE, IP y Ex-proof (aplicaciones en ambientes peligrosos)



PRIMERA LINEA DE DEFENSA

Detectar intrusión en la cerca, barda o concertina perimetral con Sistema de Cable Sensor por Fibra Óptica.

Fiber SenSys
Fiber Defender™



OTRAS AREAS PERIMETRALES

Soluciones flexibles para detectar intrusión con torres fotoeléctricas Infrarrojas (inalámbrico o cableado)



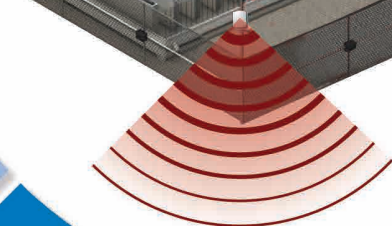
DETECCION EN AREAS INTERMEDIAS, ABIERTAS O INTERIORES

Soluciones de mediano y largo alcance con microondas, tecnologías inteligentes con láser o infrarrojo pasivo.



CONTROL Y CONTABILIDAD DE PERSONAS Y VEHICULOS

Soluciones de alta precisión por conteo del flujo de personal, visitantes, clientes, etc., en lugares públicos, tiendas o transportación



El gran vacío de México

Riesgo de Seguridad Nacional latente en instalaciones e infraestructuras estratégicas

Redacción M'S / @revmasseguridad

Parte 2 de 2

Como se mencionó en la edición 83 de **Más Seguridad**, hablar de infraestructuras estratégicas y críticas en México no es fácil. El correcto funcionamiento de estas instalaciones es vital para el sustento y desarrollo del país, puesto a que resguardan información y datos cruciales sobre la nación, además de las vidas que están en peligro latente si no se tiene la preparación necesaria para responder a las diferentes situaciones que pueden presentarse; debido a esto, dichos organismos necesitan de protección, vigilancia especializada y personalizada de acuerdo a sus necesidades y problemáticas específicas, ya que si sufren algún tipo de daño o dejan de funcionar, esto puede ocasionar una pérdida económica al país y a la seguridad nacional-

"Las infraestructuras estratégicas y críticas en México, tienen una similitud a los órganos humanos, como tales, cada órgano se enferma de diferentes cosas, y es que, al tratarse de instalaciones o de entrañas, tendemos a comprar la medicina a pesar de no estar seguro de cuál es la enferme-

dad", comenta **Manuel Zamudio**, gerente de cuentas nacionales en Axis Communications y especialista en seguridad.

En resumen, el subdirector de Seguridad Física de la Comisión Federal de Electricidad, **Capitán Gustavo Cuevas Gutiérrez**, durante la sesión de febrero de ASIS Capítulo México, mencionó algunos datos relevantes sobre el tema:

México cuenta con más 3 mil instalaciones estratégicas de las cuales el 47% corresponden a PEMEX, 17% a CONAGUA y 14% a la CFE, sin embargo, muchas de ellas tienen responsabilidades compartidas en cuanto a la protección de las instalaciones.

Si bien existen leyes que dan sustento jurídico a la seguridad de las instalaciones estratégicas, existen problemas político-sociales que nos llevan a que ello sea más

complejo, esto impide la adecuada protección, crecimiento y desarrollo de más instalaciones estratégicas, haciendo que no cumplan con los requisitos necesarios para ser una instalación vital.

A pesar de ser inmuebles en potencia que resultan relevantes para el desarrollo del país, existen obras que se cancelaron por motivos políticos, ejemplos de ello, fueron las intervenciones a instalaciones por parte de grupos defensores del medio ambiente en estados como Chiapas, Puebla y Guerrero; esto en palabras del subdirector de la CFE.

También existe la toma de instalaciones por parte de sindicatos y grupos sociales que por intereses grupales, realizan bloqueos que frenan la operación de los inmuebles, tal fue el caso de una planta generadora de energía a base de carbono ubicada en los límites de Michoacán, que en 2013 fue tomada por un grupo social bajo el argumento del daño que este inmueble podía ocasionar al medio ambiente, en este caso en particular, nunca hubo una intervención del Estado. Fue de una gravedad

particularmente alarmante, ya que esta instalación vital genera poco más del 3% de la energía del sistema eléctrico nacional, puntualiza el Capitán Cuevas Gutiérrez.

Lo anterior provocó, que más de 250 mil clientes se quedaran sin energía, dejando a zonas reducidas de algunos poblados, tuvieron que esperar más de 12 horas para la reinstalación del servicio. Esto evidenció la falta de seguridad en algunas instalaciones.

Infraestructuras críticas: Protocolos y metodología para la seguridad

Arturo García, Experto en seguridad de la Información, y catedrático en la materia, indica que las infraestructuras críticas deben ser protegidas a través del "modelo cebolla" el cual consiste en atravesar diferentes capas, es decir de afuera hacia adentro lo que sería protección perimetral, instalaciones de detección de intrusos pasando por segmentación de redes, parches, hasta códigos de aplicaciones. "En una instalación de esta magnitud el resguardo debería ser más riguroso y sobre todo respaldado por la Ley.

En nuestro país no hay una buena legislación respecto a la Seguridad Nacional tanto de la información, cibernética, de instalaciones o infraestructuras, esto también depende del personal que esté a cargo de las mismas. Tampoco existen certificaciones que avalen a una persona para ser director de seguridad de estos recintos", afirma.

Al respecto de este problema es necesario establecer un esquema normativo, que se encuentre dentro de la Seguridad Nacional de México. **Manuel Sánchez Merelo** agrega que es prudente dentro del proyecto plantear:

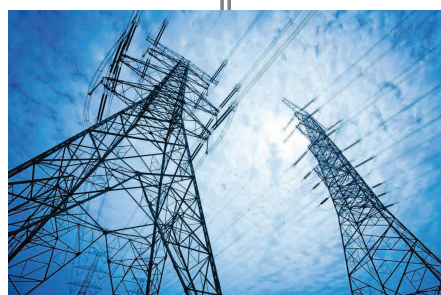
- Colaboración administrativa: el esquema normativo y legislativo se deberá desarrollar en dos aproximaciones posibles que son, la reglamentación, el diálogo y cooperación en asociación público-privada para compartir información, capacidad de interlocución y reacción, análisis de interdependencias, guías, estándares y buenas prácticas, así como para realizar ejercicios y simulacros sectoriales.
- Planes estratégicos sectoriales: serán los instrumentos de estudio y planificación con alcance en todo el territorio nacional, que permitirán conocer, en cada uno de los sectores contemplados cuáles son los servicios esenciales proporcionados a la sociedad, el funcionamiento general de éstos, las vulnerabilidades del sistema, las consecuencias potenciales de su inactividad y las medidas estratégicas necesarias para su mantenimiento.
- Planes de seguridad de los operadores: serán los documentos estratégicos que definan las políticas generales de los operadores críticos para garantizar la seguridad del conjunto de instalaciones o sistemas de su gestión. Deberán ser



elaborados por el propio operador en el plazo de seis meses a partir de la notificación de la resolución de su designación y debe presentarlo para evaluación.

Planes de protección específicos: serán los documentos operativos donde se deben definir las medidas concretas ya adoptadas, así como las que se irán implementando por los operadores críticos para garantizar la seguridad integral (física y lógica) de sus infraestructuras determinadas como críticas.

- Planes de apoyo operativo: serán los documentos donde se deben plasmar las medidas concretas a poner en marcha por las administraciones públicas en apoyo de los operadores críticos, para la mejor protección de las designadas como infraestructuras críticas y que su elaboración corresponde al cuerpo de policial estatal, o en su caso autonómico, con competencia en la demarcación territorial de que se trate, para cada una de las infraestructuras críticas dotadas de un plan de protección específico y sobre la base a los datos contenidos en éste.



Al enmarcar los puntos dentro de un enfoque de Seguridad Integral (física y lógica o cibernética) la misión fundamental es coordinar las actividades de los agentes implicados en la protección de infraestructuras críticas, tanto en el sector público como el privado.

En resumen, el desarrollo normativo y legislativo permitirá identificar los servicios esenciales prestados a la sociedad por los determinados como sectores estratégicos y críticos, su funcionamiento, las principales amenazas y sus principales vulnerabilidades bajo un enfoque integral de la seguridad de las infraestructuras frente a cualquier tipo de amenaza.

Mejorar instalaciones e infraestructuras estratégicas con soluciones tecnológicas

A pesar de que la seguridad a instalaciones e infraestructuras estratégicas de México es un tema escaso, no se puede negar la existencia de empresas multinacionales que brindan servicios para resguardar a estos recintos, principalmente con herramientas y tecnología. Se ha tornado como una situación bastante abstracta por la significación que tiene en la nación, ya que son las que rigen adecuadamente al país porque abastecen de energía, agua, alimentos, telecomunicaciones, y cada subrama que estas desprenden de igual manera son de suma importancia, como ya se ha mencionado.

Axis Communications y su compromiso con la videovigilancia

La empresa especializada en videovigilancia IP de última generación, ha mejorado la seguridad de millones de personas en todo el planeta por su innovación en tecnología digital.

Manuel Zamudio, gerente de cuentas nacionales en Axis Communications, menciona que la empresa brinda herramientas pero el usuario es quien decide cómo utilizarlas, si no existe un análisis previo cualquier dispositivo que sea instalado podría representar un riesgo, es por ello la necesidad de un consultor experimentado para cada situación de seguridad física, que sepa exactamente el porqué de cada producto en el lugar específico y con ello se da paso a la ingeniería, arquitectura, conectividad, enlaces, distancias, tipos de computadoras y procesadores, formatos en bases de datos, seguridad en la información, a quién y de qué manera se verificará de dichos cambios.

Algunas de estas medidas se pueden llevar a cabo a través de una grabación de video de alta resolución para condiciones que se requieran atacar, esto es de gran utilidad ya que de esta forma se pueden saber los puntos más vulnerables, es aquí cuando se debe pensar en una cámara que permita grabar de noche, tener visualización compleja para poder detectar a contra luz o en penumbra. Las cámaras de Axis Communi-

cations de este tipo de tecnología se utilizan mucho para proteger perímetros.

Otro de los productos que ofrece la compañía es la solución de parlantes IP, los cuales pueden reproducir de manera instantánea mensajes de advertencia que indiquen el acceso a un área privada; por otra parte, podría darse el caso de mantener una comunicación remota y segura con el individuo que intenta ingresar a instalaciones privadas de alta seguridad. Lo mismo pueden interactuar con cualquier otro dispositivo eléctrico como: apertura de puertas, encender o apagar luces, compartir con otras computadoras a través de la red (el internet de las cosas) o integrar el control de acceso físico.

Manuel Zamudio manifiesta puntos a destacar en cuanto a la seguridad en instalaciones estratégicas, menciona que las empresas implementan cámaras de video-vigilancia porque es un requisito preexistente, sin embargo, desconocen los protocolos de seguridad ante una señal de alerta, no hay procedimientos preestablecidos, no se sabe quién decide qué cámaras usar, dónde tienen que ir esas cámaras y cómo se van a usar.

Otro error de las compañías es que dejan toda la labor de protección a la tecnología, empero, un par de cámaras de vigilancia no deben remplazar la determinación y consciencia humana para valorar y jerarquizar el nivel de acción frente a una problemática. “se trata de que el hombre trabaje más feliz de la mano de la tecnología, no que esta lo remplace”, agrega.

