

REVISTA

XtremSecure®

EL MUNDO DE LA SEGURIDAD

blu!

@  tiLatina

   www.tilatina.com



VIDEOVIGILANCIA Y ALARMAS

PREVENCIÓN DEL DELITO Y LA TECNOLOGÍA

Multiproseg

A quien **valor** merece





V GUARDIAS INTRAMUROS

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



V CUSTODIA DE TRANSPORTE

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



V SISTEMAS ELECTRÓNICOS DE SEGURIDAD

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



V ANÁLISIS Y EVALUACIÓN DE RIESGOS

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

¡Contáctanos!

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

☎ 5594.5513 | 5594.5759 | 5603.0497

EDITORIAL

El uso de tecnología en materia de seguridad ciudadana es una práctica cada vez más aceptada y utilizada en México. En el país se invierten elevadas sumas del presupuesto público en la adquisición de estos productos que se consideran "eficaces" y menos intrusivos, sin embargo, aún no se cuenta con evaluaciones que permitan conocer sus diferentes efectos, tanto positivos como negativos, y ni siquiera se conoce con certeza la prevalencia de este tipo de tecnologías.

Paralelamente, los hogares mexicanos ante la inseguridad y el temor a ser víctimas del delito recurren a diferentes medidas de protección entre las que se encuentra el uso de la tecnología. Existen diferentes motivos por los cuales las familias deciden invertir en medidas de protección para sus propios hogares. Al respecto, uno de los principales cuestionamientos es si se invierte en éstas como una medida preventiva, o como una medida reactiva cuando alguno de los miembros del hogar ha sido víctima del delito.

En los hogares el miedo que las personas sienten a ser víctimas de la violencia o delincuencia es tal que se ven en la necesidad de hacer algo para protegerse individual y familiarmente. En algunos casos se trata de acciones que podrían calificarse como positivas, pero también hay algunas medidas que generan efectos negativos.

Estimado lector no olvide mandar sus colaboraciones, sugerencias o comentarios a cvillatoro@xtremsecure.com.mx



Septiembre - Octubre 2019

César Villatoro Ramírez
DIRECTOR GENERAL

Mariano Botey Hernández
DIRECTOR EDITORIAL

Gabriela Sánchez
GERENTE COMERCIAL

Jazmín Rodríguez González
CREATIVIDAD & DISEÑO

Voces de Seguridad
WEBMASTER

Eréndira Hernández Cruz
REDACCIÓN

Publicaciones GBM
DISTRIBUCIÓN

Tomás Foltyn
Edgardo Frigo
Teodoro A. Serralde Medina
Rafaela Silva
Kurt Measom

COLABORADORES EN ESTE NÚMERO

52 (55) 7663 3711
52 (55) 52 07 47 04
VENTAS

cvillatoro@xtremsecure.com.mx
COMENTARIOS



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

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

Se distribuye con circulación controlada y calificada. C2019. Todos los derechos reservados. Prohibida la reproducción total o parcial por cualquier medio, incluso los electrónicos sin autorización por escrito de los editores. La información ha sido obtenida de fuentes que se consideran fidedignas, pero en ningún caso deberá considerarse como recomendación para adquirir o utilizar bienes o servicios. El contenido de los anuncios es responsabilidad del anunciante. Editor responsable: César Leobardo Villatoro Ramírez. No. de Certificado de Reserva otorgado por el Instituto Nacional del Derecho de Autor 04-2008-041411145200-102. No. de Certificado de Licitud de Título 14085. No. de Certificado de Licitud de Contenido 11658. Domicilio de la publicación: Londres 75 Desp 401-E Col. Juárez, C.P. 06600 CDMX, Impreso en Ciudad de México.

Impresora Litho Signus, SA. de C.V. tiraje 14,500 ejemplares distribuidos en toda la República Mexicana en oficinas y exposiciones. PUBLICIDAD. Para contactar con los ejecutivos de ventas o solicitar información sobre tarifas y espacios publicitarios, comuníquense al Cel. (55) 7663 3711, Tel: 5207 4704, ó escriba a: cvillatoro@xtremsecure.com.mx

DIRECTORIO

CONTENIDO

SEPTIEMBRE - OCTUBRE - 2019



www.videovigilanciamx.com

33

VIDEOVIGILANCIA



www.electronicaytecnologia.com

47

ELECTRÓNICA Y TECNOLOGÍA



www.controldeaccesosmx.com

61

CONTROL DE ACCESOS



www.seguridadindustrialmx.com

69

SEGURIDAD INDUSTRIAL



www.ciberseguridadmx.com

79

CIBERSEGURIDAD

SÍGUENOS EN REDES SOCIALES



www.facebook.com/revistaxtremsecure



www.twitter.com/xtremsecure



www.youtube.com/xtremsecure

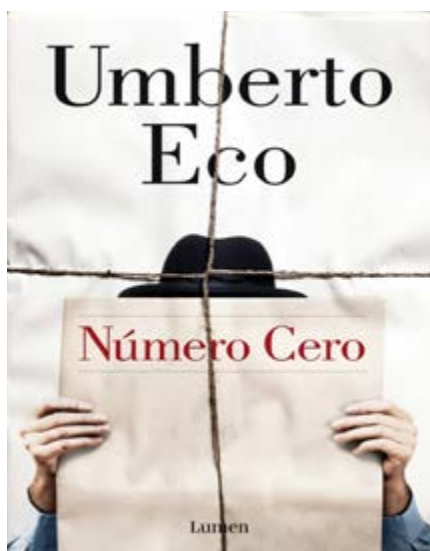
LA SEGURIDAD DE LEER

Por Mariano Botey, mboteyh@gmail.com



NÚMERO CERO

de Umberto Eco, Editorial Lumen, 2015, México.



No es cuestión de azar ni de suerte que la gente olvide mañana, lo que hoy leyó. Un periódico sea el referente con mayor ironía, aunque “el destino de un diario es parecerse a un semanario. Hablaremos de lo que podría suceder mañana, con tribunas de reflexión, reportajes de investigación, avances inesperados”; pero leemos extractos fugaces por falta atención, y paradójicamente seguimos extraviados de lo que acontece el día, ya sea por estar desinformándonos a través de las “sociales” redes, o porque no se publica lo que podría ser noticia con relación a la educación, sea el único tema que no engaña, pues sospecho que lo más relevante quede en el tintero del mañana en los archivos del después. “A nuestros lectores hay que tranquilizarlos, no alarmarlos”. Habría que tejer de la mano de obra del periodista artesano, un nuevo periodismo, desde una profunda crítica de la realidad cotidiana, con nexos a la realidad virtual. “Las sospechas nunca son exageradas. Sospechar, sospechar, solo de este modo se encuentra la verdad”. No podemos comunicarnos por separado, porque a veces damos por hecho, datos que no se verifican, arriesgándonos a perdernos en navegar en la red. “Vivimos

en la mentira, y si sabes que te mienten, debes vivir instalado en la sospecha”. No son cosas distintas; somos nosotros quienes no estamos empleando el instinto que nos hace distintos. Este sea un mundo posible para el futuro de un buen periodismo. Esta novela es imprescindible para el estudiante de Comunicación y Periodismo, donde el semiólogo Umberto Eco trasciende la orientación del buen oficio y lo que se tiene que hacer bien: investigar con buen criterio; y con tinte irónico: hacer un periódico que no se publicará: Número Cero. “Leer manuscritos que jamás serán publicados puede llegar a ser un oficio”. Jugar con esa mágica palabra, la que nunca muere o la que no existe en la incertidumbre: esperanza, en esa espera que todos aguardamos, y que esos periodistas que han estado de fracaso en fracaso, persistan su trabajo con profesionalismo y actitud de un nuevo día: borrón y cuenta nueva y seguir escribiendo, un día cero sea una nueva oportunidad, un número cero porque “se puede tener la fecha que se quiera”, y claro está, en ese periódico desde la imprenta de la ironía: Domani (que significa: mañana) esa esperanza se prolonga o replantea cuando surge un romance entre el experimentado periodista Colonna y la joven Maia; vaya paradoja del periodismo, se aprende de aquellos talladores de la palabra y quienes saben amar su oficio aún en los escollos del sufrimiento, porque para aflorar la verdad; “Los perdedores, como los autodidactas, tienen siempre conocimientos más vastos que los ganadores. Si quieres ganar tienes que saber una sola cosa y no perder el tiempo en sabértelas todas; el placer de la erudición está reservado a los perdedores. Cuanto más sabe uno, es que peor le han ido las cosas”. Se tiene que pasar a prueba los metales pesados de la duda y los andenes de la crítica. “Tengan en cuenta que hoy en día para rebatir una acusación, no es necesario probar lo contrario, basta deslegitimar al acusador”. Esta novela de Eco nos refleja un boceto del periodismo tan complejo e inverosímil, aunque con tintes

reales que salpican el piso de la realidad; hay quienes se delatan ensuciando sus pasos y se encubren con sandalias de la ficción; hay otros que caminan sin miedo porque se conducen con la información veraz, en esa ética profesional; así es Umberto Eco, verificando el dato, y puliendo el signo; así es este último libro, que tenía pendiente como buen periodista: crítico y analítico. Esta novela es meramente una crítica a la prensa menguada y de periodistas que se prestan al mal uso de la información, entre chantajes y extorsión. ¿Habría una diferencia en nuestro país con respecto al periodismo y el periodista? Sea menester lo que anticipó Eco en controlar la veracidad que está en la red; pues será ardua tarea para quienes estén en esas nuevas rutas del periódico tradicional: seguir siendo en el futuro, garantes de la democracia, la libertad y la pluralidad. Las noticias después de todo, no son necesarias inventarlas sino darle un reciclaje, con certeza será nota del momento: “La gente tiene una memoria corta. Les voy a proponer un ejemplo paradójico: todos deberían saber que Julio César fue asesinado en los Idus de marzo, pero las ideas al respecto son confusas; buscamos entonces un libro inglés reciente en el que se reconsidere la historia de César y con eso sacamos un titular de impacto, «clamoroso descubrimiento de los historiadores de Cambridge. César fue asesinado verdaderamente en los Idus de marzo”. Contamos la historia de nuevo y ya tenemos una noticia pistonuda”. El itinerario periodístico de Umberto Eco, lo registra la antología “Diarios mínimos”, y “Segundo diario mínimo”, por mencionar algunos. La tarea de un periodista no es tan fácil ejecutarla; hasta ahora no tiene la seguridad como se presume en escudarse que hay libertad de prensa; Eco nos da una cátedra que no sólo en la ficción suceda sino en la actualidad. “Había perdido todas las certezas, salvo la seguridad de que siempre hay alguien a nuestras espaldas que nos está engañando”.