Una de las razones por las que Axis destaca con su sistema de vigilancia, es por su innovadora tecnología digital, la cual utiliza termografía, esto avisa cuando una persona sobrepasa la temperatura promedio del cuerpo, para así detectar el nerviosismo cuando realiza un acto delictivo.

Optex y sus soluciones para combatir amenazas

Otro aliado de las instalaciones vitales es Optex, compañía especializada en la detección de amenazas e intrusiones. Desarrolla productos y soluciones de detección: automatización, utilizados en procesos de producción industrial, pero también es reconocida mundialmente por ser el proveedor número 1 para sensores de puertas automáticas, en accesos vehiculares y peatonales.

“Optex ofrece principalmente soluciones que detecten intrusiones o amenazas de manera temprana o anticipada, sea en tierra como en perímetros exteriores, en áreas entre edificaciones, perímetro y desde luego para descubrir en los interiores de edificios. Brinda recursos especializados como radares, por ejemplo, estos para proteger blancos en el mar o lagos, mostrar lanchas que representen una amenaza, hasta situaciones por aire como drones o sistemas de detección de fibra óptica para



la localización temprana de túneles, afirma Hans Dieter Klein, presidente de Optex Latinoamérica.

Menciona que desde que la compañía incorporó Fiber SenSys Inc. y Raytec Ltd, los proyectos y clientes que son atendidos en el ámbito de instalaciones estratégicas del país y América Latina, han aumentado considerablemente. Su contribución tecnológica crece de manera importante.

En la actualidad, Optex suministra soluciones de detección de intrusos en los sectores energético, penitenciario, transporte ferroviario, puertos marítimos, aeropuertos, sitios de comunicación y centros logísticos, entre otros.

Desde 2012, la compañía se ha enfocado en mantener contacto cercano con los usuarios finales y autoridades del país, ya que es de suma importancia para el buen funcionamiento de sus soluciones, especialmente con las complejas tecnologías que se instalan, esto para que los usuarios

entiendan el producto en el que invirtieron.

“Finalmente, en la implementación de las tecnologías se requiere de personal que tenga conocimiento en seguridad perimetral y electrónica, preferentemente con estudios en ingenierías de comunicación o electrónica, aunado a una comprensión estricta del sector que atienda y en especial al tipo de inmueble que resguarda”, refiere Hans Dieter Klein.

Seguridad perimetral

Juan José García, director comercial de Senstar Latin America, empresa fabricante de sistemas electrónicos para emitir alertas tempranas y detección de intrusos en áreas perimetrales en más de 80 países, indica que sus soluciones se centran principalmente en el mercado de transportes terrestre (carga y público), aeropuertos, puertos marítimos y ferrocarriles.

En el caso del sector energético se ocupa de plantas nucleares, hidroeléctricas, termoeléctricas, subestaciones eléctricas, petroquímicas, refinerías, sitios de almacenamiento/ distribución de gas y petróleo, estaciones de rebombeo de combustible, entre otros. Para las instalaciones militares y fuerza policial, sirve a polvorines, estaciones de policía, armerías, aerobases navales, guardia nacional, servicios secretos, centros de comunicación.

Atiende además prisiones federales y estatales, por otro lado para el mercado de valores, salvaguarda bancos centrales, por último y no menos importante se encargan de preservar las fronteras.

Algunos de los sistemas fabricados por Senstar que se han implementado en instalaciones e infraestructuras son:

- Cable sensor microfónico con detección puntual para montados sobre barreras físicas como; mallas, muros, rejas, concertinas.
- Cable sensor enterrado electromagnético con detecciones puntuales.
- Cable sensor de fibra óptica de largo alcance con detección puntual.
- Sistema de detección por microondas para protección de áreas abiertas con línea de vista.
- Sistema de detección de alambre tenso.
- Sistema de detección electroestático.

Los sitios que se han mencionados son protegidos contra amenazas de robo, sabotaje, vandalismo o ataques terroristas, que pueden impactar en la continuidad de la operación, aunado a posibles pérdidas de vidas humanas.

Como estas tres compañías existen muchas más, nacionales o internacionales, de alta demanda y expertas en la materia, sin embargo, como bien lo han mencionado los especialistas, si cada procedimiento no es sometido a un examen exhaustivo, la tecnología aunque sea de punta requiere de la importancia por parte de las autoridades





para realizar metodologías y procesos para la situación por la que atraviesa.

¿Y las autoridades?

Como ejemplo de la preocupación por las instalaciones estratégicas, la Comisión Nacional de Seguridad fortalece sus capacidades en el tema de protección física. Ejemplo de ello, en el pasado mes de febrero la dependencia informó que el Servicio de Protección Federal (SPF) concluyó el Taller Seguridad y Resiliencia de Infraestructuras Críticas, impartido por un grupo de instructores del Buró de Seguridad Diplomática de los Estados Unidos, a través del Programa Antiterrorismo (ATA), como parte de los acuerdos de cooperación internacional en materia de capacitación y profesionalismo.

En dicho curso participaron 24 elementos del Servicio de Protección Federal, Policía Federal (PF) y Centro de Investigación y Seguridad Nacional (CISEN), quienes reforzaron y homologaron sus conocimientos en cuanto a componentes y activos de la infraestructura vital, operaciones terroristas, explosivos, análisis de amenazas, políticas y procedimientos, operativos de la fuerza de seguridad, tecnología, inspección y validación, derechos humanos, participación comunitaria, entre otras habilidades.

En las oficinas centrales del SPF, su titular **Alfonso Ramón Bagur**, informa que ya son 100 elementos los que se han capacitado desde 2015, distribuidos en cinco grupos, y son los encargados de replicar los

conocimientos al resto de los integrantes del SPF. “Queremos de manera paulatina ser nosotros quienes desarrollemos esta habilidad para capacitar a los encargados de la seguridad de instalaciones estratégicas en 24 estados del país”, añade.

¿Qué necesita México?

La protección de instalaciones e infraestructuras estratégicas hace precisa una rigurosa identificación de los riesgos e inseguridades, su alineación con la propia seguridad corporativa o institucional, la aplicación de un programa de inteligencia y protección, la colaboración e integración de las instituciones que prestan servicios de seguridad pública y privada, el desarrollo de un plan de gestión de crisis y la elaboración e implementación de planes y personal especializado dedicado a este ámbito.

Sin duda, el motivo de presente trabajo periodístico pretende destacar lo que existe y lo que falta en la materia, porque si bien es

un tema que nos incumbe a todos, desafortunadamente en manos de muy pocos esta la solución a este vacío que en breve podría desatar un grave problema económico, político y social.

Hablando de las soluciones tecnológicas que hay en el mercado y son cada vez más innovadoras, resistentes y eficaces, se pueden encontrar desde cámaras térmicas, de videovigilancia, radares, cables sensores de fibra óptica, por mencionar algunos, sin embargo, la instalación de las mismas en áreas estratégicas depende del personal autorizado y análisis exhaustivos que pocos expertos realizan. Se debe facilitar la implementación de las herramientas para contar con instalaciones protegidas integral y holísticamente. Por otra parte, configurar un plan de seguridad dentro del marco legal correspondiente junto a la adopción de la normativa técnica armonizada donde los nuevos conceptos y las tecnologías presenten nuevas oportunidades. **ms**



Hans Dieter Klein
Optex



Manuel Zamudio
Axis
Communications



Arturo García
Experto TI



Manuel Sánchez
Merelo
Consultor



Juan José García,
Senstar



Alfonso Ramón
Bagur
Titular SPF



DE HACKERS Y OTROS DEMONIOS INFORMÁTICOS

Armas de grueso calibre

¿Por qué creen que existen armas "de uso exclusivo del Ejército"? Algunas personas pudieran pensar que para hacerlas funcionar, solo se requiere jalar un gatillo. Tal vez es cierto pero no es suficiente. Vamos más lejos, una persona con permiso para portar armas seguramente las podrá operar, pero eso tampoco es suficiente: se requiere pertenecer a ciertas organizaciones, tener una licencia específica, haber recibido entrenamiento especial y usarlas para un propósito particular.

Lo mismo ocurre con herramientas de seguridad informática que se utilizan para evaluar la seguridad de un equipo de cómputo: cualquiera puede darle clic al botón de iniciar, pero no es suficiente. Se requiere también de haber recibido entrenamiento especial y ejecutarlas bajo un estricto protocolo. Se requiere seguir protocolos para: seleccionar el tipo de software, definir el momento de ejecutar la evaluación, obtener la aceptación del dueño de la infraestructura para proceder, contar planes de actuación y recuperación al finalizar la prueba, entre muchos otros factores que se deben tomar en cuenta.

Algunas personas piensan que este tipo de armamento digital es inofensivo. Entonces me atrevo a decir -con conocimiento de causa- que son ignorantes y no las conocen. Las personas que ya llevamos algunos años en esto hemos vivido la experiencia de ver cómo se pasan las computadoras que son evaluadas y hasta dejan de funcionar ciertos equipos de la red. Incluso hemos tenido que hacer algunas pruebas de evaluación a altas horas de la madrugada con tal de no interrumpir la operación.

Es cierto, un atacante no se tomará esas molestias ni tendrá esas precauciones. Por supuesto debemos estar alertas, contar con protocolos de respuesta probados, cadenas de mando establecidas, avisos definidos a los involucrados, etc. Pero bueno, esa es otra historia, una muy buena que ya tocaré en otra oportunidad. En esta columna estoy hablando particularmente de "pruebas c-o-n-t-r-o-l-a-d-a-s" o "hackeo ético" como ahora le dicen.

En fin, nuevamente llamo a la cordura para realizar y usar estas armas informáticas de grueso calibre, por algo son de uso exclusivo del ciberejército.

Bueno, esta es mi opinión, ¿cuál es la suya?

El demonio del mes: Los atacantes que se podrían aprovechar de dos graves vulnerabilidades que se dieron a conocer recientemente: Meltdown y Spectre. Estas vulnerabilidades afectan a los procesadores (o "chips") instalados en computadoras que usan por ejemplo productos de Microsoft, Apple, Google y otros. Estas debilidades podrían aprovecharse para obtener información confidencial que manejan esos equipos. ¿Lo solución? Instalar las actualizaciones y parches que esos fabricantes han liberado. Por cierto, ¿Usted ya lo hizo? Ahí se lo dejo de tarea... **m's**

Cualquier comentario o sugerencia no dude en consultar al Profe de seguridad.

¡Hasta el próximo número!

Suscripciones al (55) 55272279

asistencia@revistamasseguridad.com.mx

Pregunte por Promociones

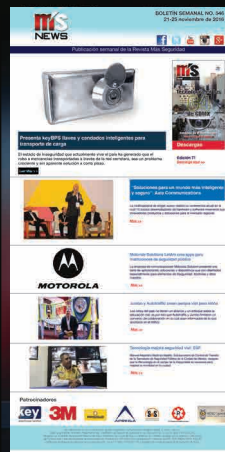


SUSCRÍBASE



Información especializada en seguridad electrónica, física, contraincendios, automotriz, del transporte pública etc.

REVISTA



BOLETÍN
Semanal Electrónico

infosecurity[®]

MEXICO

23-24
MAY 2018

Ciudad de México
Centro Citibanamex



PRASANNA RAMAKRISHNAN
Global Head of InfoSec Risk, Philips

23 MAY / 15:00 - 16:00 HRS.

CON LA PRESENCIA DE
KEVIN MITNICK
El hacker más famoso del mundo
24 MAY / 17:00 - 18:30 HRS.