SEGURIDAD PRIVADAMX



REVISTA DIGITAL

ESPECIALIZADA EN SEGURIDAD PRIVADA

www.seguridadprivadamx.mx

ASIS CAPÍTULO MÉXICO

“Seguridad y Gobernabilidad”



El pasado 2 de julio se realizó, en la Hacienda de los Morales de la Ciudad de México, la reunión mensual de ASIS Capítulo México. Como en cada ocasión, Pedro Sanabria, presidente ejecutivo del Capítulo, dio a conocer los avances de la asociación durante el mes, el principal de ellos fue el crecimiento de la membresía, que ya llegó a los 420 socios, Xtrem Secure “El Mundo de la Seguridad” estuvo presente en dicha reunión como cada mes.

Sanabria informó de la conclusión del proceso de Certificación en Protección Profesional (CPP) con la participación de 19 alumnos presenciales y dos en línea. También invitó a los asistentes a la Security Week LATAM ASIS 2019, que se llevará a cabo del 13 al 17 de octubre próximo en el Centro Citibanamex.

Como se ha venido haciendo en las reuniones de este año, se entregó un reconocimiento especial a otro de los expresidentes del Capítulo, en esta ocasión fue a Samuel

Ortiz Coleman, reconocido no sólo por su participación como presidente en dicho Capítulo (2009), sino también por su labor informativa en el sector.

La empresa patrocinadora de la reunión fue SERVISEG. Su presidente, Mario Espinosa Boulogne, destacó la trayectoria de la empresa y recordó que está próxima a cumplir su aniversario número 25, siempre trabajando bajo los mismos principios: compromiso, integridad, confianza, trabajo en equipo y cumplimiento.

En esta ocasión, Jorge Tello Peón, experto en seguridad e inteligencia, presidente y director general de Madison Inteligencia México, ofreció una interesante conferencia titulada “Seguridad y gobernabilidad”. El conferencista ha sido Consejero de Seguridad Nacional, Subsecretario de Gobernación y Director General del Cisen, entre otros cargos en el gobierno federal, en donde laboró por más de 20 años.

“No se está haciendo nada para frenar los abusos al pueblo, la inseguridad crece y las empresas de seguridad privada se fortalecen, les va muy bien debido a la inseguridad que a todos nos afecta”, destacó.

El especialista resaltó que el gobierno tiene enormes retos *“cómo hacer crecer la economía, aunado a que el populismo y el nacionalismo reaparecen en todo el mundo. Son tiempos de guardar y observar, las cosas tienen que cambiar, por el bien de todos.”*



Hay muchos niveles de impunidad y muchos delitos no se castigan. En mi opinión, hay poca ciudadanía, los mexicanos reclaman pero no participan, simplemente hay que recordar las pasadas elecciones donde se presentó un abstencionismo del 70 por ciento. Debemos tener cuidado de que México no se divida, hay que mantenerlo unido”.



GECSA

SEGURIDAD PRIVADA



SI LO PUEDES PREVER
LO PUEDES RESOLVER

www.gecsa.com.mx

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

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





GECSA, 20 AÑOS DE PASIÓN POR LA SEGURIDAD



Grupo Empresarial Casa proporciona servicios profesionales y de calidad a toda clase de establecimientos industriales, comerciales y particulares, unidades habitacionales, centros recreativos y educativos, y a cualquier instalación o persona que lo solicite.

Desde su origen, en febrero de 1999, **GECSA** ha sido dirigida por José Carlos Sánchez Guzmán, mejor conocido como "El capitán". Ingresó al Colegio Militar a los 15 años y se graduó, como subteniente de infantería, en 1980. Posteriormente llegó a obtener el rango de capitán.

GECSA está cercano al millar de empleados y presta sus servicios en toda la república mexicana. "En la actualidad, nos dice el capitán, una empresa de seguridad es muy rentable, pero hay que darle seriedad y respeto. Cuando uno forma una empresa de seguridad, tiene obligaciones y derechos, una de esas obligaciones es pagarle a tu gente en tiempo y forma. El principal recurso de las empresas es su personal, y es al que más se le somete a veces. Pagar tus impuestos y el Seguro Social, eso también es respetar. Respetar a tu personal como una empresa socialmente responsable. Por eso digo: Respeten lo que les da de comer".

Un plus que entrega **GECSA** a sus clientes es, sin lugar a dudas, la atención personalizada, siempre a cargo del capitán: "Muchos creen

que cuando se es dueño de una empresa se trabaja de eso, de dueño, pero no, yo siempre platico con mis clientes y tengo una buena comunicación con ellos, y dicen que eso les gusta, que yo mismo les resuelva sus problemas y los atienda”.

Sobre los retos que enfrenta la industria, el capitán nos comenta: “Sin duda, el principal reto es la profesionalización, después la capacitación y la administración. Esos creo que son los principales retos no sólo de las empresas de seguridad, sino de cualquier empresa. Actualmente, el principal problema que tenemos es la competencia desleal, por un lado de las empresas patito, que sólo enturbian el mercado, abaratando costos y bajando el nivel de los servicios. Y por otro lado, las corporaciones policiacas que los gobiernos de los estados rentan como guardias privados, y que luego usan como cajas chicas. Ahora habrá cambios, y quizá eso afecte a muchas empresas de seguridad privada”.

Sobre el cambio de gobierno, el capitán fue claro al decir: “Con la famosa 4t ha habido cambios muy importantes, y principalmente se reflejan en la morosidad que ha habido desde el pasado primero de diciembre. La incertidumbre que estamos viviendo por la cuarta transformación perjudica a muchas empresas, entre ellas las de seguridad. Como sugerencia puedo decir que no nos resta más que trabajar, cuidar nuestro trabajo y seguir adelante. Si sigue esto así, Yo creo que no pasamos de un año”.

Xtrem Secure.- ¿Ha tenido que hacer ajustes para enfrentar estos cambios?

Cap. José Carlos “Claro que tuvimos que hacer ajustes, ajustes con los clientes y con el personal, ajustes en todo. Los sueldos son primero, son sagrados y esos no deben tocarse. Primero la gente, y entonces uno tiene que hablar con los proveedores y arreglárselas, pero pensando siempre primero en la gente”.

Sobre sus planes, nos comenta: “En diciembre esperamos tener mil empleados, y tener la empresa de guardias armados. Para el 2020 esperamos trabajar fuera de la república mexicana. Este año ya estuvimos en platicas en Perú y Panamá para ofrecer los servicios, pero no se concretaron esos acuerdos, sin embargo, sentaron los primeros pasos para la internacionalización de la empresa”.

Xtrem Secure.- ¿Cuándo usted fundó GECSA hace 20 años, pensó que llegaría hasta donde está, y



sobre todo que estaría toda su familia involucrada en ella?

Cap. José Carlos “No, la verdad no. En la vida militar yo siempre fui una persona de choque, yo no era de los inteligentes. En el Colegio Militar me reprobaron en matemáticas y hasta me arrestaron durante 15 días por eso. Salí y no fui un militar purificado, siempre me decían lo que tenía que hacer. Cuando ya era oficial en el ejército no me gustaba que me mandaran, entonces pensé que debía buscar una forma de no depender de nadie, y no me equivoqué de profesión, soy militar de corazón y si volviera a nacer, volvería a ser militar”.

“Tuve la idea de hacer la empresa cuando fui director del Colegio de Policía. Esta empresa empezó dándole seguridad a todas las unidades habitacionales militares, casinos y cementerios militares, así empezó. En ese tiempo GECSA nada más trabajaba para el ejército, luego comenzamos a darle el servicio a Kimberly Clark, con cuatro guardias, y con el tiempo llegamos a tener 300 elementos con ese cliente”.

“Nunca pensé que se integraría mi familia, y ahora es una empresa 100 por ciento familiar, mi esposa es la subdirectora y es mi socia, y mis hijas, una es gerente de operaciones y la otra de administración, pero nunca pensé que así sería... y no me arrepiento”.

Para finalizar, le preguntamos sobre sus sentimientos con respecto a la empresa que dirige, y esto fue lo que nos dijo: “Es una satisfacción muy grande, sobre todo cuando uno va a cualquier parte de la república y encuentra gente que reconoce nuestro trabajo. Me apasiona la seguridad, y siempre me ha apasionado. También doy clases en Protección Federal, en ASIS, y me la paso muy bien conviviendo con los alumnos. Me gusta estudiar y compartir el conocimiento. No, no me arrepiento, y le doy gracias a Dios, día a día”. **XS**



Las Certificaciones Internacionales más **IMPORTANTES EN SEGURIDAD**



Durante la reunión mensual de la AMEXSI, celebrada el pasado 25 de julio, tuvimos la oportunidad de escuchar las experiencias de los que se han atrevido a participar y aplicar por las certificaciones internacionales más importantes en seguridad.

En la reunión también se reconoció, como El mexicano del mes, al Lic. Gerardo de Lago Acosta, por su extraordinaria aportación a la sociedad y en concreto al gremio de la seguridad.

El Lic. Gerardo de Lago cursó la carrera de Químico Farmacéutico Biólogo (QFB) en la Universidad La Salle, iniciando inmediatamente su carrera en Procter & Gamble, donde durante 15 años desarrolló puestos como gerente de Relaciones Laborales, gerente de Producción y gerente de Administración de Riesgos, hasta convertirse en el gerente de Security para Latinoamérica Norte con responsabilidad por la seguridad de todas las operaciones de P&G en México y Centroamérica, posicionándose como el experto regional

para Latinoamérica en temas de Planeación de Continuidad de Negocios y como Responsable del establecimiento del estándar de Equipo Electrónico de Seguridad.

Actualmente el Lic. de Lago es el director de la División de Consultoría de Pretorian Specialized Security Services, firma especializada en seguridad con base en la ciudad de México. Cuenta con el grado de Profesional Certificado en Protección (CPP) de ASIS, y completó recientemente una maestría en Homeland Security por la Universidad de Phoenix.

En esta ocasión se presentó un panel de experiencias sobre las certificaciones de ASIS Internacional, los que ya acreditaron y los que se están preparando. Arturo Martínez



Emmanuel González Sojo, Director General de Uniformes JR.