ARTURO GARCÍA HERNÁNDEZ
CISO, Banco de México

23 MAY / 16:30 - 17:30 HRS.



Consulta el programa completo en
www.infosecuritymexico.com



1a. FASE
ANTES DEL
31 DE MARZO

30%
de descuento

Adquiérello por
\$2,450.00
MXN
IVA incluido

2a. FASE
ANTES DEL
15 DE MAYO

15%
de descuento

Adquiérello por
\$2,975.00
MXN
IVA incluido

NO TE QUEDES FUERA

Compra tu boleto para Infosecurity Summit 2018 y obtén un descuento especial sobre el precio base (\$3,500 MXN)

+10%
de descuento
adicional

INGRESANDO
EL CÓDIGO
MSINFO2

Alianzas

Patrocinador
Diamond

Patrocinadores
Platinum

Patrocinadores
Gold

Organizado por



Se elevan costos de ciberataques financieros

Redacción M'S / @revmasseguridad

Miles de empresas a nivel mundial han aumentado de manera considerable sus inversiones en ciberseguridad en los últimos años, esto con motivo de defenderse de la también creciente ola de ciberataques que se registran a nivel global. Y es que la mayor inversión en sistemas de defensa para prevenir o mitigar va de la mano con el aumento del costo financiero de los mismos, como se desprende de un reciente estudio realizado por el Ponemon Institute, en colaboración con Accenture.

El informe indica que el costo financiero del cibercrimen para las empresas, aumentó 27,4% en 2017, con respecto al 2016. En términos generales, las principales afectaciones que sufren las compañías por cuenta del cibercrimen, se originan en malware, ataques a través de páginas web, denegación de servicios, filtración de información a través de empleados activos o exempleados, código malicioso que abren accesos a las plataformas corporativas, el famoso phishing – una modalidad de la denominada ingeniería social, el ransomware – o secuestro de plataformas o información – el robo físico de dispositivos electrónicos, y los robots informáticos, conocidos también como botnets. A esto, podemos nombrarlo también tráfico de información.



Según evidenció el Ponemon Institute, los ataques más costosos en términos financieros para las empresas que los sufren, se producen por malware y ataques dirigidos de tipo web. Estos dos tipos, coinciden en que su objetivo es obtener acceso a información de las organizaciones.

Las compañías más expuestas a los ciberataques, actualmente, son las del sector financiero, seguidas por las de servicios y energía, aeroespacial y de defensa, entretanto, las menos expuestas se encuentran, en su orden, en los sectores de hospitalidad, educación y ciencias de la vida.

Se estima que la inversión de las empresas en defensa y prevención de ciberataques alcance una cifra de US\$6 billones de dólares anuales, durante los próximos tres años. En 2017, el incremento de las inversiones de este tipo en las organizaciones a nivel global, fue de aproximadamente 23%.

La utilización de tecnologías como seguridad adaptativa, inteligencia artificial o microsegmentación, permiten acorralar a los hackers ofreciendo fuertes barreras que deben ser articuladas de manera estratégica por las organizaciones. **m's**



BlackRuby: ransomware que además hace minería de criptomonedas

Redacción M'S / @revmasseguridad

S21sec, compañía española de seguridad digital, detectó un nuevo malware denominado BlackRuby, que ofrece a los atacantes la posibilidad de elegir a las víctimas por país. Otra particularidad es que el dispositivo infectado puede ser usado para minar criptomonedas, sin el consentimiento del dueño legítimo.

Una vez instalado el virus, éste escanea la computadora en busca de determinados archivos, los encripta y coloca la nota de rescate: la víctima deberá pagar \$650 USD en bitcoin o no podrá recuperar sus archivos (unos \$12 mil pesos, dependiendo el tipo de cambio). En la nota se especifica un correo electrónico al que se tiene que notificar el pago.

Según los atacantes, la víctima obtendrá un "Black Ruby Decryptor", junto con la clave privada de su sistema. Sin embargo, nada garantiza que los archivos sean efectivamente devueltos o que no se haya hecho una copia de ellos.

También se ha reportado el uso de los dispositivos infectados como "mineros" de la criptomoneda Monero, especialmente en el caso en el que las víctimas se nieguen a pagar el rescate, o los cibercriminales no se muestran satisfechos con un pago en particular.

La importancia del respaldo

Realizar respaldos de información periódicos es una de las maneras más efectivas de combatir la eficacia del ransomware.

S21sec recomienda que haya 2 tipos de respaldo: en un dispositivo físico (como una usb que se guarde en la oficina) y uno virtual (en un servicio como Dropbox o Google Drive); de esta manera, el usuario siempre tendrá a la mano una forma de recuperar sus datos. **m's**

EXP[®] SEGURIDAD INDUSTRIAL M É X I C O

24-26 ABRIL
2018 Ciudad de México
Centro Citibanamex

Asiste sin ningún costo. Regístrate hoy en: www.exposeguridadindustrial.com

*Registro sin costo hasta el 20 de abril. No incluye conferencias



ENCUENTRA



La mayor oferta de productos de seguridad industrial.



INTERACTÚA



Más de 100 expositores y 2,000 m2 de exhibición



DESARRÓLLATE



VII Congreso Internacional de Seguridad Integral

Descarga nuestra APP móvil

Mantente informado sobre nuestros ciclos de conferencias, actividades, nuevos expositores, productos y más.

Expo Seguridad



Visita nuestro blog

Conoce las últimas tendencias del mercado, nuevos productos y novedades de la expo.

blog.exposeguridadindustrial.com

Evento organizado por



Congreso organizado por



www.exposeguridadindustrial.com

El logotipo de Expo Seguridad Industrial México es una marca de RELX Intellectual Properties SA, objeto de uso bajo licencia.





Las enseñanzas de los sismos ocurridos en México en septiembre de 2017

El pasado mes de septiembre de 2017, en la República Mexicana se registraron 5 mil 071 sismos, de los cuales 17 fueron con intensidades de moderadas a fuertes; sin embargo el ocurrido el 19 de septiembre, con magnitud 7.1, con epicentro en Axochiapan, Morelos, marcó a los mexicanos debido la pérdida de vidas y daños materiales.

La mayor enseñanza en materia de prevención y respuesta, que dejaron los terremotos, fue la necesidad de continuar con los simulacros y la importancia de tomarlos en serio. En cada hogar, escuela, institución pública o privada deben realizarse análisis de seguridad y protección civil. No hay que escatimar recursos materiales y humanos para mejorar los planes de evacuación.

Alberto González, de la Consultoría en Protección Civil - ASEM CONAVI, indicó que ante un sismo de magnitud 7, la infraestructura existente en la Ciudad de México tiene las características de sismo resistencia adecuadas.

“Debemos recordar que lo más importante es estar preparados revisando instalaciones, dando mantenimiento a las mismas y haciendo evaluaciones periódicas; eso se está comenzando a tomar en serio y por consecuencia, una mayor cantidad de población estará preparada para afrontar un sismo de intensidad fuerte”, destacó González.

El especialista señaló que, en materia de prevención, debemos quitarnos de la cabeza ideas como “no pasa nada, ni lo digas, va a seguir temblando, estamos en la tierra, es un planeta vivo o estamos en una zona sísmica”. Es más inteligente pensar en el peor escenario y de ahí comenzar nuestro plan de respuesta en función de “quiénes somos, cuántos somos y quién está con nosotros”.

En cuanto a la Alerta Sísmica de la Ciudad de México, el experto consideró que la masificación de una mala información del funcionamiento de dicha alerta y una venta de garantía de supervivencia, han generado confusión en el propósito de esta herramienta.

Alberto González señaló además que cuando se presentan sismos mayores a 7 grados y con severas afectaciones, las autoridades son sobrepasadas en todo el mundo. Lamentablemente en México la falta de respeto de la población civil hacia las autoridades a todos los niveles e incluso dentro de las propias dependencias, complica el orden en la respuesta a la emergencia.



Asimismo expuso que en los recientes sismos del mes de septiembre, la población tuvo la capacidad de responder a esta emergencia intentando ayudar a los afectados, sin embargo “en el afán de ayudar, los ciudadanos hemos complicado la situación, esto debido a que cuando quieres decirles: “un momento, necesito que...” se molestan por la rapidez con la que creen se debe actuar, pero esto es un tema humano, donde vemos a otros en una situación complicada y queremos ayudarlos. Además, en muchas ocasiones la falta de confianza o la lentitud de las autoridades motiva a que la sociedad civil responda”.

Por su parte, Raúl Cantón y Lara, presidente de la Organización de Consultores de Protección Civil, indicó que los mexicanos no estamos preparados para afrontar sismos superiores a los 7 grados, debido a que nos falta educación, capacitación y adiestramiento.

Cantón y Lara agregó que los sistemas de alerta son un aviso para que las personas sepan, con algunos segundos de anticipación, que se acaba de generar un sismo y puedan tomar las decisiones que cada quien, en función de sus conocimientos y experiencia, crean conveniente. El sonido de la alerta no significa “corre o agáchate o lo que sea”, es una alerta nada más.

“En materia de respuesta, las instituciones gubernamentales no tienen la capacidad de enfrentar los estragos causados por un movimiento sísmico; ciertamente hay muchas personas preparadas, hay especialistas en cada una de las situaciones que se pueden presentar durante un desastre, pero la reacción y la coordinación

son muy importantes, por ello es que la sociedad civil reaccionó mucho más rápido que las autoridades y grupos especializados”, aseveró el experto, quien además opinó que no existen desastres naturales, los desastres son socialmente contruidos, toda vez que la sociedad civil cuenta con la capacidad de apoyar al rescate de personas: eso quedó demostrado en los sismos de 1985 y 2017.

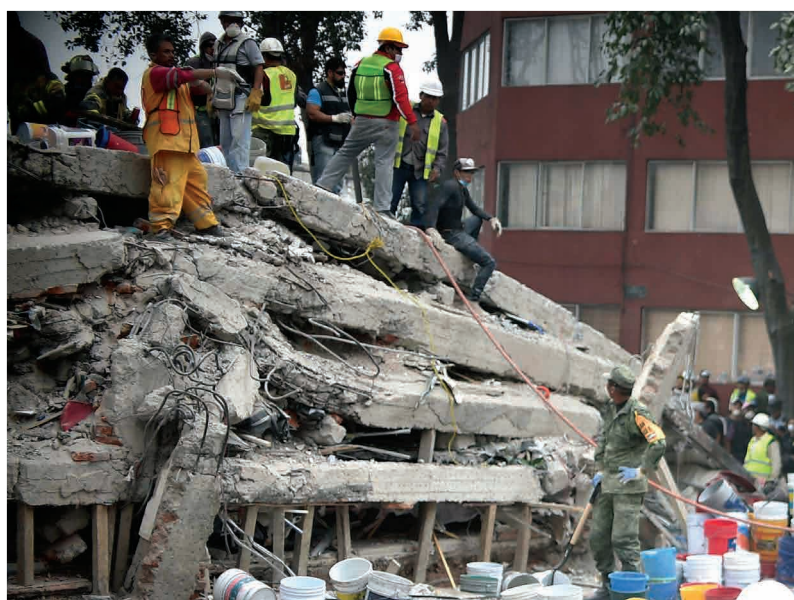
No obstante, nos falta mucho para hacer frente de forma eficiente y efectiva a situaciones similares. Lo más importante es estar conscientes de la importancia de estar preparados, primero, para realizar procedimientos o actividades de prevención y luego qué hacer y cómo actuar ante un desastre.