10 años

Gracias por tu confianza

CONTAMOS CON COBERTURA
A NIVEL NACIONAL



SEGURIDAD PRIVADA

▶ **VIGILANCIA
INTRAMUROS**

▶ **CUSTODIAS**

▶ **SEGURIDAD
ELECTRÓNICA**

▶ **MONITOREO Y RASTREO
VEHÍCULAR**

Tel. (0155) 5916-5931

laadukalmekak@hotmail.com • laadu@laadusp.com

cpromo@laadusp.com • ventas@laadusp.com



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



Jorge Romo, CPO, DSI, Director General de LK Seguridad Privada

Avalos, presidente de la AMEXSI, moderó esta conferencia atípica, que tuvo el objetivo de compartir el conocimiento y las experiencias de aquellos que han pasado por un proceso de certificación.

El Ing. Alejandro Barrera, CPP, PCI, PSP, se refirió a los motivos que le hicieron decidirse a optar por el proceso de certificación: “Bueno, yo creo que como la mayoría de nosotros, que tenemos diferentes profesiones, de alguna manera todos debemos dejar de ser profesionistas y convertirnos en profesionales. Y precisamente buscando esa evolución a través de estándares

establecidos, así que indagando me encontré con que ASIS es una extraordinaria fuente de información y pues busqué una certificación reconocida, ese fue el camino”.

Por su parte, el Lic. Arturo López Novoa, CPP, recomendó a quienes se están preparando para obtener una certificación: “Hay que leer mucho, y estar preparados, yo les recomendaría formar grupos de trabajo, con amigos o colegas, para estudiar y compartir información”.

El Lic. Gustavo Espinosa Vázquez, DSI, DSE, nos platicó cómo fue el proceso de preparación para obtener la certificación, aunque desafortunadamente no la ha logrado hasta el momento: “Bueno, previo al examen uno tiene una gran presión y son muchos sentimientos encontrados porque uno invierte tiempo en prepararse, y dinero, y esfuerzo, pero más allá de eso, creo que uno tiene que esforzarse no al 100 por ciento, sino al 120 por ciento. Sí hay un sentimiento de frustración cuando el resultado no es el que uno esperaba, pero también hay se echarse para adelante y seguir. Ahorita tenemos un grupo de trabajo en el que nos estamos preparando para la siguiente certificación”.

Enriquecedor y ágil fue este ejercicio de comunicación, que esperamos se repita con frecuencia.

En esta ocasión, el evento de la AMEXSI fue patrocinado por Uniformes JR, empresa con más de 11 años en el mercado y con una sólida reputación.

ALAS en Santo Domingo y Bogotá

En la semana del 5 al 10 de agosto, la Asociación Latinoamericana de Seguridad realizó de forma casi simultánea eventos en República Dominicana y en Colombia (sumado a los eventos que se realizan en México que tienen mayor periodicidad).

El 8 de agosto, se llevó a cabo en Santo Domingo el Encuentro Tecnológico ALAS en el hotel Barceló. Como siempre, la capital dominicana respondió con una asistencia masiva, consolidándose así como una de las plazas más importantes para la Asociación en lo que a actividades se refiere. 106 asistentes se dieron cita en el evento, lo que muestra un crecimiento del 24% con respecto al año anterior, entre los cuales se

encontraban, además de los integradores y otros integrantes de la cadena, usuarios finales importantes como: Sistema Nacional de atención a Emergencias 911, Grupo Puntacana, Cámara de Comercio y Producción de Santo Domingo, Dirección General de Aduanas, Pinewood Dominican Republic Studios (PWDR), entre otros.

El encuentro contó con la exposición tecnológica de marcas como NVT Phybridge, BOSCH, CDVI, Softguard, Spark, BCD Video, KBC Networks y con una amplia agenda académica.

Al día siguiente en Bogotá se realizó un desayuno ALAS enfocado en el mercado vertical de hotelería. Si bien los desayunos

son eventos más cortos y más pequeños, la asistencia de cerca de 70 personas sorprendió gratamente a patrocinadores y organizadores, mostrando que en Colombia se viene haciendo un trabajo en el que la Asociación va tomando protagonismo en el mercado y volviéndose cada vez más relevante como punto de encuentro. La presencia del gremio hotelero se vio representada por el Grupo de Hoteles GHL, Cotelco Nacional Asociación Hotelera y Turística de Colombia, Grupo Oxohotel, EK Hotel, Hotel Dreams Dominicus, Hoteles Charleston entre otros. El evento, que se desarrolló en el Hotel Sonesta, contó con la exposición de Hanwha, Johnson Controls y Mircom.



Jornada “MUJERES EN SEGURIDAD”



La lucha por la paridad de género ha sido constante desde hace décadas, en el caso de la seguridad pública y privada en México, a pesar de que las mujeres trabajan a la par de los hombres, aún existen grandes retos para lograr la igualdad de oportunidades.

En nuestro país existen más de 2 millones de puestos de trabajo en materia de seguridad y ciberseguridad; sin embargo, en los puestos directivos en estos rubros, tan sólo el 2 por ciento son ocupados por mujeres. Este es el contexto se realizó la primera jornada de Mujeres en Seguridad, un panel de especialistas que busca discutir las principales problemáticas que enfrenta México con respecto a la seguridad y las oportunidades para las mujeres en el sector.



La jornada se llevó a cabo el pasado 16 de julio en las instalaciones de la UDLAP Jenkins Graduate School en la Ciudad de México, y contó con la participación de la Dra. Patricia Trujillo Mariel, coordinadora operativa de la Guardia Nacional; la Mtra. Maribel Cervantes Guerrero, secretaria de Seguridad del Estado de México; Ana Elisa Santos, gerente de Corporate Security en BASF México; Lourdes Morales Aguilar, manager supply chain security de América en Walmart; y María Teresa Septién, directora ejecutiva para Latinoamérica en AFIMAC Global.

En su intervención en el panel de expertas, María Teresa Septién aseguró que el principal reto para las mujeres, en puestos directivos en empresas de seguridad, es poder demostrar su talento como profesionales: “Siempre ha existido el estigma de que la seguridad es un tema exclusivo para hombres, lidiar con esa cultura y cambiar esa mentalidad, es un reto al que se han tenido que enfrentar las mujeres dedicadas al tema de la seguridad”.

Por su parte, Lourdes Morales Aguilar, primera mujer en ocupar un puesto de seguridad gerencial en Walmart, señaló que “para romper estos paradigmas en la sociedad no sólo es necesario llegar a ocupar puestos directivos, sino también, desde esas posiciones, abrirle camino a otras mujeres”.

En la jornada, la Mtra. Maribel Cervantes impartió la conferencia magistral “Violencia contra las mujeres”, en la que habló sobre la estrategia llevada a cabo en la Secretaría de Seguridad del Estado de México para combatir los feminicidios y las violaciones.

“Para combatir la violencia contra las mujeres es necesario fomentar la cultura de la prevención, la cual debe empezar desde casa”, aseguró. “Debemos tener una estrategia para reconstruir la comunidad y el tejido social, las familias y sus hogares. Volver a hacer del hogar un lugar seguro”.



El pasado 24 de julio se realizó, en instalaciones de la Universidad Panamericana, la presentación del Diplomado en Desarrollo de Empresas de Seguridad Exitosas y Sustentables, creado por la ASUME, la Universidad Panamericana y el High Potencial Development Center, dirigido principalmente a empresarios y directores de compañías de seguridad.

Durante el evento, Armando Zúñiga Salinas, coordinador general de Agrupaciones de Seguridad Unidas por un México Estable (ASUME) aseguró que: “Con el afán de seguir cultivándonos, y cultivando a nuestro sector, surge la idea de crear este diplomado como una de las acciones para unir más a los miembros del sector de la seguridad, al igual que lo es el impulso a la Ley Federal de Seguridad Privada y a la creación de una cámara que verdaderamente nos represente y nos dé certeza a todo el sector”.

“Hoy estamos aquí por otro objetivo, que se refiere a la formación, a la capacitación como empresarios. Nuestro sueño, y espero que lo compartamos todos, es que este sector sea admirado y respetado por muchos, porque cumplimos un objetivo fundamental para la seguridad en nuestro país, dando certeza a las inversiones y a las empresas”.

“El diplomado tiene como fin incrementar la competitividad de las organizaciones a través de un proceso de mejora continua, personal y organizacional. Los participantes estudiarán los elementos clave que intervienen en la generación de valor de una compañía y su interacción entre ellos y con las variables del entorno”.


El diplomado tendrá una duración de 120 horas y estará dividido en seis módulos:

1. Estructura financiera sana. Con la finalidad de generar finanzas sanas en el negocio, el participante comprenderá la interrelación e influencia que existe entre la micro y la macroeconomía.
2. Formulación e innovación del modelo de negocio. El estudiante aprenderá a construir o reconstruir el modelo de negocio de la empresa e identificar los procesos de innovación necesarios para robustecerlo.

DIPLOMADO

en Desarrollo de Empresas de Seguridad Exitosas y Sustentables

3. Mercado y relación con los clientes. El alumno analizará las variables que intervienen en el diseño de una estrategia comercial innovadora y exitosa, tomando en cuenta las capacidades de la empresa y las oportunidades de negocio.
4. Dirección y sus procesos. El profesional identificará el papel de la dirección y sus procesos en las acciones de mejora continua e innovación, de tal forma que se convierta en un agente de cambio y sea el principal impulsor del éxito de la empresa.
5. Efectividad organizacional. El participante aprenderá a definir las estrategias necesarias para la construcción de una organización efectiva y así poder determinar las prioridades en el plan de negocios.
6. Sustentabilidad de las empresas. El alumno estudiará la forma de sostener un negocio en el tiempo y hacerlo crecer con sus propios resultados, al tiempo que opera como una empresa socialmente responsable.

El Diplomado comenzará en septiembre de este año y concluirá hasta marzo del 2020. Las inscripciones siguen abiertas. 



Tu seguridad
desde una
nueva
perspectiva



Fotografía: Cristian Jonathan Reyes

Síguenos:



5525 3242

grupopismexico.com



GRUPO IPS MÉXICO
GARANTÍA EN SEGURIDAD



Diplomado de PROTECCIÓN A CICLOS PRODUCTIVOS

El Operador Económico Autorizado (OEA), es un programa voluntario que busca fortalecer la cadena logística internacional a través de la implementación de estándares mínimos de seguridad y normativa aduanera, adaptándose a las necesidades de cada país, contra la contaminación de la carga comercial con drogas, armas y dinero, personas, mercancías prohibidas, sustancias peligrosas o utilizadas para el terrorismo, entre otros.