Cantón y Lara resaltó que en situaciones de actuación para casos de emergencia, hay procedimientos y protocolos ya establecidos a seguir, los cuales deben asumirse como principios generales para poder formar un criterio y en función de éste, tomar

vió a provocar daños en la estructura del Palacio Nacional, mientras que en 1818 sucedió uno aun peor que resquebrajó edificios en el barrio de la Merced, San Francisco y San Diego y en los hospicios de Terceros, la Santísima y San Hipólito, entre otros.

Desde entonces y hasta el Terremoto Maderista de 1911, se estima que hubo al menos una decena adicional de terremotos que provocaron grandes daños a la ciudad y sus alrededores y que obligaron a sus habitantes a reinventarla en más de una ocasión.

La madrugada del 7 de junio de ese año, a unas horas de que el Presidente Francisco I. Madero, entrara triunfante a la Ciudad de México, para declarar el inicio de la democracia en nuestro país, tembló y ni el flamante Servicio Sismológico Nacional, fundado siete años antes por Porfirio Díaz, pudo predecir la llegada del movimiento magni-



decisiones para actuar o para saber qué hacer en esa situación específica.

“Para proceder o actuar en caso de alguna emergencia no hay recetas de cocina, ninguna emergencia es igual, ni impacta igual, ni se comporta de la misma manera; es importante que tomemos los protocolos como una guía que hay que ajustar y adecuar a las circunstancias que se están presentando en esos momentos, inclusive un simulacro nunca es igual, aunque sea la misma hipótesis” dijo el especialista.

Los simulacros dan ciertas pautas, proporcionan conocimientos, preparan para tomar decisiones y ayudan a pensar y a actuar con más seguridad, pero finalmente hay que tomar decisiones en el momento de la emergencia y actuar en función de cada criterio, de lo que dicte la lógica y de los estudios que al respecto se hayan realizado.

El funcionario en mención recordó que los temblores de 1911, 1957, 1985 y 2017 tienen algo en común: provocaron grandes daños en la Ciudad de México y sucedieron a poco más de 30 años de distancia, uno del otro.

Entonces ¿qué tan acertada es la teoría de que a cada generación de capitalinos le toca un sismo de magnitud mayor a 7 grados? El 28 de marzo de 1787, un terremoto de magnitud 8.6 sacudió a la Ciudad de México, dañando el Palacio Nacional y varios edificios históricos de la capital de la entonces Nueva España.

Tres años después hubo otra hecatombe que vol-

tud 7.7, que provocó daños totales o parciales en distintos edificios y la muerte de, al menos, 40 personas.

No tuvo que pasar ni una sola generación para que otro temblor, esta vez con magnitud superior a 7, arrasara con una población cercana a la capital. En noviembre de 1912, ese sismo con epicentro en Michoacán arrasó con gran parte de la infraestructura de varios poblados mexiquenses.

Dos generaciones enteras después, el 28 de junio de 1957, sucedió otro temblor conocido como “El temblor del Ángel”. La madrugada del domingo 28 de julio de 1957 se presentó un sismo de magnitud 7.7, cuyo epicentro se ubicó a 100 km al sureste de Acapulco (Guerrero), a una profundidad de 25 km, con el resultado de 700 personas muertas y 2 mil 500 lesionadas.

Y ni hablar del sismo ocurrido en el año de 1985, donde la población civil se volcó para apoyar en los rescates, inclusive en esa ocasión se abanderaron automóviles particulares con la bandera de la Cruz Roja para transportar a los lesionados.

El sismo más reciente fue el ocurrido el 19 de septiembre de 2017, con epicentro en el interior del continente. En este caso el mayor problema no fue el sismo, sino la vulnerabilidad en las zonas de impacto, la calidad de las construcciones y la capacidad de las personas para reaccionar y tomar decisiones adecuadas para protegerse. m's

Protección integral en aeropuertos

■ Alonso Nájera/ @revmasseguridad

- La OACI es la encargada de crear las reglas para toda la red aeroportuaria

- Existen grandes vacíos en temas de normatividad y legislación para el uso de seguridad electrónica

1 de 2 partes

Cuando se trata de viajar en avión, el usuario promedio visualiza solo una parte de los inconvenientes que esto conlleva, como lo son el robo de equipaje, vuelos retrasados o cancelados, pasajeros despistados o mal intencionados, deterioro o pérdida de equipaje, venta de más asientos de los que se tienen disponibles, por mencionar algunos, sin embargo, la importancia que le atañe al aeropuerto el ser una instalación estratégica, genera estas y otras problemáticas que ni siquiera nos imaginamos, por lo tanto, tampoco sabemos cómo protegernos de ello.

A lo largo del texto, se ahonda en el tema con datos recaudados de especialistas en materia de seguridad, quienes proporcionan métodos, información sobre qué productos utilizar, problemáticas comunes y riesgos que no han sido atendidos del todo.

A diferencia de otras instalaciones estratégicas, el proteger un aeropuerto representa un riesgo internacional; la cercanía de nuestro país con Estados Unidos eleva este riesgo, ya que a diferencia de otras instalaciones vitales, el peligro se encuentra a nivel local. En aeropuertos las implicaciones son mayores, cualquier interferencia ilícita se reporta la Organización de Aviación Civil (OACI), la cual se encarga de crear nuevas reglas para toda la red aeroportuaria internacional.

En concreto, el aeropuerto debe cuidar tres elementos clave: pasajeros, equipaje e infraestructura. Estos puntos son blanco de los delincuentes y presentan necesidades distintas, mismas que, gracias a la investigación que conllevo este trabajo y con la ayuda de expertos en materia de seguridad, se buscará obtener una radiografía de la problemática general de estas instalaciones.

Riesgo en las infraestructuras

El ir y venir de los aviones desencadena riesgos que no solo tienen que ver con los pasajeros, su mercancía o su información.

En el 2016 el Aeropuerto Internacional de la Ciudad de México (AICM) expidió un documento por una solicitud de recursos a la Secretaría de Hacienda y Crédito Público (SHCP); esto debido a que una de sus dos pistas presentaban problemas estructurales por falta de mantenimiento mayor. Sin embargo, en aquel entonces

el director de la terminal negó que hubiera peligros operacionales.

Esto representaba daños considerables a la infraestructura del aeropuerto, además del riesgo a la seguridad de los pasajeros. Para atender esta situación, según el análisis costo-beneficio que la terminal entregó a la Secretaría de Hacienda, solicitaba autorización del uso de 133 millones de pesos para realizar las reparaciones correspondientes.

Dichas fallas a la pista provocaron hundimientos que a su vez se volvieron encharcamientos durante los periodos de lluvias, detonando el riesgo por derrape de las aeronaves y un alto peligro para los aviones al despegar y aterrizar, ya que los hundimientos no pueden ser calculados por los sistemas PAPI (Precision Approach Path Indicator).

Referente a ello, Alejandro Argudín, director del AICM, explicó que las tareas de mantenimiento que se hicieron en la pista permitían mantener el estándar operacional exigido por la Dirección General de Aeronáutica Civil, "por lo que no hay por qué alarmarse", sin embargo, no negó que se debían realizar trabajos más exhaustivos y que para el 2016 contaba con un presupuesto de 2 mil 600 millones de pesos para mantenimiento de toda la terminal.

Seguridad privada: capital humano

Más que complicado, la protección de aeropuertos es un servicio muy especializado, el personal que cuida a estas infraestructuras debe obtener capacitación otorgada por la Autoridad de Aeronáutica Civil (AVSEC) para ello, OACI es la encargada de crear

las reglas para toda la red aeroportuaria, además de otorgar la acreditación a los guardias junto con la Dirección General de Aeronáutica Civil (DGAC) en México

Dicha acreditación, obliga a las empresas de seguridad privada a cumplir con diversos documentos que demuestren sus habilidades, además de una solicitud formal por escrito.

El entrenamiento que va enfocado a cuidar un aeropuerto donde haya civiles es diferente al que recibe un guardia que cuida una base aérea de carga. Cuando el elemento de seguridad va a vigilar perímetros o controles de acceso, la preparación que lleva un inspector de punto de inspección es distinta, requiere una capacitación muy específica que tiene que ver el uso de rayos X e identificar pasajeros sospechosos, entre otras.

El ala protectora

Serviseg, empresa especialista en seguridad integral, desde el 2001 brinda protección a más de 15 aeropuertos en distintos puntos de la República Mexicana. “Controles de accesos, zonas del tránsito, perímetros, bandas de equipaje, plataforma, áreas de aeronáutica, y estacionamientos, las partes que el pasajero no conoce o permanece poco tiempo, es ahí donde estamos y nos especializamos”, refiere Daniel Espinosa, director general de Serviseg.

Para la protección de un inmueble como el aeropuerto, Serviseg emplea guardias intramuros, monitoreo a través de CCTV, alarmas, monitoreo electrónico y rayos X en puntos de inspección, todo esto con el fin de detectar en el equipaje un material que haya estado en contacto con el pasajero y que pueda representar un riesgo como pólvora, sustancias químicas o armas.

Es indispensable la colaboración entre las autoridades federales y las empresas de seguridad privada para la protección de estas infraestructuras. Existe un Comité local de seguridad en el que participan las empresas de seguridad privada y las autoridades aeroportuarias, cuando en dichos inmuebles se presentan delitos contra la salud, la Procuraduría General de la República (PGR) es quien atiende la amenaza, agrega Daniel Espinosa.

En palabras del directivo, el delito más común es el tráfico, existen más intervenciones cuando quieren introducir armas u otro artículo peligroso o algo relacionado con el traslado de personas. Una vez detectada la amenaza, se le da aviso a las autoridades correspondientes.

Existen amenazas menos previstas por el usuario y sin embargo están presentes en los estacionamientos con abandono de vehículos. Los delincuentes los dejan ahí para “enfriarse” después de cometer un acto delictivo en ellos o simplemente pudiera relacionar al criminal con la transgresión a la ley.

Es importante mencionar que todas las empresas de seguridad privada necesitan una acreditación técnica que emite la DGAC, contar con el permiso federal, tener registro de la razón social y contar con el programa de capacitación autorizado ante la Secretaría de Gobernación.

Certificaciones para la seguridad física

De acuerdo con José Luis Alvarado, director de Custodias de Servicio de



Seguridad Integral, Personalizada y Via Satélite. (Grupo Papriza) el rápido avance en los mecanismos y técnicas usadas por el terrorismo internacional, obliga a las empresas a estar cada vez más preparadas para combatir eficientemente cualquier acto de interferencia ilícita en toda instalación.

En el caso de los aeropuertos, es importante el empleo de la seguridad física, para ello son necesarias certificaciones en las que se evalúan las aptitudes y capacidades del aspirante a ser un guardia de seguridad.

Para cumplir con dicha labor, el personal de protección debe demostrar su capacidad técnica, jurídica y administrativa, todo esto sujeto a los lineamientos creados por la DGAC.

Actualmente en grupo Papriza se está analizando la circular CO SA 17.12/17, la cual establece los requisitos que deben cumplir las empresas de seguridad privada y/o corporaciones policiales y de seguridad estatal, para la obtención y/o renovación de la acreditación técnica para la prestación de servicios aeroportuarios y/o complementarios en seguridad y vigilancia”

“Esto pone a las empresas privadas en el camino de la profesionalización, tanto de los elementos de seguridad como de las compañías mismas, con programas de capacitación y calidad acordes con la normatividad nacional e internacional, que no solo haga a estas instituciones mejores empresas, sino que puedan brindar a sus clientes la tranquilidad de cumplir con los requisitos de todas y cada una de las autoridades aeronáuticas del mundo” puntualiza José Luis Alvarado.

Aprinsa y su aportación a la seguridad física

“La infraestructura aeroportuaria contiene un mundo lleno de tecnologías, por lo cual requiere nuevos protocolos de seguridad. Basta de efectos disuasivos que no funcionan. Con tantos adelantos encontramos un gran número de herramientas para la seguridad física, muy funcionales.

Hoy vemos sistemas que no funcionan o son fácilmente evadidos. Un verdadero espejismo en seguridad. Hoy a usted, autoridad aeroportuaria, le damos a conocer productos funcionales y que la sociedad demanda. La seguridad de nuestra población requiere que se actualicen y dejen el esquema tradicional. La gente requiere prevención”, refiere Antonio Trewick, director general de APRINSA, firma mayorista de armas no lesivas.

Para el servicio de protección de aeropuertos, APRINSA presenta los nuevos guantes eléctricos modelo DefenderAPN, los cuales utilizan el concepto de la mano vacía, el cual es defenderse sin armas.

A su oferta incluye productos funcionales como las pistolas eléctricas APRINSA, mismas que son utilizadas en varios aeropuertos del mundo, que con precisión quirúrgica detienen la amenaza dando paso a la paz y seguridad. Son equipos funcionales, y mas en lugares donde hay concentraciones de miles de personas. La disuasión debe ir acompañada con efectividad.

“También podemos hacer referencia a los escudos eléctricos, productos que proveen un campo de fuerza defensivo para proteger a la población, mientras que los bastones eléctricos detienen amenazas antes que adquieran otra magnitud de violencia”, afirma el directivo.

Su portafolios de soluciones integran el rifle APRINSA modelo Tigger, fabricado en una aleación aeroespacial (metal, no plástico) que es extremadamente funcional al usarse, ya que dispara municiones de talco, sal o pimienta, lo cual las hace fantásticas por su precisión y



funcionalidad, ideales para el uso de guardias de seguridad en aeropuertos.

Es importante mencionar que los productos APRINSA proveen soluciones ideales para la infraestructura aeroportuaria. “Hemos encontrado que cada equipo es funcional en situaciones distintas y en ocasiones, pueden usarse en un mismo tipo de eventualidad. Todo esto, respetando la actuación del uso de la fuerza”, refiere Antonio Trewick.

Además que se provee la capacitación correspondiente para el uso de estos productos, por si fuera poco éstos mismos ayudan en el protocolo de seguridad en instalaciones, por ello la empresa sugiere que al equipar al personal de protección física, se utilicen equipos de la misma marca.

Es tan fácil en esta recomendación –agrega el directivo- tener las soluciones adecuadas con una marca de prestigio como la nuestra. Un siglo revolucionario lleno de innovaciones y en seguridad nunca se escatima; al hacerlo puede ser demasiado tarde. Un verdadero placer ofrecerles estas observaciones del siglo XXI.

Sentidos humanos convertidos en tecnología

A pesar de que en cualquier aeropuerto pueden observarse cámaras y personal de seguridad, esto no quiere decir que se lleve la custodia y los protocolos correctos, menciona Manuel Zamudio, gerente de cuentas nacional de Axis communications, y algunos de los puntos débiles en la protección de estas instalaciones.

“Cuando se trata de proteger, primero compramos la medicina y no sabemos cuál es la enfermedad; los aeropuertos no se escapan de esto, ponen las cámaras de videovigilancia porque es un requisito preexistente, sin embargo se desconocen los protocolos y cómo reaccionar ante la señal de alerta. Carecen de procedimientos preestablecidos, no hay preparación necesaria en áreas de informática, no están debidamente informados ni capacitados en cuanto al ancho de banda y ciber seguridad, se está demostrando la vulnerabilidad de los sistemas de seguridad electrónica, no se está tomando en cuenta a la hora de diseñarlos, se escatima mucho en esta situación. Normalmente las aerolíneas se deslindan de esta responsabilidad en lugar de designarla a alguien especializado”, comenta Manuel Zamudio.

Además, otros de los problemas de estas instalaciones es que todos sus sistemas están aislados, no hay una integración de las diferentes plataformas (control de audio, de acceso físico, audio vigilancia, control incendios) lo ideal sería integrarlos y esa es una de las cosas que Axis hace posible.

Sin embargo, no todo es por una mala gestión de seguridad en las empresas. En temas de normatividad y legislación para el uso de seguridad electrónica, encontramos grandes vacíos o textos que favorecen a tecnología obsoleta, esto por parte del gobierno y del operador aeroportuario.

Las alternativas

Como lo mencionábamos, existen diferencias entre cuidar aeropuertos de pasajeros y de carga, Ambos poseen necesidades compartidas, sin embargo, en palabras de Manuel Zamudio, hay diferentes formas de resolver la misma situación. “En Axis

el catalogo nos da para resolver el mismo problema de diferentes formas”, agrega.

Axis utiliza tecnología que, además de buscar economizar la energía eléctrica y ayudar de manera responsable a la sustentabilidad, tiene cualidades que permiten detectar audio, tener una visión nítida de lo ocurrido, además de sus mecanismos termográficos cuya función es detectar cuando un pasajero eleva su temperatura promedio en condiciones normales del cuerpo, para así percibir si el nerviosismo por cometer un acto ilícito es la razón de su alta temperatura, esto también permite encontrar artículos de alto valor cuando los ingieren.

Al respecto, ofrece cámaras cuyas herramientas de seguridad electrónica, por medio de una analítica puede detectar cuando alguien está entrando a un lugar que no le corresponde, incluso teniendo actividad sospechosa.

En cuanto al sistema sonoro, busca innovar y agregar actualizaciones de sonido a los sistemas de video que no soportan el audio, ya sean micrófonos digitales o análogos.

La tecnología debe estar hecha para soportar todos los percances que amenazan los sistemas de seguridad: delincuencia, riesgos ambientales, etc.

Deben elegirse las soluciones adecuadas dependiendo del problema a tratar. Hay casos registrados en los que los incendios en ciertas instalaciones fueron provocados por fallos en su sistema de seguridad.

Contra los peligros

A lo largo de la existencia de Axis, la tecnología ha sido su mejor aliado. Revolucionando los sistemas de vigilancia, pasando de lo analógico a lo digital, cambiando de sistemas cerrados a abiertos, creando analíticas de audio capaces de detectar cuando hay agresiones verbales al personal, cámaras de alta resolución, sistemas integrales que permitan tener procesos más inteligentes, seguros y automatizados.

Para la seguridad en los estacionamientos en aeropuertos, brinda un sistema que utiliza una tarjeta de proximidad para hacer el proceso más rápido cobrando directamente a una tarjeta de crédito o identificando al conductor por la matrícula de su auto.

Síntomas del aeropuerto

Manuel Zamudio, además de brindar información sobre los productos de Axis, proporciona una radiografía de algunos de los males que por su experiencia en el ámbito de la seguridad, pudo visualizar.

Uno de los ejemplos de estos males es le carga de toda la responsabilidad por parte de los empleados a las empresas que implementan los sistemas de seguridad, la comunicación entre dichas instituciones y el personal aeroportuario es muy pobre, provocando que los encargados de vigilar el funcionamiento de esta tecnología no estén debidamente capacitados.

Otro de los problemas entre la tecnología y el personal de protección, es la errónea creencia de que estos dispositivos reemplazarán a las personas cuando en realidad su función es hacerles el trabajo más fácil.

En palabras de Manuel Zamudio, varias empresas escatiman en la eficiencia, ya que muchas veces eligen la funcionalidad por medio del precio, haciendo que lo instalado no se incorpore de manera



esté seguro de cómo funciona. También se debe a que el personal directamente vinculado a la seguridad, no está al tanto en temas de protección informática, recursos humanos, operaciones o finanzas.

El peligro merodea los aeropuertos



No solo existen riesgos fuera de los aeropuertos, la seguridad a las afueras, es una responsabilidad compartida entre autoridades federales y personal de protección. Pese a este trabajo en conjunto, hay antecedentes de tragedias ocurridas a unos pasos de las puertas de los inmuebles.

Por citar un ejemplo, en las inmediaciones del aeropuerto capitalino se han registrado diversos asaltos ¿el motivo? Obtener información, tarjetas de crédito, dinero en efectivo o por el enfrentamiento entre bandas delictivas.

Es precisamente la tecnología la que tendría que funcionar como "antibiótico" para el mal que adolece el aeropuerto: la corrupción. Y es que este problema contamina también a los órganos encargados de seguridad, siendo estos quienes, debido a un infiltramiento, ponen en riesgo el bienestar de la población cuando tendría que lo contrario.

Para prueba de lo anterior, el caso ocurrido el 26 de junio del 2012 en el que se frustró un operativo contra agentes involucrados en el trasiego de cocaína, destapando así una red de funcionarios locales y federales.

La Secretaría de Seguridad Pública de la Ciudad de México (SSP), informó que el enfrentamiento entre los uniformados de la Policía Federal sucedió alrededor 08:30 de la mañana en el área de comida rápida y en un pasillo que da a locales comerciales de la Terminal 2.

Según el vocero del AICM, Jorge Andrés Gómez Pineda, nunca se afectaron las operaciones aéreas de la Terminal 2, sin embargo, esto representó una situación inédita en el aeropuerto, ya que este enfrentamiento sembró el terror a un grado nunca antes visto en el inmueble.

El antecedente, sin duda fue un día triste para la historia no solo del AICM, sino también para quienes están al pendiente de la seguridad aeroportuaria. No hay que olvidar que todos los días, el aeropuerto de la CDMX carga con la responsabilidad de resguardar a más de 90 mil pasajeros que pasan por él hacia más de 100 destinos en tres continentes.

Sin embargo, aquel terrible suceso también sirvió como aprendizaje para que los otros aeropuertos del país, se reinventen en materia de seguridad y no vuelva a ocurrir un incidente de tal magnitud.

Ejemplo de innovación

Hablando de aeropuertos nacionales, hay quienes se adelantan en la labor de estar a la vanguardia en cuanto a equipos de seguridad y tecnología de punta para la protección se refiere.

El aeropuerto de Cancún es el segundo más concurrido de México, solo después del AICM. Ha crecido rápidamente. Pasó de tener un flujo de pasajeros de 7 millones en 1999 a aproximadamente 23 millones anualmente en la actualidad. Para manejar el creciente número de usuarios, una cuarta terminal se puso en operación este 2018, lo que la convierte en el único aeropuerto de México con cuatro terminales.

(Continuará...)



Riesgos latentes en instalaciones estratégicas

Son muchos y poco visibles los problemas que rodean al resguardo de instalaciones estratégicas en México, como por ejemplo la necesidad de fortalecer la militarización de la seguridad en este tipo de inmuebles, la optimización de las normas para responder a la vulnerabilidad de instalaciones físicas y el peligro latente que genera el mal uso de internet, coincidieron expertos en la materia.