Recientemente, México ha decidido involucrar a la Policía Federal en la protección a la cadena de suministro, siguiendo el ejemplo de países como Colombia, donde OEA está a cargo de la Dirección de Impuestos y Aduanas Nacionales en conjunto con la Policía Nacional a través de la Dirección Antinarcoóticos.

El Consejo de Seguridad en Cadena de Suministro y la división de Gendarmería de la Policía Federal, iniciaron hace aproximadamente tres años un diplomado de protección a ciclos productivos de 140 horas, con el objetivo de homologar criterios con respecto a la gestión de seguridad en cadena de suministro conforme a ISO 28000.

Implementarlo, permite que industria y autoridad, trabajen en un esquema de responsabilidad compartida, al sensibilizar a los elementos policiacos con respecto al impacto de cuidar nuestras fronteras, la gestión del riesgo, normas mexicanas de

seguridad, y facultades del SAT ante mercancías extranjeras ilícitas, riesgos en las cadenas logísticas aeroportuaria y portuaria marítima.

En ese contexto, el pasado 18 de julio se impartió el módulo de ISO 28000 del diplomado, en las instalaciones de la Universidad La Salle de Neza, donde Eduardo Hernández Ruiz, presidente del Consejo de Seguridad en Cadena de Suministro, presentó el módulo y dio la bienvenida a los asistentes.

Por su parte, José Ángel Vidaña Meraz, vicepresidente del Consejo de Seguridad en Cadena de Suministro, habló de la gestión estratégica de proyectos de seguridad en la cadena de suministro conforme la norma ISO 21500 y Jaime Mancera Aguilar y Eduardo Hernández Ruiz presentaron la ponencia "Aplicación en la práctica de la nueva norma de seguridad en cadena de suministro Proy-NMX-W-188-SCFI en todos los sectores productivos del país".

También participó el Dr. Mario Arroyo Juárez, del Instituto Iberoamericano de Seguridad privada, que presentó la ponencia "Seguridad: la clave para la competitividad y el desarrollo" y, finalmente, Miguel Ángel Osuna Rodríguez, de Red PBIP, quien habló del Código de protección a buques e instalaciones portuarias y la norma ISO 28000. **IS**



SEPSA CUSTODIA DE VALORES

Seguridad y Confianza



Sepsa Custodia de Valores es una de las empresas más prestigiadas en nuestro país en lo que se refiere al transporte seguro de mercancías. Fue fundada en 1976 en Monterrey. Años más tarde, en 1988, fue adquirida por Grupo Seguridad Integral.

Actualmente cuenta con más de 1,300 empleados y da servicio en toda la república a través de 13 sucursales propias y, utilizando la infraestructura del GSI, abarca más de 180 unidades de negocio.

Desde 1997 se amplió, de sólo transportar valores, a dar un servicio integral de administración de efectivo, desde suministro a cajeros automáticos hasta el proceso de empaquetado de nóminas. Hoy posee la mejor tecnología, y los mejores procesos, para el manejo de efectivo.

El Ing. Iván Martínez Benítez, director general de **Sepsa Custodia de Valores**, la define así: "Somos una empresa que ha intentado involucrarse en la mayor parte de las áreas de la seguridad. Nacimos como una empresa únicamente de custodia de mercancía, a través de unidades blindadas, y evolucionamos ampliando la gama de servicios al transporte seguro de mercancías, con unidades de carga blindadas, con un esquema de monitoreo, a unidades propias y de nuestros clientes, y también proporcionamos el servicio de guardias de seguridad.

"Somos una muy buena opción para el transporte seguro de mercancía por todo el trabajo que nos avala, por el equipo que conforma la empresa, es un equipo que ha avanzado mucho. Somos la única empresa que maneja una estadística casi nula de robos y es a raíz de eso, de la profesionalización de nuestro personal y a que todos nuestros procesos están certificados".



Xtrem Secure: ¿Qué tan importante es tener una buena comunicación con el cliente?

Ing. Iván Martínez: Desde luego que es importante tener una buena comunicación y, sobre todo, una buena retroalimentación con el cliente. El principal elemento de la seguridad es la prevención, y eso lo hacemos junto con el cliente; antes de iniciar cualquier servicio, platicamos con el cliente sobre su historial de eventos de pérdida para que podamos desarrollar la estrategia adecuada para su protección y, en caso de tener algún incidente, podamos reaccionar de manera adecuada.

Las rutas son dinámicas ya que la delincuencia utiliza diferentes estrategias basadas en lugar y tiempo, por eso debemos alimentar nuestro sistema de planeación de rutas con las estadísticas actualizadas de las incidencias, tanto del producto, como de las autopistas o carreteras, sin olvidar la normativa y reglamentos de tránsito aplicables a cada entidad.

En cuanto al monitoreo, hemos modificado el concepto tradicional a “acompañamiento virtual” que es un híbrido entre el seguimiento activo por medio de un monitorista certificado y los sistemas de alertamiento inmediato en el sistema de rastreo y sus componentes.

Xtrem Secure: ¿Cómo controlan el manejo de la información confidencial?

Ing. Iván Martínez: Tenemos dos estrategias, la parte legal donde damos a conocer al personal las responsabilidades y repercusiones del mal uso de la misma, así como una estrategia de seguridad basada en la redundancia, clasificación y “necesidad de saber”.

Nuestro personal está perfectamente calificado y capacitado. Con un riguroso proceso de reclutamiento nos aseguramos de contar con el mejor personal. La capacitación empieza con el proceso de Inducción a la compañía, luego sigue con un Programa básico con temas como primeros auxilios, derechos humanos, uso de la fuerza, límites de actuación y, desde luego, también incluye prácticas de tiro, procedimientos / consignas, y seguridad en los trayectos.



Xtrem Secure: ¿Qué certificaciones tiene la empresa?

Ing. Iván Martínez: Nos hemos ocupado de reflejar nuestro conocimiento y experiencia en certificaciones que lo avalen, por ejemplo, contamos con las certificaciones ISO 9001:20015, ISO 28001:2007, somos Empresa Socialmente Responsable, y la formación del personal se hace bajo las competencias del sistema CONOCER, por lo que nos hemos convertido en Centro de valuación en los estándares EC0060 Vigilancia presencial de bienes y personas, y del EC0023 Monitores de sistemas de geolocalización.

Somos integrantes activos de la AMESP (Asociación Mexicana de Empresas de Seguridad Privada) lo que nos permite vincularnos con las autoridades correspondientes al ramo, y tener recursos adicionales para la capacitación, así como estrategias conjuntas con otras empresas para el mejoramiento de nuestros procesos.

Nuestro compromiso es ese: la actualización constante de nuestros procesos, y la búsqueda de tecnologías innovadoras en seguridad integral, concluyó el Ing. Iván Martínez. **XS**



TALLER

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



31000 : 2018



28000:2007



21500:2012





Prevención de accidentes y robo en **SUPPLY CHAIN**

En entrevista para Xtrem Secure "El Mundo de la Seguridad" el especialista Hermelindo Rodríguez Sánchez, gerente corporativo de seguridad, puntualizó que las autoridades al verse sobrepasadas por la delincuencia organizada, los empresarios del sector supply chain y líneas de autotransporte, se esfuerzan en desarrollar diferentes prácticas y estrategias para evitar afectaciones en las empresas que representan, con el riesgo de los robos que los afecta de forma importante, ya que cifras del año anterior registran que se incrementó en un 70% el robo en carreteras, debido a esto se han implementado acciones enfocadas a la norma ISO 39001, por lo que a continuación expongo lo siguiente:

Conceptos de Afectación

El registro de incidencia más importante se ha detectado en la parte en que los operadores de transporte son los principales causantes de la problemática, ya que de ellos provienen diferentes situaciones como la fuga de información, la colusión con la delincuencia organizada e incluso el auto robo de sus unidades, por lo tanto nos hemos dado a la tarea de aplicar diferentes medidas como implementar acciones para contrarrestar todas las afectaciones que día a día ocurren en nuestro país, que son accidentes, muertes de operadores, robos y secuestros, por lo que a continuación se relacionan diferentes buenas prácticas para el control de confianza, prevención de accidentes y robos.

1.- Operadores Confiables

Para contar con un buen control de nuestros operadores, se han realizado exámenes de confianza con personal cautivo

y de nuevo ingreso, con pruebas de doping, de grafología, pruebas de confidencialidad y de rostro, así como el apoyo de una empresa de recurso confiable, quien es nuestro aliado mas importante al momento de aplicar los estudios socio-económicos, frecuencias de voz y un sinnúmero de exámenes de confianza, lo que proporciona una garantía para la continuidad del negocio y evitar que haya fuga de información.

2.- Jornadas de trabajo

Anteriormente se contaba en la parte operativa con los operadores, un rol de trabajo de 21 días de trabajo por 7 días de descanso, lo que originaba un alto consumo de anfetaminas y metanfetaminas, que como consecuencia de ello, se contaba con personal enfermo y cansado, aunque les ayudaba un poco el consumo de pastillas, porque no dormían en más de 24 horas continuas, pero no era del todo favorable, por lo cual se realizaron a todos los operadores un estudio toxicológico (doping), lo cual dio como resultado



GRUPO
M  **SEC**
SEGURIDAD PRIVADA ARMADA

MONITOREO Y SEGURIDAD PRIVADA, S.A DE C.V.

Viveros de Atizapán No.1 esq. Sor Juana Inés de la Cruz, Col. Viveros de la Loma,
C.P. 54080, Tlalnepantla, Estado de México

Tels: (01) 55 53901618 | 55 5565 0732 | 55 5556 0812
comercial@moseg.com.mx

www.moseg.com.mx

que todos salieron positivos en el consumo de cocaína y marihuana. Los operadores fueron separados de la empresa de forma inmediata, posterior a esto los que tuvieron positivo con metanfetaminas y anfetaminas, se les dio la opción de continuar trabajando, con la consigna de no consumirlas.

En consecuencia, un servidor implemento la opción de cambio de jornada laboral, que se propuso al consejo directivo del Grupo, un rol de 3 días de trabajo por 3 días descanso, mismo que fue autorizado con la presentación en conjunto de un programa de salud ocupacional, el cual velaría por la salud del personal, el rol de trabajo fue tomado en cuenta con los operadores y les gustó mucho, por lo que el cambio fue instantáneo, de inmediato se empezó a ver al personal motivado al tener la opción de poder de ver más a su familia, de tener un descanso más acorde a su trabajo, y de ya no tomar pastillas, sobre todo porque se estaban tomando acciones médicas con su salud, ya que se aplicó a todos exámenes médicos, saliendo algunos con diferentes afectaciones tales como: glucosa alta, fatiga, anemia, estrés generado por las distancias de origen-destino, hipertensión y síntomas cardiológicos, por lo cual se llevaron a cabo las atenciones a cada uno de ellos, lo cuál pago la empresa. El personal cambió inmediatamente su forma de pensar en referencia a sus patrones y observaron que se estaban realizando acciones por su salud y agradecieron las medidas correctivas, ahora si toda la atención se enfocó en realizar bien su trabajo en carretera.

3.- Prevención de Accidentes

Derivado del programa de salud ocupacional y el cambio de jornadas laborales, la empresa vio cambios importantes en sus ingresos, crecimiento, estabilidad laboral y financiera, así como un personal operativo comprometido y saludable, que originó proporcionar bonos por diferentes modalidades, kilometraje, apoyos, antigüedad y accidentes, por lo que se aplico de nueva cuenta estudios toxicológicos y todos salieron negativos en consumos de estupefacientes y drogas, en la parte de monitoreo se implemento comunicación permanente para reportar tráfico pesado, detenciones autorizadas por



cansancio, por sueño, por zonas desoladas, por zonas rojas, dando como consecuencia que el índice de accidentes bajara de forma importante gracias a una constante comunicación para evitar accidentes y evitar distracciones de los conductores.

4.- Prevención del robo

Una vez que se tuvo buena reacción a nuestras acciones, nos dimos a la tarea de implementar recorridos con los operadores en las diferentes rutas del país, norte y sur, por lo que se realizaron procedimientos de seguridad para la disminución del robo, en primer lugar al contar con operadores confiables que pasaron por diferentes filtros de exámenes, que originaron la permanencia y el ingreso a la empresa, esto ya nos ayudaba a que no habría una fuga de información y colusión con delincuentes, así mismo se realizaron también protocolos de actuación en el caso de robo o intento de robo, adicional al botón preventivo, se instalaron cámaras de videovigilancia y equipo de grabación, también se realizaron paradas autorizadas en coordinación con personal de la policía federal, quienes nos apoyaron en el auxilio y apoyo de supervisión de nuestras unidades. Nos dimos a la tarea de supervisar todas las paradas y con un mapeo de los GPS, tuvimos en cuenta la permanencia de las unidades y con el reporte de novedades del operador, así como las claves estratégicas para cuando tuvieran al delincuente con ellos y en la misma conversación con ellos, lo cual sucedió en un par de ocasiones, saliendo ilesos y con la recuperación de la unidad, todo esto nos dio la confianza de continuar operando de la misma forma.

Conclusión

En conclusión algunas de las acciones tomadas para contar con un recurso confiable, que nos apoye en disminuir el riesgo del robo, así como la tranquilidad del personal en el estado de salud y evitar el consumo de estimulantes, las jornadas de trabajo que fueron muy eficaces para la prevención de accidentes, así mismo se complementa con los manuales de operadores, procedimientos de seguridad y protocolos de acciones, nos dieron la solución a nuestros conflictos de accidentes y robos, de malas acciones de los operadores en contra de la empresa, con el robo de neumáticos, combustible, dinero de viáticos y auto-robos, también contando con la buena coordinación de las autoridades municipales, estatales y federales, que siempre ha sido muy atinada y de buena relación con todos los comandantes de región. **RS**





¡LA CALIDAD
NO ESTÁ EN CONTRA
DEL PRECIO!

UNIFORMES A LA MEDIDA
PARA EMPRESAS DE SEGURIDAD



Federal



Privada



Pública



Militar

CLIENTES
LEALES:



- INFORMES -

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

www.uniformesjr.com.mx



Principios de actuación de los prestadores de **SERVICIOS DE SEGURIDAD PRIVADA**

Por Mtro. Teodoro A. Serralde Medina, teodoro@serraldeconsultores.com

El artículo 152 de la Ley General del Sistema Nacional de Seguridad Pública establece la obligación de que los particulares que se dediquen a estos servicios, así como el personal que utilicen, se registrarán por las normas y principios de actuación previstos en la Ley General del Sistema Nacional de Seguridad Pública. Los principios de actuación se contemplan en los artículos 27 a 35 de la Ley Federal de Seguridad Privada, y se encuentran basados en la legalidad, objetividad, eficiencia, profesionalismo y respeto a los derechos humanos, previstos en el artículo 21, párrafos noveno y décimo de la Constitución Política de los Estados Unidos Mexicanos.

Es importante destacar que los elementos operativos de seguridad privada no tienen el carácter de autoridades, razón por la cual en la exigencia y aplicación de los principios de actuación se debe acotar al respeto de los derechos fundamentales y garantías constitucionales que tiene cualquier particular. De forma principal, los derechos a la intimidad, así como a la protección de los datos personales puede ser un límite de aplicación de las normas y principios de actuación policiales.

De igual manera, el precepto en comento establece la obligación de los prestadores de servicios de seguridad privada de aportar los datos para el registro de su personal y equipo, así como de información estadística y sobre la delincuencia al Centro Nacional de Información.

Si bien es cierto que la obligación de aportar información al Sistema Nacional de Seguridad Pública es fundamental para las instituciones de seguridad, también lo es que dicha aportación de información debe respetar los derechos fundamentales a la intimidad y de protección de datos personales que tienen los elementos de seguridad privada. En ese mismo sentido, desde nuestro punto de vista, debe establecerse una base de datos especializada en prestadores de servicios de seguridad privada,

que sea acorde a la Ley Federal de Seguridad Privada y que permita que se cuente con información actualizada, conforme a la dinámica y realidad de los servicios de seguridad privada.

Actualmente la información de los prestadores de servicios de seguridad privada, en particular de los elementos operativos, es inscrita en el Registro Nacional de Personal de Seguridad Pública, es decir, de elementos de seguridad pública.

De acuerdo a lo anterior, es indispensable que se genere una base de datos nacional con información de los prestadores de servicios de seguridad privada, cuyo registro sea dinámico y acorde a la realidad del sector, la cual es distinta a las instituciones de seguridad pública.

Finalmente, las empresas privadas de seguridad tienen la obligación de que su personal operativo sea evaluado a través de procedimientos de control de confianza. Al respecto, debemos precisar que los controles de confianza no pueden ser iguales a los aplicados a los elementos de seguridad pública, derivado de los derechos a la intimidad y protección de datos personales, antes citados. Aunado a lo anterior, la relación laboral, en el caso de los prestadores de servicios de seguridad, es privada y por lo tanto no puede ser aplicada de forma estricta ya que se afectan derechos laborales, que sólo pueden ser limitados por los tribunales del trabajo y no por una autoridad administrativa o por el propio prestador de servicios.

Resulta necesario que se realice un debate serio en cuanto que se establezcan bases de datos personales sistematizadas enfocadas a los prestadores de servicios de seguridad privada, respetando los derechos fundamentales de los elementos operativos, pero en donde también se puedan corroborar los antecedentes policiales o de seguridad privada de cada elemento, así como que se les tenga debidamente identificados, para dar certeza a los usuarios de los servicios de seguridad. **XS**



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

Contamos con amplia experiencia en materias:

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



Servicios profesionales jurídicos y administrativos de la más alta calidad



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



Nuestros servicios jurídicos se basan en el trabajo profesional y responsable

www.serralde.com

ALMABA:

Honestidad y Lealtad, ante todo

Sin duda, Corporativo Almaba es una de las empresas más sólidas y prestigiadas del sector en nuestro país. Dirigida desde hace 17 años por Lizett Almazán Villaseñor, la empresa ha logrado distinguirse, y posicionarse, como una de las mejores opciones en el mercado nacional.



Hace algunos días visitamos sus instalaciones y platicamos con la Lic. Almazán. Esto fue lo que nos dijo:

"A corto plazo, queremos seguir creando políticas internas que nos permitan seguir dentro de un mercado bastante competitivo, deshonesto y hasta desleal, en todos los sentidos, porque lo es. Se hacen muchos negocios debajo de la mesa. Estas políticas deben permitirnos crecer y dar a nuestros colaboradores esa calidad de vida que nos permita mantenernos en el mercado al cabo de muchos años".

"El ser una empresa de seguridad de segunda generación no es nada fácil, hacer el cambio de generación en todo no es sencillo, pero el haber librado bien esa etapa nos permitirá pasar a una tercera o una cuarta generación con un crecimiento sostenido y, además, seguir aportando al país, para mí eso es sumamente importante".

¿Qué tan difícil ha sido trabajar en un ambiente dominado por hombres?

"Mucho, mucho. Empezando porque en mi familia, mi madre era un poco misógina, estaba hecha al estilo militar, y para que se diera que yo manejara la empresa se dieron muchas circunstancias internas, familiares más que empresariales. Pero a partir de ahí ha sido una lucha constante, porque creo que las primeras en tener problemas de misoginia somos las mujeres. Yo creo que el principal reto no son los hombres, a ellos les cuesta trabajo tratar con las mujeres, quizá porque somos más concretas, enfocadas, directas. Yo creo que los hombres se la llevan un poquito más campechana. Las mujeres somos un poquito más misóginas, nos cerramos más a que otras mujeres entren al propio gremio, somos las que más nos cerramos las puertas y no permitimos que otras mujeres entren, en lugar de abrirnos las puertas y ayudarnos. No lo hacemos, solitas nos ponemos el pie. A veces las puertas las tenemos que tocar, pero a veces las tenemos que empujar, y creo que las mujeres tenemos que empujar las puertas. Es cierto que ha sido difícil, pero ha valido la pena".

¿Alguna vez ha sido rechazada por ser mujer?