Teniendo como marco la sesión del mes de febrero de ASIS Cooperativa Capítulo México, personalidades dedicadas a la seguridad, se cuestionaron el eficiente resguardo que se hace de instalaciones estratégicas de nuestro país.

Al respecto, el subdirector de Seguridad Física de la CFE, Capitán Gustavo Cuevas Gutiérrez, abordó temas como las obligaciones de las Fuerzas Armadas en instalaciones de riesgo y cómo deben actuar en caso de que se presente una situación. También mencionó algunas de las diferencias en cuanto a cuidados de instalaciones críticas, como lo son el tipo de cámaras de videovigilancia que deben instalarse y la diferencia de entrenamiento del personal, esto dependiendo del tipo de instalación. Manifestó su preocupación en cuanto



a la falta de claridad por los huecos en el marco legislativo para la protección de estos recintos.

Por su parte, Juan Manuel García Cross, director general Grupo Corporativo de Prevención, habló de la labor realizada por la empresa en sus más de 15 años en el mercado, cuyo enfoque ha sido ofrecer seguridad privada de calidad. Además, mencionó el peligro que existe en internet para el resguardo de la información, ya que hoy en día, los hackers son una amenaza por la que debemos estar preocupados, y las infraestructuras críticas no son la excepción.

Desde otro punto, el titular de la Dirección General de Seguridad Privada (DGSP) de la SEGOB, Bernardo Espino, habló de su trayectoria en empresas enfocadas al rubro de la seguridad y de la importancia de la capacitación del personal para el correcto cumplimiento de todas las modalidades y normas señaladas por la ley, sobre todo cuando se trata de su operación en instalaciones estratégicas.

Para finalizar, el presidente de ASIS Capítulo México, Gabriel Bernal reafirmó la misión de ASIS de auxiliar a las personas y empresas en su práctica en las diferentes disciplinas de la seguridad, con el objetivo de mejorar su desarrollo y desempeño para así elevar el valor de su estatus profesional. **ms**

Culmina primer diplomado en Administración de Seguridad Física en instalaciones gubernamentales

ASIS Capítulo México, el Servicio de Protección Federal (SPF), junto con la Secretaría de la Función Pública y representantes del Servicio de Seguridad Diplomática de los Estados Unidos de América, se reunieron con motivo de la graduación de la primera generación del diplomado en Administración Física en las instalaciones Gubernamentales (DAS).

El curso fue impartido por expertos en materia de seguridad del Servicio de Protección Federal y fue dirigido a más de 80 participantes de los sectores público y privado, entre los que se encontraban directivos de más de 40 instituciones. Dicha capacitación tuvo una duración de cuatro meses.

Representantes de dependencias de gobierno y colaboradores de ASIS Capítulo México, se encargaron de entregar el reconocimiento a los graduados, quienes fueron elogiados por su entrega y disposición por adquirir los conocimientos necesarios para concluir su preparación.

Atestiguaron este importante evento para los miembros de ASIS, Alfonso Ramón Bagur, titular del Servicio de Protección Federal (SPF); Mireya Barbosa Betancourt, titular de la Unidad de Desarrollo e Integración Institucional de la Comisión Nacional de Seguridad (CNS); Bernardo Espino



de Castillo Barrón, titular de la Dirección General de Seguridad Privada (DGSP) de la CNS y Gabriel Bernal Gómez, presidente de ASIS Capítulo México, quienes además firmaron el acta de integración del grupo de coordinación para la Seguridad de Instalaciones Gubernamentales, cuyo objetivo es el intercambio de buenas prácticas para adoptar esquemas unificados que beneficien la seguridad de las instalaciones federales.

“Esta primera generación es única, no por el hecho de ser la primera, sino por lo que ello representa. El primero siempre enseña al de atrás”, señaló Alfonso Ramón Bagur, responsable del SPF. **ms**

Tu seguridad
desde una
nueva
perspectiva



Fotografía: Gustavo Llanquih Reyes

www.grupoipsmexico.com.mx

Tel. +52 5525 3242



GRUPO IPS MÉXICO
GARANTÍA EN SEGURIDAD

Disminuyó 29.5% robo a transporte de carga en la CDMX



Redacción M'S / @revmasseguridad

Derivado del trabajo coordinado entre la policía capitalina y transportistas de carga, se ha logrado una reducción de 29.5% en los ilícitos que afectaban a este gremio y aunado a ello se han reducido significativamente las emisiones contaminantes en beneficio del medio ambiente, informó el Secretario de Seguridad Pública de la Ciudad de México, Hiram Almeida Estrada.

En el marco de la firma de convenio entre la Secretaría de Seguridad Pública de la Ciudad de México (SSP-CDMX) y el Grupo Técnico de Empresarios del Autotransporte, mencionó: "Es muy satisfactorio encontrar que en los ámbitos de los sectores privados empresariales, tengan la voluntad de trabajar de manera coordinada con las autoridades. El esfuerzo colectivo es un ejemplo de un ejercicio de gobierno moderno, eficaz, legal, pero sobre todo siempre muy cercano hacia la gente y sus sectores productivos".

Resaltó que se dejaron de cometer 50 delitos en agravio a transportistas durante 2017 con relación a 2016, por ello es importante celebrar por segunda ocasión la firma de este acuerdo con una naturaleza muy clara, de generar condiciones suficientes acorde a las características y necesidades tanto de los sectores empresariales y de los habitantes de la ciudad, por lo que se ponen en marcha corredores seguros en beneficio del medio ambiente y la movilidad, así como en temas de seguridad.

Por su parte el director de la CONCAMIN, agradeció al gobierno de la Ciudad y al titular de la SSP-CDMX, por la renovación del convenio que se firma y añadió "por tercer año consecutivo el compromiso es en beneficio del tránsito, la movilidad y del medio ambiente en la Ciudad de México".

El titular de la policía de la Ciudad de México, informó

- Se firmó un convenio entre la Secretaría de Seguridad Pública de la Ciudad de México (SSP-CDMX) y el Grupo Técnico de Empresarios del Autotransporte

como parte de estas acciones la dependencia ha implementado 446 operativos.

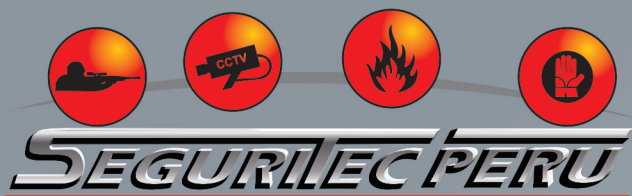
Por parte del sector transportista asistieron, el presidente de la Cámara Nacional de Autotransporte de Carga (CANACAR), Rogelio F. Montemayor Morineau; la directora general del Consejo Mexicano de la Industria de Productos de Consumo (CONMEXICO), Lorena Cerdán Torres; el presidente del Comité Ejecutivo Nacional de la Confederación de Transportistas Mexicanos (CONATRAM), Elías Dip Ramé y el presidente de la Asociación Nacional de Transporte Privado (ANTP), Alex Theissen Long.

Antecedentes

El 27 de octubre de 2016, se firmó un convenio entre SSP-CMX y diversos sectores industriales, autoservicios y tiendas departamentales, comercio y servicios de transporte de carga para hacer más eficiente la circulación de este tipo de vehículos y contribuir al mejoramiento del tránsito, la movilidad y la disminución de emisiones contaminantes a la atmósfera en la Ciudad de México, con vigencia al 31 de diciembre de 2017.

El objetivo es contribuir al mejoramiento de la circulación vehicular, movilidad y a la disminución de emisores contaminantes atmosféricos en la Ciudad de México y su zona metropolitana, mediante la restricción en su totalidad del acceso de todos los vehículos de carga, con placas federales y locales de 3^{1/2} toneladas y mayores de conformidad con la clasificación de la Norma Oficial Mexicana NOM-012-SCT-02-2014, de lunes a viernes, en un horario de 06:00 a 10:00 horas, en las vialidades de ingreso a la Ciudad de México, como el acceso carretera de Querétaro, Toluca, Puebla, Cuernavaca, Texcoco y Pachuca. **m's**





Feria Internacional

Seguridad Física, Industrial,
Incendio, Rescate & Policía

Mayo 23 - 25
2018

Lima - Perú



Seguridad Física

¡Reserve su Stand Hoy!

www.thaiscorp.com

Sede:



Seguridad Industrial



Policía



Rescate



Incendio

Organiza: **THAIS CORPORATION** - Tel.: (511) 201-7820 - Email: thais@thaiscorp.com

Oficialización:



Prensa Asociada:



CHINA:
Beijing Worldboston International
Business Exhibition Co., Ltd.
Tel: +86-10-87688258
Alice Zhang
alice@worldboston.com

TURQUIA:
Amiral Fair
Tel: 90-533-5435789
Erhan Ersever
info@amiralfair.com

Fortalece Colombia exportaciones de productos militares

Bogotá, Col.- Hacer alianzas entre los sectores público y privado es muy sencillo, pero mantenerlas con éxito es la tarea titánica que pocos organismos consiguen, sobre todo si de exportar se trata.

En Colombia hay un palpable caso de éxito entre los dos nichos que fomentan una sana industria militar en beneficio de la seguridad nacional y el Ministerio de Defensa (MinDefensa) es el artífice de esta dinámica.

Teniendo como marco Expodefensa 2017, en entrevista exclusiva con el Viceministro de Defensa, General Retirado José Javier Pérez Mejía, explica que luego de 40 años de servicio en la Fuerza Aérea colombiana, desde hace cuatro años atiende a un grupo de empresas y entidades del Sector Defensa, integrado por 19 compañías y entidades como la Industria Militar (INDUMIL), el Astillero Naval (COTECMAR), Corporación de Alta Tecnología (CODALTEC), Corporación de la Industria Aeronáutica (CIAC), la aerolínea Atena y hoteles en Bogotá, Cartagena, Santa Marta y Buena Aventura.

“Tenemos los Clubes de Oficiales y de Suboficiales, a la Organización de la Defensa Civil Colombiana, en el sector de salud hospitalares y una gran cantidad de organizaciones. Mantenemos 11 mil empleos directos y 2017 manejamos aproximadamente unos 2 millones de dólares en nuestras empresas, las cuales han participado en el desarrollo industrial del país”, informa el General Pérez Mejía.

Puntualiza que muchas compañías tienen de cinco a 60 años de existencia en Colombia, por ello el MinDefensa demostró en la

pasada Expodefensa 2017, cuáles son las capacidades y la evolución que han tenido estas empresas en los últimos años y compartir con el sector toda su oferta tecnológica y armamentista, por ello el interés de comercializar fuera del país sudamericano.

“Este año la empresa naviera COTECMAR le vendió a Honduras un buqué de desembarco anfibio administrativo. Tenemos avances de varias posibles negociaciones con países en América Latina. Buscamos concretar uniones con diversos Ministerios de Defensa y sector privado, el cual por cierto maneja la industria de defensa en el mundo y pues Colombia no puede ser la excepción.

Tendrá que desarrollar una gran participación del sector privado para crecer, para innovar y mantenerse en los niveles de desarrollo de tecnología que la hacen competitiva y la puedan hacer sostenible en el tiempo”, afirma el funcionario.

Reitera el objetivo de Colombia (a corto plazo) de incrementar sus exportaciones y cita como ejemplo a COTECMAR que vendió al mercado externo 20 millones de dólares e INDUMIL que registró 60 millones de dólares. “Son cifras que antes no teníamos, gracias a nuestra alta competitividad en el mercado internacional, no solo por la experiencia de lo que producimos porque ya ha sido probado y comprobado en Colombia, sino porque producimos a unos precios altamente competitivos y con la misma calidad de los grandes productores en los rubros de seguridad y defensa.