"Sí, que no me reciban por ser mujer, sí, muchas veces. Muchas puertas se me han cerrado por ser mujer, sí. Porque no hay confianza por ser mujer, y casi te preguntan tú de dónde vienes, y además porque yo no vengo de la policía, netamente soy

empresaria de la iniciativa privada, no soy expolicia o exmilitar, y eso me ha costado un poco de trabajo, pero eso me ha enseñado muchísimo. Yo creo que verdaderamente me ha dado más tenacidad para entender un poco mejor este sector, y valorarlo. Me gusta mucho lo que hago, aprecio mucho lo que hago".

¿Hace más de 20 años, cuando empezó a trabajar en la empresa, pensó que llegaría a dirigirla?

"Siempre lo quise y nunca pensé que lo iba a conseguir. Sí lo quería, sí lo veía. En la casa lo veía con mi papá y desde que pude hacerlo me le pegaba, iba a recursos humanos, o me metía en contabilidad. Yo me metía y no les agradaba mucho que dijéramos y en la medida de lo posible trataban de sacarme, y eso me hizo ser más tenaz, no sé si necia o tesonera, pero eso me hizo quererlo más".

¿Se arrepiente? ¿Ha valido la pena todo el esfuerzo?

"No, no me arrepiento de nada. Ha valido la pena. Yo creo que podemos trascender y trascendemos por nuestros actos, y más cuando lo que hacemos lo hacemos con convicción y con amor, y cuando hacemos las cosas así las hacemos mejor. Yo creo que Almaba ha sido un semillero de gente buena, de Almaba ha salido gente muy buena y se ha colocado en otras empresas. Creo que eso es bueno, creo que la empresa tiene mucho más para dar, y muchos años más para dar".

¿Qué sucede cuando encuentra que para conseguir un cliente tiene que recurrir a la corrupción?

"Normalmente no proporciono los servicios. Cuando ha sucedido, y sí ha sucedido, nosotros terminamos no dando el servicio. Eso ha mermado un poco nuestro crecimiento. Nosotros no hemos crecido al paso agigantado de muchos otros porque nosotros no tendemos a bajar precios ni a dar dinero por tener los servicios. Nosotros no crecemos a un ritmo tan acelerado porque preferimos no entrar en eso. Sí, hay quienes piden dinero, pero no todos, porque también hay gente honesta que quiere tener buenos servicios, pero muchos otros no. Esto se da en todos los sectores, no nada más en la seguridad. La corrupción es algo que está matando al país, ha evitado que el país crezca de manera general, entonces nosotros evitamos ese tipo de situaciones. Hay cosas con las que simplemente no juego, no juego".



WOMEN IN SECURITY 2019

El pasado 1 y 2 de agosto, en la ciudad de Cartagena, en Colombia, se llevó a cabo la segunda edición del Women in Security WIS, un movimiento auspiciado por ASIS Internacional. La primera edición se realizó en Perú el año pasado.

En el evento se dieron cita casi 200 personas, el 80% de las cuales eran mujeres, reunidas para hablar del papel y de los logros de las mujeres profesionales y activistas de la seguridad en Latinoamérica, pero no fue un congreso de mujeres, o para mujeres, fue un congreso de mujeres para la seguridad.



El enfoque de todo el congreso fue armado por un grupo selecto de mujeres representantes de Ecuador, Chile, Argentina, Perú, Colombia y, desde luego, de México. Este comité de mujeres en la seguridad le está dando un giro al congreso, los temas fueron variados, se hicieron varias mesas redondas, una de ellas dedicada a ver la importancia de la mujer en la seguridad, y otra, que fue muy emotiva, fue un panel de esposas en las fuerzas armadas y militares.

En una mesa redonda estuvieron la vicepresidenta de Colombia, Marta Lucía Ramírez, y la representante de las Naciones Unidas, que hablaron de cuál es la transformación que el mundo de la seguridad está teniendo en relación a las mujeres, y se habló de cómo proteger a la mujer de los riesgos y cómo las mujeres desde distintos enfoques están protegiendo al mundo, no compitiendo, pero sí confluyendo, convergiendo.

La Vicepresidente invitó a las mujeres del mundo y del país, a perseverar, a creer en sí mismas, a emprender, a lograr sus objetivos: *“Las mujeres colombianas constituimos el 52% de esta sociedad y durante muchos años hemos tenido, desafortunadamente, un lugar secundario. Yo veo este cargo como una gran responsabilidad de transformar, de verdad, las condiciones de todas las mujeres”.*

Se hizo el compromiso para que el próximo año el Women in Security Latinoamérica se realice en México, donde se espera que la agenda convierta a este congreso en un emblema, no de las mujeres y que hablen entre ellas, sino de las mujeres que deciden en la seguridad y que cada día demuestran más su valor, su capacidad y sus alcances en un mundo donde la mujer tiene, sin lugar a dudas, un papel fundamental. **RS**



III FORO LATAM Seguridad Patrimonial

Los días 18 y 19 del mes de julio se realizó, en el hotel Fiesta Americana de la Ciudad de México, la tercera edición del Foro LATAM Seguridad Patrimonial, organizado por CEO Global Network, una compañía dedicada a la coordinación y desarrollo de conferencias y encuentros multisectoriales, dirigidos a tomadores de decisiones de las más importantes corporaciones de Latinoamérica.

El concepto fundamental del foro es que la capacidad de una empresa para proteger sus bienes es un factor clave para determinar la fiabilidad que tiene para prestar sus servicios, y el departamento de Seguridad Patrimonial es uno de los pilares fundamentales que la sustentan. Sin embargo, los riesgos y amenazas evolucionan rápidamente en un entorno en el que los avances tecnológicos y los cambios en el mercado abren nuevas oportunidades y canales para la exposición a estos, por lo que IT y Seguridad de la Información son un actor que cobra cada vez más fuerza y protagonismo.

Cada compañía es vulnerable a esta serie de amenazas de una manera particular y diferente a cada momento. Por ello, para llevar a cabo un análisis de riesgos dinámico e integral que identifique posibles exposiciones, amenazas, y la forma en que afectan en diferentes contextos, permite a las organizaciones una mayor adaptación y nivel de protección ante este entorno cambiante. El trabajo en conjunto entre los responsables de Seguridad de la Información, IT y Seguridad Patrimonial es

la forma correcta de blindar a las empresas y mantener sus funciones de manera eficaz y eficiente.

El objetivo del foro era garantizar Networking y Benchmarking auténticos y la búsqueda de intercambio de estrategias, en el que los ejecutivos de seguridad de diferentes empresas, reconocidas a nivel mundial, pudieran profesionalizarse un poco más, intercambiando experiencias y conocimiento.

Durante el primer día de conferencias se presentaron: Adrián Álvarez, director corporate Security, Risk & Loss Prevention en Kimberly-Clark, Ana Elisa Santos, Security manager México Ca & C en BASF, Henry Granados, gerente de Servicios Gamma Ingenieros, Gerardo Corchado, director global Security Americas Group de Novartis, Javier Martínez, director de EPI Training AND Consulting, S.C. y Kael Malo-Juvera, Regional Security manager de IBM, quien hizo un análisis sobre la visión del usuario final respecto a las necesidades que deben cumplir, en materia de seguridad las empresas, buscando no sólo el interés comercial, sino la efectividad.

En la segunda jornada de conferencias estuvieron: Lucio Arcila, regional Security Advisor México, Centroamérica y Venezuela de Microsoft, Dani García, Corporate Security director de Brown-Forman, Mario Franco, regional Security manager en Schneider Electric y Jesús Consuelos, especialista en seguridad de la información y socio fundador en GLID3R Ciberseguridad. Además hubo una mesa de diálogo integrada por Jesús Consuelos, Lorenzo Ramírez, gerente corporativo de Seguridad Patrimonial, y Mario Franco. **15**



CORPORATIVO



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



NUESTROS SERVICIOS

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

SEGURIDAD ELECTRÓNICA

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

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

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

**Empresa conformada
por profesionales con
amplia experiencia**

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

www.zncorporativo.com

ATENCIÓN A CLIENTES ¿Tema olvidado?



El pasado 18 de julio se realizó el interesante Webinar organizado y dirigido a miembros de la AMEXSI. En esta ocasión, este interesante ejercicio de comunicación estuvo a cargo de Eduardo Barrón Rivera, CPP, DSI.

El tema fue la atención a clientes: “Todo tiene raíz en la atención que damos al cliente, la correspondencia que tengamos con él, la empatía con sus necesidades. Muchas veces el cliente nos plantea algún problema que ellos tienen, alguna necesidad que les surge, y nosotros no somos empáticos y decimos “este cuate está loco” o “es una jalada lo que nos está pidiendo” pero no nos ponemos en sus zapatos para poder pensar que tal vez es algo que a él le están pidiendo y que para su empresa es importante y nosotros no somos empáticos y lo vemos con desdén”.

Por eso son muy importantes los tiempos de atención: “El tiempo que nosotros le damos de respuesta a nuestros clientes es vital. Luego nos mandan un mensaje y lo vemos tres o cuatro horas después, o nos están llamando y no tomamos la llamada, o si es miércoles, les decimos que nos vemos el lunes, sin ponernos a pensar que si él está llamando con urgencia, no podemos darle hasta 5 días para tener la respuesta que andan buscando. Eso es, desde la perspectiva del cliente, algo grosero”.

“Hay diferentes conceptos de la seguridad, pero el que a mí me gusta usar es aquel que dice que la seguridad es un sentimiento, y por tanto, es pensar en qué parámetros está la relación con la empresa que me está brindando seguridad. A lo mejor nosotros mandamos guardias o patrullas, o todos los recursos técnicos, y sin embargo el cliente nos dice “Oye, tu servicio no está funcionando” porque él no siente la atención, o la seguridad en el servicio que le estamos prestando. Entonces todos los esfuerzos que hagamos están fracasando”.

“Una vez vendido el servicio, ¿quién se encarga de dar seguimiento? ¿Qué debemos hacer para ser siempre la primera opción de nuestros clientes? Generalmente es el coordinador operativo el que da seguimiento a nuestros clientes, pero cuántos de ellos están realmente capacitados para hacerlo, cuántos de nuestros jefes operativos, supervisores, jefes de servicio, los vemos con desdén y no nos sentamos nunca en una mesa para intentar darles una visión ejecutiva de lo que es el servicio al cliente y ellos no lo entienden”.