Ejemplo de estas exportaciones son Brasil y Honduras que adquirieron lanchas de río y mar, así como buques. En el caso de los Emiratos Árabes, Colombia le vende bombas para aviones caza, incluso en 2017 cerró negocio por 42 millones de dólares, lo cual potencia la entrada a otros países del Medio Oriente.

- *La industria militar es fuente de empleo directo para 11 mil personas.*
- *Exporta a Brasil, Honduras y Emiratos Árabes*



Entrevista con el Viceministro de Defensa, General Retirado José Javier Pérez Mejía

En el segmento de seguridad, con CODAL-TEC el MinDefensa exporta su tecnología para Centros de Mando y Control para ciudades, con productos diseñados y desarrollados in-house.

En el caso específico de México, las relaciones son muy cercanas y las autoridades conocen la gama de productos, especialmente los navales, por lo que hay especial interés de la Secretaría de Marina (SEMAR) para co-producción o comprar.

“Colombia es un país líder en proyectos militares. Tenemos muchas posibilidades de crecer, de competir, de importar tecnología, pero sobre todo de capacitar a nuestra gente en la industria militar. Adicionalmente en 50 años de conflicto, nos obligó a desarrollar muchos proyectos o productos que no encontrábamos en el mercado, por ejemplo bombas de aviones. Nos tocó desarrollarlas desde cero, sin asesoría extranjera y hoy exportamos este tipo de armas.

De acuerdo con el Viceministro General Retirado José Javier Pérez Mejía, han sido de varias vías que motivaron el desarrollo de la industria militar colombiana:

- 1.- Producto de la necesidad y un conflicto.
- 2.- La capacitación de sus hombres en el exterior.
- 3.- Decisión.

“Una muestra de la capacidad de producción, calidad de los productos y tecnología de última generación, se exhibió en Expodefensa 2017, muestra



desarrollada en Colombia en co-participación con el MinDefensa desde hace 15 años, la cual se ha consolidado en la región sudamericana y europea, pues participan una amplia variedad de países expositores y visitan delegaciones militares de prácticamente todo el mundo. En 2019 sin duda mostraremos novedades que pronto estarán disponibles para todo el mundo”, finaliza el funcionario. **m/s**

**BUILT
STRONGER
TO LAST LONGER!**

**AMPLIA TUS HORIZONTES
Y CUENTA CON EL RESPALDO
DE EXPLORER CASES**



Explorer Cases es una gama completa de estuches indestructibles a prueba de agua: la solución ideal para satisfacer las necesidades de los usuarios más exigentes, en las condiciones más extremas.

Marca líder en el sector, conocida y reconocida internacionalmente: nuestros productos son considerados los recipientes de uso técnico más fiables en el mercado; Somo el líder europeo en el design y en la producción de soluciones de maletas y estuches de protección de alto rendimiento.

VISITANOS EN NUESTRO STAND - 3947

HARD CASES
MADE IN ITALY

EXP
SEGURIDAD

24-26 Abril - Ciudad de México

EXPLORER
CASES

www.explorercases.com

Perfil del profesional de la seguridad en América Latina

Parte 2 de 2

Iniciativas regionales

En su libro “Liderazgo estratégico en seguridad” (2017), José Paulino González identifica 16 habilidades y destrezas que califica como indispensables para un líder de seguridad: visión estratégica, toma de decisiones y pensamiento crítico, gestión y seguimiento/ ejecución, trabajo en equipo, comunicación efectiva, planificación estratégica, finanzas estratégicas, realismo y pragmatismo, escucha activa, relacionamiento estratégico, negociación, innovación con propósito, intuición y percepción del riesgo, respuesta a emergencias y crisis, trabajo bajo presión y ambientes hostiles, y gestión del talento humano. Esta apreciación surge de la consulta a casi 100 profesionales vinculados a diversas áreas de la seguridad.

Entre junio y agosto del 2017, consulté la opinión de poco más de 80 colegas de Argentina, Chile, Colombia, Brasil, República Dominicana, Perú, Ecuador, México y Venezuela. Los resultados, aunque numerosos, convergían mayoritariamente hacia cuatro claras tendencias sobre lo que se espera de un profesional de la seguridad en América Latina.

Comunicador. Es la habilidad más solicitada y valorada. Se trata no sólo de saber qué va a comunicar, cómo y a quién, sino cuál es el momento oportuno para hacerlo. Incluye la gestión de la información, sabiendo seleccionar y recomendar las fuentes más confiables. El uso eficiente de las redes sociales puede contribuir a consolidar su credibilidad o a derrumbarla por completo, por lo que el control a la impulsividad y la inmediatez es sinónimo de madurez. En especial en momentos de crisis relacionadas con la seguridad, el responsable del área es con frecuencia el más consultado por la alta dirección, para tomar decisiones que implican la protección asertiva de personas y bienes. Es oportuno el comentario de Tony Robbins “Para comunicarse de manera efectiva, debemos darnos cuenta de que todos somos diferentes en la forma en que percibimos el mundo y usar este conocimiento como una guía para nuestra comunicación con los demás”.

Visión integral. Aunque está íntimamente relacionada con la capacidad de prever situaciones, no se limita a ello. El entorno debe ser considerado como factor perturbador o favorecedor de la seguridad de una organización. Las evaluaciones del mismo incluyen todo tipo de componentes que antes ni siquiera eran considerados. Y es que, por ejemplo, a medida que los miembros de un grupo social evolucionan, las condiciones e influencias se modifican. La movilidad de personas, recursos, políticas e ideologías son cada vez más aceleradas. Un reconocido pensador de estos últimos factores a quien se sugiere estudiar es Moisés Naim, en especial en sus libros “El fin del poder” y “Repensar el mundo”. Argumenta que el mundo debe ser repensado continuamente si se desea entenderlo y marchar a su ritmo.

Relacionamiento. Si algo caracteriza las relaciones profesionales en América Latina tanto en el ámbito público como en el privado, es el contacto “cara a cara” y las referencias

personales. El responsable de la seguridad de una organización debe lograr, mantener y acrecentar su círculo de influencia. Para consolidar el tan necesario y enriquecedor networking, se deben considerar colegios profesionales y asociaciones de la industria. Por lo general, los titulares de cargos en instituciones del Estado cambian con rapidez, por lo que hay que estar atento permanentemente. El favorecerse de las mejores prácticas es imposible bajo condiciones de aislamiento. Recordemos a Stephen Covey cuando dijo “La tecnología reinventará los negocios, pero las relaciones humanas seguirán siendo la clave del éxito”.

Capacitación formal.

Las amenazas son en oportunidades, como un ser vivo con una amplísima capacidad de adaptación, por lo que en seguridad afrontar los riesgos no es una carrera de 100 metros planos. Hay que prepararse para un largo y arduo maratón donde siempre se debe estar adelante. Los conocimientos formales en seguridad, bien sea por la vía de la academia o mediante certificaciones profesionales reconocidas son ampliamente valorados. Aunque no se subestima la experiencia en entornos hostiles y gestión de riesgos, está demostrado que el acompañamiento perfecto exige capacitación formal, permanente y dinámica en esos temas. Bien lo anticipó Alvin Tofler “Los analfabetos del siglo XXI no serán aquellos que no sepan leer ni escribir, sino aquellos que no puedan aprender, desaprender y reaprender”.

Por lo general, en América Latina los profesionales de la seguridad desarrollan sus gestiones en un entorno considerablemente hostil, con una disponibilidad de recursos muy limitada y bajo condiciones de permanente incertidumbre. Si existe la disposición a la preparación continua y una positiva actitud de líder, no costará mucho evidenciar la oportunidad de aprendizaje que esto representa y los extraordinarios resultados que pueden obtenerse. Pero para ello no basta la intención, estar listo y capacitado para cuando llegue el momento marcará la diferencia con los que se mantuvieron en su zona de confort. **ms**



*** Alfredo Yuncoza**
Venezuela

Consultor de seguridad con más de 25 años de experiencia profesional en organizaciones nacionales y transnacionales de diversa naturaleza. Past Regional Vicepresident, ex vicepresidente regional de ASIS Internacional (R 8B). Presidente del Comité de Seguridad de la Cámara Venezolana Británica de Comercio. Invitado frecuente como ponente a eventos de la industria en México, Ecuador, Colombia, E.U., y Venezuela. ayuncoza@gmail.com
Twitter: @alfredoyuncoza

intersec

BUENOS AIRES

29 – 31 Agosto, 2018

La Rural Predio Ferial - Buenos Aires, Argentina

Exposición Internacional de Seguridad,
Protección contra Incendios,
Seguridad Electrónica, Industrial
y Protección Personal

www.intersecbuenosaires.com.ar

 @Intersec_BA

 /IntersecBuenosAires



messe frankfurt

Cámara Argentina
de Seguridad

Messe Frankfurt Argentina: + 54 11 4514 1400 - intersec@argentina.messefrankfurt.com

Promueve FEPASEP

alianza de la industria en LATAM

Bogotá, Col.- Reza el dicho que en la unión está la fuerza y eso es lo que justamente busca la Federación Panamericana de Seguridad Privada (FEPASEP), ahora presidida por el colombiano Oswaldo Parada Prieto, quien asegura que la organización está más viva y activa que nunca con la elocuente participación de Argentina, Brasil, Colombia, Panamá, Uruguay y Honduras.

¿Para qué existe la FEPASEP?

-Surge de la necesidad de los diferentes gremios de la seguridad privada, de las diferentes cámaras de América Latina de unirse para defender políticas públicas, para poder multiplicar en nuestras diferentes naciones las soluciones a nuestros problemas, pero también para compartir experiencias.

¿Qué busca la FEPASEP?

-Proteger nuestros mercados, la industria, favorecer al personal nacional, blindarnos ante la entrada de multinacionales a la industria de seguridad privada en América Latina, acabar con la facultad discrecional que tiene el Estado en muchos de nuestros países para terminar de tajo, de un día a otro con nuestras empresas, desprotegiendo el emprendimiento empresarial. Buscamos fijar políticas públicas que entiendan que somos un brazo aliado de la fuerza pública, que somos el principal coadyuvante de la policía y del ejército, que somos una entidad netamente privada pero que desde lo privado podemos poner a disposición todos nuestros recursos para contribuir a la seguridad y la ciudadanía.

¿Dónde actúa la FEPASEP?

-Lo estamos haciendo en América Latina y es un recurso que al Estado no le cuesta y es un beneficio que pones a disposición los empresarios privados para proteger también al ciudadano y ayudar en la defensa de la lucha contra la criminalidad.

¿Quiénes pueden afiliarse a la FEPASEP?

-Las asociaciones y cámaras sectoriales, es decir que al interior de cada país, es el gremio el que hace parte, no es el empresario individualmente.

¿Con quién busca relacionarse la FEPASEP?

Nuestro llamado aprovechando la oportunidad que se nos brinda **Más Seguridad** aquí en Colombia y América Latina, es para que los en los países, las diferentes cámaras se asocien a la FEPASEP, entiendan la magni-

tud del proyecto. Si logramos tener a todas las cámaras latinoamericanas de la industria entorno a un solo gremio, podemos difundir las políticas públicas, ayudarnos frente a nuestros gobiernos. Ya hemos participado en diferentes congresos con diputados y senadores explicándoles desde la FEPASEP como coadyuvamos a la política pública, a la formación y estandarización de la vigilancia privada.