“Como usuario, de repente es frustrante que cuando tienes alguna necesidad y tu empresa prestadora de servicio no es empática y lejos de darte una solución te da un cuestionamiento, o un reclamo, o de plano te dice “lo que tú me estás pidiendo es absurdo”. Y no, lo que nosotros debemos hacer no es cuestionar, sino ofrecer alternativas. Dicen por ahí que una buena atención al cliente puede hacer más competitiva a tu empresa que un excelente precio o la calidad en el producto”.

“Regularmente metemos al aula a nuestro personal para darles temas como manejo de armas, o un intento como de liderazgo, manejo de crisis, pero nunca los sentaste a darle una competencia para que pudiera hablar con su cliente, para que pudiera darle respuestas sensatas a su cliente, para que pudiera escuchar a su cliente y una vez que tenga las cosas en orden, llevarlo de la mano y proponerle innovación, cambio de estrategias y hacerle ver que le aporta valor a la relación, que no le vende nada más el servicio sino que le aporta valor y que le da una competencia a nivel interno de su área, que hace brillar el área de seguridad en su empresa, y ser ya no su proveedor, sino cambiar la estrategia, cambiar la visión de ser un proveedor a ser un socio estratégico del negocio”.



Multiproseg es una de las empresas más sólidas y acreditadas del sector de la seguridad privada en nuestro país, ofrecen sus servicios de seguridad intramuros en las 32 entidades de la república mexicana. Para conocer un poco mejor a Multiproseg, entrevistamos en sus oficinas al Lic. Miguel Ángel Champo del Valle, socio director de la empresa.

“La seguridad privada nunca va a sustituir a la seguridad pública por el tema de los delitos del fuero común, como asaltos y robos que sí se previenen bajo un esquema de seguridad privada, sin embargo, no los atacamos, eso es responsabilidad exclusiva del gobierno, local y federal. Nosotros somos socios comerciales de nuestros clientes, y damos continuidad de negocio a las empresas, prevenimos pérdidas y brindamos manejo de crisis”.

“La función de la seguridad privada, insisto, no va relacionada con el crecimiento de la inseguridad. La parte de la seguridad privada que sí va de la mano con el crecimiento de la inseguridad es la parte que manejan las escoltas, pero es un rubro enfocado a clientes específicos y bien definidos”.

“El tema de no tener una cámara que nos represente como sector, y de no tener una regulación adecuada, implica que no haya mucha certeza para el empleado y también, vamos a ser honestos, no cobramos lo justo, si Yo cobrara lo justo podría pagarle al guardia un mejor salario. Lo que más nos perjudica son los impuestos, entre más gana un guardia, más impuestos pagamos además del seguro social. Realmente es muy marginal la utilidad que tenemos”.

Respecto a la competencia fue directo, como suele ser, y nos dijo: “Esta empresa la dirigimos entre mi esposa, en la parte administrativa, y yo, que me dedico básicamente a las relaciones públicas, creo que eso les da certeza a nuestros



clientes de que somos una empresa honesta y confiable, y creo que estar en todo momento en contacto con los usuarios de nuestros servicios les da confianza y tranquilidad. La diferencia es el trato personal que ofrecemos”.

“Soy honesto, soy un empresario leal con el sector, con los clientes, y creo que mientras mantenga estos principios, no tengo rival. Tenemos competidores, no enemigos, así que competencia hay mucha, pero eso nos hace buscar ser los mejores”.

¿Ha sentido algún cambio en su relación con los clientes del sector gubernamental en la actual administración?: “Sí, y por mi parte hay mucha preocupación porque ya empieza a sentirse la falta de flujo de recursos, en el sector privado todavía no, pero sí lo están previendo, pero en el sector gobierno, en mis clientes, sí ya se está sintiendo. Antes te pagaban a tiempo, para una empresa de servicios, como nosotros, que te paguen a tiempo es lo más importante, porque obviamente nosotros pagamos a tiempo a nuestros empleados. Mi preocupación sí es muy grande porque hay mucha incertidumbre con la consolidación, que va a implicar que unos 15 mil guardias se soliciten a unas pocas empresas, y todas las demás que prestaban el servicio, que son cientos o quizá miles, se vean afectadas. En ese sentido, el sector privado es más estable”

Para finalizar, le pedimos que nos diera su opinión sobre la competencia desleal que enfrentan las empresas del ramo, y esto fue lo que nos dijo: “En la ley no existen dientes para poder sancionar a las empresas piratas, como siempre, los cautivos somos los que estamos a la orden de que nos hagan visitas de inspección extraordinarias, y si te encuentran una irregularidad te pueden amonestar, suspender o hasta multar”.

“Te soy honesto, el mercado de las empresas piratas no me preocupa, me preocupa más que la autoridad realice un buen trabajo. El nicho que ocupan las empresas piratas es muy cerrado, básicamente le trabajan a unidades habitacionales y servicios por el estilo, es un mercado muy reducido. Son más un riesgo para quienes los contratan que para el sector”.

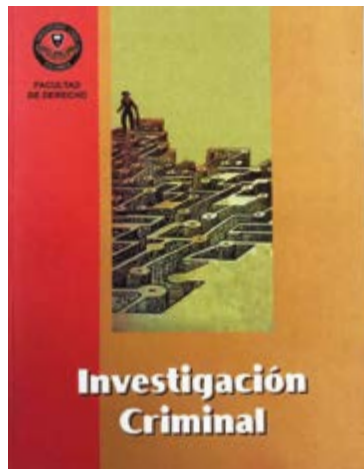


LA BIBLIOTECA DEL SENSEI

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

En esta ocasión quiero recomendarles dos textos relacionados con la investigación corporativa, la criminología y la criminalística.

El primero de ellos es un libro de la Universidad Libre de Colombia, de la Facultad de Derecho, que habla de lo que es la investigación criminal, y parte del hecho de establecer unos aspectos jurídicos fundamentales acerca de la metodología de la investigación criminal.



"LA INVESTIGACIÓN CRIMINAL"

Facultad de Derecho, Ed. Universidad Libre de Colombia

Es muy importante que cuando hablamos de la investigación a nivel público, o a nivel privado, tengamos bases metodológicas para su manejo y en la distinción entre la investigación pública y la privada está la situación jurídica, que es la clave de todo.

Mientras que en la seguridad pública se hace investigación en toda la extensión de la palabra, en el ámbito privado hacemos lo que se llama análisis de responsabilidades o investigación corporativa.

En este libro los autores, que son básicamente un consejo universitario coordinado por Pablo Elías González Monti, hacen una excelente esquematización para poder establecer lo que es el análisis operativo de la criminalidad y también varios ejercicios, incluyendo lo que es el análisis criminal, las técnicas de la entrevista y también lo que son las técnicas de entrenamiento.

Este es un documento con muy buenos esquemas, muy fáciles de interpretar y de entender, que permiten que cualquier persona pueda desarrollar o perfeccionar sus habilidades de investigación. Este es un libro súper importante para quienes trabajamos la seguridad corporativa.

"MANUAL DE CRIMINALÍSTICA"

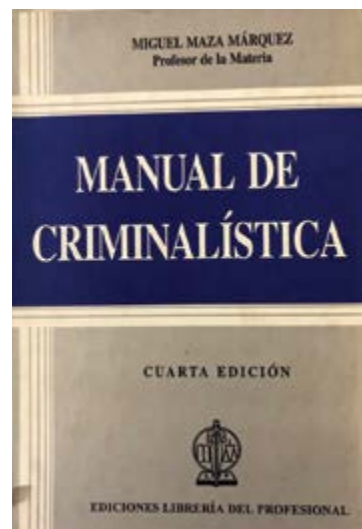
Por Miguel Maza Márquez, Ed. Librería del Profesional, 2003

El segundo texto de esta ocasión, en el orden de la investigación corporativa y criminal, es un texto más avanzado, de Miguel Maza Márquez, que se llama Manual de Criminalística. Este también es un texto internacional, también de origen colombiano, que nos habla en varios capítulos de las esencias de la criminalística, hablando de la investigación criminal como una herramienta para garantizar la objetividad y la metodología científica de la investigación.

Explora aspectos muy específicos como la balística, la dactiloscopia, la química y manejo de explosivos, algunos aspectos de la documentología, el manejo de la grafoscopia, grafología y análisis de textos, incluso aspectos técnicos como los sellos, el papel, las tintas y hasta el papel moneda. El libro explora también el campo del fraude electrónico como uno de los desafíos de la seguridad.

También nos habla de las escenas del delito, de cómo se procesan, habla de la informática criminalística y lo que puede ser el crimen del futuro, que en el 2000 se veía venir, y que hoy es uno de los elementos más desafiantes para la seguridad de las empresas.

Estos dos libros no pueden faltar en la biblioteca de consulta constante y frecuente de un buen gerente de seguridad. Recuerden, muchas veces nosotros, como gerentes de seguridad, no hacemos el trabajo, pero sí lo supervisamos y nadie puede dar lo que no tiene. Si no conocemos las bases técnicas y jurídicas de la investigación, nuestras acciones de seguridad quedarán incompletas. Hasta la próxima. JS



VIDEOVIGILANCIAMX



REVISTA DIGITAL

ESPECIALIZADA EN VIDEOVIGILANCIA

www.videovigilanciamx.mx



VIDEOVIGILANCIA

con lente monitorizada y seguimiento automático

El proveedor de soluciones de redes, comunicaciones y videovigilancia D-Link ha anunciado la disposición de su nueva cámara de videovigilancia WiFi mydlink DCS-8515LH. Su reducido tamaño le permite instalarla en cualquier lugar del hogar.

Cámara DCS-8515LH de D-Link.

Esta nueva cámara de seguridad incorpora una lente monitorizada capaz de seguir el movimiento de objetos, personas y animales.

La cámara mydlink DCS-8515LH incorpora una lente monitorizada con un ángulo de visión de 105 grados en vertical y 340 grados en horizontal. Ofrece una resolución de HD de 720p y realiza un seguimiento automático de personas, animales y objetos para aumentar la seguridad, incluso por la noche, gracias a su visión nocturna.

En cuanto a sus conexiones, D-Link ha equipado a su dispositivo con la tecnología Wi-Fi para eliminar las conexiones por cable y facilitar tanto su instalación como la transferencia de datos. Permite una comunicación bidireccional gracias a su altavoz y micrófono integrado, al tiempo que es compatible con los asistentes virtuales como Amazon, Alexa y Google Assistant.

Gestión remota 24/7

Los usuarios tienen a su disposición la aplicación mydlink para los teléfonos móviles o tablets con los sistemas operativos Android e iOS. A través de

la aplicación, recibirán notificaciones emergentes causadas por una detección por movimiento y/o sonido, acompañada de una imagen del momento.