¿Qué países tienen mayor participación?

-Argentina, Uruguay, Brasil, Panamá, Honduras y por supuesto Colombia, son los más dinámicos que viene liderando este proyecto latinoamericano.

¿México continúa afiliado?

-México ha sufrido diferentes situaciones que desafortunadamente cuando hay cambio de presidente del capítulo o de gestores de juntas directivas, se pierden esas sinergias, ya no asisten a las citaciones que hace la FEPASEP en el continente.

¿Cómo afiliarse a la FEPASEP?

Se pueden afiliar vía ANDEVIP www.adevip.com o pueden consultar la página de la FEPASEP www.fepasep.com.co y www.fepasep.net.com

¿Cuál es el requisito indispensable?

Estar legalmente constituida la asociación, pertenecer a alguna cámara sectorial o de comercio (si aplica) y estar reconocido por los empresarios de seguridad de sus países. La afiliación es totalmente gratuita.

Algo para agregar...

Decirles que Colombia es una hermana República que está interesada en coadyuvar a todos los procesos gremiales donde se necesite y ahí estamos dispuestos a concurrir con nuestra experiencia,

a presentarles el modelo gremial, mostrarles como hemos logrado sostener un modelo sectorial durante más de 32 años, como lo hemos fortalecido y mantenido el reconocimiento de nuestros gobiernos nacionales, pero también como este modelo gremial se logra robustecer en la política pública, como ha logrado establecer legislaciones propias en seguridad privada, las cuales favorecen a los empresarios nacionales de la seguridad intramuros. **m's**



Oswaldo Parada
presidente de
FEPASEP

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

Oportunidad única para ampliar su red de contactos.

El evento de actualización por excelencia!

04 | LIMA / PERÚ
2018
 A B R I L | NM LIMA HOTEL



COMPAÑÍAS EXPOSITORAS



ORGANIZACIONES ALIADAS



Fuerza Aérea Mexicana

103 años



Guillermo Espinosa

Tecámac, Edomex.- El Presidente de México, al encabezar la ceremonia conmemorativa del Día de la Fuerza Aérea Mexicana (FAM), reconoció que los valores y el amor a nuestro país de las mujeres y hombres de la institución sirven a la patria con honor y lealtad.

Destacó el papel que desempeñó la FAM para el transporte de personal de rescate, provisión de alimentos y medicinas, así como el auxilio a la población afectada, después de los sismos de septiembre pasado.

El Jefe Supremo de las Fuerzas Armadas, destacó que desde la Base Aérea ubicada en Ixtpec, luego de los sismos, se realizaban diariamente, cientos de operaciones de despegue y aterrizaje para el traslado de ayuda humanitaria en territorios dispersos en los estados de Oaxaca y Chiapas.

A 103 años de la creación de la institución aérea, el Presidente, hizo un recuento de los inicios de la aviación en México y resaltó las acciones de los elementos del Escuadrón 201 que participaron en la Segunda Guerra Mundial, en el Océano Pacífico.

Enfatizó que hoy en día México cuenta con la mejor Fuerza Aérea de la historia, ya que posee la flota más moderna, mejores instalaciones aeronáuticas y el personal altamente capacitado.

“Hoy contamos con un tercio más de las que teníamos apenas hace cinco años, la inversión en aviones Hércules de transporte pesado, en helicópteros, en aeronaves de reconocimiento, de entrenamiento y de caza”, destacó.

Puntualizó que de 2013 a 2017, se han invertido más de 28 mil millones de pesos en infraestructura, aeronaves y equipamiento, por ello la FAM es una institución adiestrada y equipada para estar en posibilidades de cumplir las misiones encomendadas para la seguridad del país.

El instituto aéreo armado, cuenta con 7 mil 569 efectivos (7 mil 521 hombres y 48 mujeres), tiene a lo largo del territorio nacional 18 bases aéreas distribuidas de manera estratégica.

El sistema educativo militar aéreo cuenta con mil 741 estudiantes (mil 657 hombres y 84 mujeres), distribuidos en sus plan-

teles de Jalisco (Base Militar No.5) y el Estado de México (Base Militar No. 1).

El Presidente señaló que se debe reconocer a todo el personal de las Fuerzas Armadas. “La entrega y compromiso de los más de 270 mil, soldados pilotos y marinos, merecen el respaldo corresponsable, y sin regateos de la población a la que resguardan, eso incluye asegurar una buena calidad de vida para ellos y sus familias”.

Por otra parte, el Presidente inauguró la unidad militar de Santa Lucía 3, la cual inició su construcción en junio de 2017 y terminó en diciembre del mismo año, la Inversión total superó los 84.2 millones de pesos.

Las instalaciones están conformadas por cuatro edificios departamentales, una oficina de administración, un tanque elevado y una planta de tratamiento de aguas residuales.

Con esta suman ya 40 nuevas unidades habitacionales entregadas al personal militar.

- Con 2 mil 563 viviendas, 12 mil 825 personas beneficiadas
- De 2012 a 2017, se han otorgado 18 mil 304 créditos para vivienda al personal del Ejército y Fuerza Aérea Mexicana.
- De 2014 a 2017, se han destinado más de 460 millones de pesos en becas para que el personal militar realice estudios en México y en el extranjero.

En la ceremonia de aniversario, el Comandante de la Fuerza Aérea Mexicana (FAM), el General de División Diplomado del Estado Mayor, piloto aviador Miguel Enrique Vallín Osuna, anunció que las operaciones de la FAM, se trasladarán a las instalaciones del nuevo Aeropuerto Internacional de la Ciudad de México.

“Ese cambio nos permitirá convertir a Santa Lucía en una Base Aérea especializada en helicópteros, así como llevar otras operaciones a nuevas instalaciones en Querétaro, y en el Colegio del Aire en Zapopan, Jalisco”, mencionó el Comandante de la FAM. **ms**





FIRE + EFFICIENCY + SAFETY + SECURITY + DRONES

Nuevo pabellón
de **Drones**

Nuevo pabellón de
Tecnologías Contra Incendio

Gran enfoque en
Soluciones TI

**SOLUCIONES INAGOTABLES DE TECNOLOGÍA
LA MAYOR EXHIBICIÓN DE LA REGIÓN**



+ Información ESS

Organizan:



Apoyan:



Media partners:



Bradbury y su peligroso pronóstico futurista

1 de 2 partes



“Un día en la estación de bomberos, los bomberos reciben una llamada que una anciana ha guardado libros en su casa. Los bomberos corren hacia su casa y comienzan a destruir el contrabando. Montag le pide a la mujer que salga de la casa porque toda la casa será destruida, pero ella se niega a dejar sus preciosos libros. La casa, junto con la anciana y sus libros, está en llamas, pero no antes de que Montag se robe uno de los libros (la Biblia)”.

Este es uno de los fragmentos medulares del libro futurista de Ray Bradbury titulado Fahrenheit 451. El mensaje de la obra es directo y claro: leer significa pensar y pensar te hace infeliz, por ello no debes pensar.

Brevemente explicaré que la trama de este libro gira en torno a Guy Montag, un bombero encargado de quemar los libros por orden del gobierno. Un día conoce a Clarisse McClellan una chica que vive al lado de su

casa, esta le hace reflexionar acerca de si es feliz o no, confuso y ya con dudas sobre si los libros son buenos o no, decide robar uno cuando van a quemar una casa. Días más tarde Clarisse desaparece.

En Fahrenheit 451, los bomberos no apagan incendios, por el contrario, los provocan cada vez que ubican un cúmulo de libros o bibliotecas enteras, el objetivo es destruir los libros en busca de un mundo feliz y que los ciudadanos dejen de pensar.

El nombre del libro hace referencia a la temperatura en la escala de Fahrenheit a la que el papel de los libros se inflama y arde, equivalente a 232,8 °C. La película homónima basada en esta obra

fue realizada en 1966 y dirigida por François Truffaut.

Para aclarar las cosas, Fahrenheit 451 es una novela distópica (que es la representación imaginaria de una sociedad ficticia e indeseable en sí misma con características negativas), publicada en 1953. A Bradbury se le destaca porque fue un escritor de misterio, del género fantástico, terror y ciencia ficción.

Dentro de su trama, después de unos días leyendo Montag estaba buscando a alguien que le guiase en cuanto al tema de los libros, su contenido y su poder, recordó que hace un año estuvo hablando con un hombre que sabía del tema, el profesor Faber, este le dio su dirección y Montag aún la guardaba, fue a su casa (con la Biblia) y habló con él.

Poco a poco la situación se volvió intolerable, comenzaron a salir más casas con libros, los helicópteros del gobierno comenzaron a bombardear la ciudad, Montag decide huir a casa de Faber, la situación se había salido de control, deciden verse en el río cercano a la ciudad. Al llegar se encuentra con unos antiguos profesores y su ‘líder’ Granger, quienes buscan difundir sus conocimientos, y le explica que cada uno ha memorizado un texto de un libro para compartirlo, lo que, sin saber, es el comienzo de una nueva vida, de un mundo mejor...

El mensaje de Fahrenheit 451 es reflexivo y semejante a otros libros tales como:

- Un mundo feliz
- 1984
- Quema de libros
- Censura
- Libertad de expresión. m's

(Continuará...)



* **Pedro Venegas Chávez**
México

Es un comunicólogo con más de 25 años de experiencia dentro y fuera de los medios de comunicación. Se ha desempeñado como analista y consultor del gobierno federal, ha sido asesor en Evaluación de Imagen Institucional y Prospectiva de varios Secretarías de Estado. Además es editor en jefe de varias publicaciones políticas, columnista y articulista. Es especialista en temas de seguridad a través de su experiencia adquirida en la mayoría de las dependencias donde ha trabajado encargadas de la Procuración de Justicia y la Seguridad Pública.



APRINSA
www.aprinisa.com

Fabricante de
tecnología
menos lesiva



Guante eléctrico modelo Defender APN

- Provee incontables ventajas, ya que su funcionamiento se basa en el término "mano vacía" (defenderse sin armas)... ¡Lo máximo!
- Fabricado con tecnología de última generación.
- Su diseño ergonómico y comodidad es su secreto, fabricado con espadex reforzado con micro fibra lo hace un guante muy fresco.
- La protección en falanges es de material TPU, protección en nudillos, puños de neopreno y cierre de velcro.
- Provee 2.2ma, con voltaje a 8kv, crea un gran efecto disuasivo y su desempeño es único.
- Su funcionalidad es asombrosa al usarse de respuesta defensiva de acuerdo al uso de la fuerza.
- Producto para cuerpos de seguridad privada y pública.
- Ventas a gobierno o empresas de seguridad privada.
- Un producto mexicano y exclusivo de la empresa APRINSA (MR).
- Patente en trámite.

www.aprinisa.com

Correo: venta@aprinisa.com

Tel. (33) 3642-0693 y 3641-5684

Multiproseg

A quien **valor** merece



Guardias



**Custodia
de mercancía**



Tecnología



**Análisis
de riesgo**



Tel. 5594 5513

Av. Armada de México 1500, Residencial Cafetales C.P. 04930 Deleg. Coyoacán
info@multiproseg.com.mx www.multiproseg.com.mx