Asimismo, se puede visionar en directo el interior del hogar y realizar zoom mediante un gesto táctil de la pantalla del terminal móvil. En el momento que se ejecuta una alarma, el sistema comienza la grabación almacenándola en la nube, con una

capacidad ilimitada y gratuita durante las 24 horas recurrentes.

Los parámetros de sensibilidad son ajustables en función de las necesidades de cada vivienda. Como característica extra, la cámara de seguridad mydlink DCS-8515LH incluye un botón de llamada de emergencia, cuyo número es configurable. **XS**





Control de acceso Abierto, flexible y seguro.

Nuestras soluciones de control de acceso son abiertas y se ajustan a sus necesidades. Le dan la libertad de mezclar y combinar el mejor hardware y software e integrarlos perfectamente con otros sistemas, incluyendo su sistema de videovigilancia. Puede usarlos para todo, desde identificación básica y control de entradas, hasta gestión avanzada de acceso. Nuestro portafolio de control de acceso incluye: controladores de puerta de red, estaciones de puerta de red, relés de E/S de red, lectoras de tarjetas y más, todos aportan los beneficios de IP abierta.

www.axis.com/products/access-control

AXIS[®]
COMMUNICATIONS



Partes de una **CÁMARA DE VIDEOVIGILANCIA** antivandálica exterior

Las Cámaras de Videovigilancia Full HD antivandálicas para exterior desarrolladas con piezas o componentes independientes, son la mejor opción en los entornos profesionales y están indicadas para Comunidades de Vecinos, garajes, aparcamientos, patios, polideportivos, hoteles, gasolineras, supermercados...

Estas cámaras de vigilancia antivandálicas son muy versátiles y las posibilidades de configuración que ofrecen son infinitas, ya que permiten intercambiar ópticas con diferentes alcances y profundidad, incluir LEDs infrarrojos para visión nocturna, incorporar cámaras IP o analógicas, con mayor o menor resolución etc. Sus prestaciones y características se pueden adaptar a la medida de las necesidades de la instalación de videovigilancia.

Gracias a su gran tamaño y robustez, las cámaras de vigilancia antivandálicas con piezas intercambiables generan un gran efecto disuasorio y su grado de protección es óptimo. Soportan los golpes evitando que puedan descolocarse o desplazarse y gracias a su carcasa antivandálica exterior, la electrónica de la cámara queda perfectamente protegida.

La postventa y el mantenimiento de una cámara de videovigilancia antivandálica Full HD son mucho más baratos que el de las cámaras de vigilancia compactas ya que en caso de avería, se puede sustituir el componente averiado

de la cámara de videovigilancia antivandálica, conservando el resto de las piezas, al contrario que las cámaras de videovigilancia compactas, que cuando sufren una avería deben ser sustituidas por cámaras de seguridad nuevas con el sobrecosto que esto supone. Además, si con el paso del tiempo la instalación requiere de unas necesidades especiales como una mayor profundidad o un mayor alcance, podría sustituirse la óptica sin necesidad de adquirir una cámara de videovigilancia nueva. Si optamos por cambiar de tecnología y queremos sustituir las cámaras analógicas por cámaras de videovigilancia IP, bastará con cambiar la cámara "box" o cámara interior, aprovechando el resto de componentes, de la misma manera que si necesitamos cámaras de mayor resolución, bastaría con cambiar la cámara box manteniendo el resto de componentes. En definitiva, a medio y largo plazo, las cámaras de vigilancia antivandálicas suponen un gran ahorro de costes en mantenimiento y averías.

Al poder ajustar e intercambiar las ópticas de la cámara de vigilancia antivandálica, se consigue una precisión de imagen óptima en función de la distancia que se pretende captar por la lente, optimizando así la calidad de las imágenes. Al ser cámaras antivandálicas, además de funcionar sin fallo ante cualquier inclemencia meteorológica (agua, nieve, granizo, frío/calor extremos...), están protegidas frente a cualquier tipo de sabotaje, siendo prácticamente imposible romper o inutilizar.

1. VISERA: sirve para que la luz no deseada no intervenga en la imagen que capta la cámara de vigilancia antivandálica, de esta manera se evita el contraluz y se reducen los puntos muertos por reflejo.

2. IRIS: forma parte de la óptica y controla la luz que entra al sensor. El iris puede ser manual o automático. Si es automático (auto iris) se adapta a la luz del escenario de la misma manera que lo hace el ojo humano, evitando las imágenes blancas o completamente oscuras. Además, las nuevas cámaras box cuentan con sistema de compensación de contraluz BLC y WDR (White Dynamic Range) que ilumina las zonas oscuras de la escena.

3. ÓPTICA: existen diferentes tipos de óptica que se pueden adaptar a las cámaras de vigilancia BOX según las características del sensor, apertura del iris, sensibilidad, objetivos (fijos, varifocales, zoom motorizado...), distancia focal... Al poder configurar la cámara de seguridad con diferentes ópticas, se puede optimizar el campo de visión de la cámara de vigilancia.

4. CÁMARA BOX: este tipo de cámaras de videovigilancia permiten cambiar el tipo de lente según el ángulo de visión y zoom que se necesite. También se puede cambiar la cámara box por otras de mayor calidad o tecnologías diferentes (cámara de

vigilancia IP por ejemplo), conservando el resto de componentes.

5. BALUN: transforma las líneas de transmisión de balanceadas a o no balanceadas.

6. PROTECCIÓN ANTIVANDÁLICA: protege a la cámara de vigilancia de cualquier inclemencia meteorológica como la nieve, lluvia, granizo... y de los golpes, se mantiene fija captando imágenes de todo lo que sucede. Está indicada para su funcionamiento en el exterior.

7. VENTILADOR: permite la protección térmica de la cámara de videovigilancia, impidiendo que se calienten sus componentes. Su función es la misma que el ventilador de un PC.

8. FUENTE DE ALIMENTACIÓN: estabiliza la tensión con seguridad protegiendo a los componentes de la cámara de seguridad antivandálica en caso de sobre alimentación.

9. RÓTULA: permite darle el ángulo necesario a la cámara de videovigilancia antivandálica para que capte de forma precisa el espacio a proteger.

10. TUBO DE ACEROFLEX: aísla y protege los cables del agua y la humedad e impide que puedan ser cortados o saboteados. Es hermético y muy resistente.

11. SOPORTE: permite fijar la cámara de videovigilancia antivandálica en cualquier superficie, ya sea en pared, techo, poste...

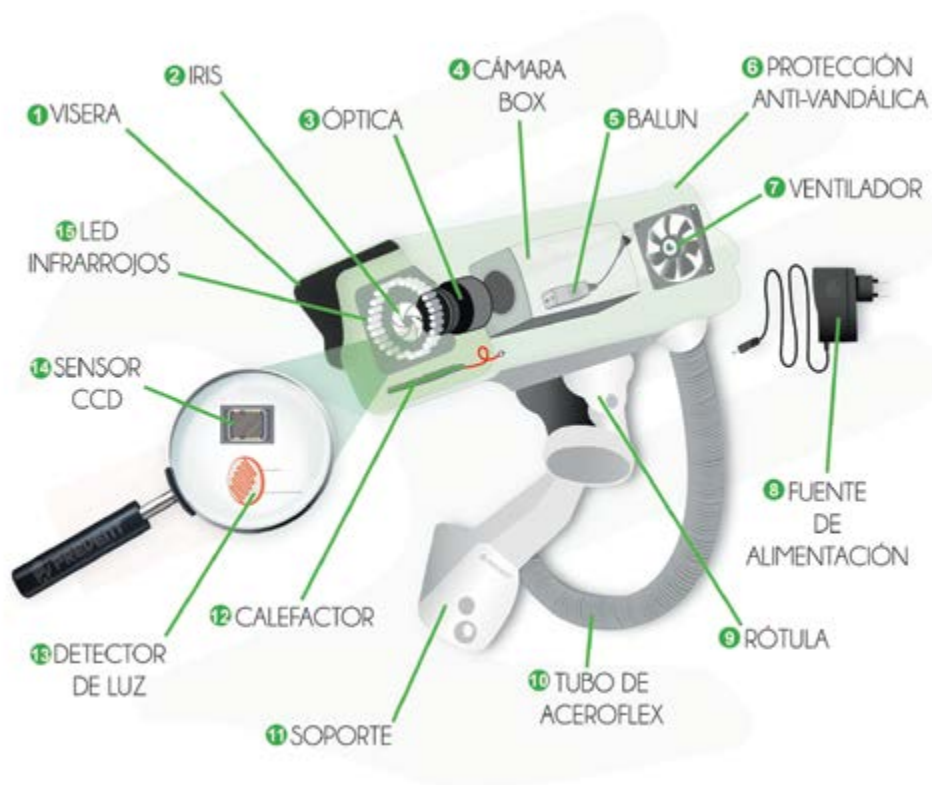
12. CALEFACTOR: impide que el cristal de la cámara de vigilancia se empañe (sistema antivaho) con los cambios de temperatura, asegurando que la imagen de la cámara de seguridad sea siempre nítida.

13. DETECTOR DE LUZ: detecta el nivel de luminosidad y activa los LED infrarrojos de la cámara de vigilancia en caso de que sea necesario.

14. SENSOR CCD: transforma las señales luminosas que recibe la lente en señales electrónicas que pueden ser transmitidas en formato digital (cámaras de seguridad IP) o analógico.

15. LEDS INFRARROJOS: se activan de forma automática cuando hay poca iluminación, permitiendo que la cámara de videovigilancia grabe en la oscuridad y en situaciones de escasa iluminación en blanco y negro (0,01 lux). Si resulta necesario, se puede añadir a la cámara de seguridad antivandálica un foco de infrarrojos externo de mayor alcance. **RS**

En la siguiente infografía explicamos detalladamente cuáles son las partes que componen una cámara videovigilancia antivandálica exterior y para qué función cumple cada uno de sus componentes dentro del conjunto.





AXIS SOLUTIONS CONFERENCE 2019



El pasado 22 de agosto se realizó la tercera edición del Axis Solutions Conference en el Foro Corona del Hipódromo de las Américas, en la Ciudad de México. Los asistentes tuvieron la oportunidad de conocer las soluciones tecnológicas más innovadoras del mercado de la videovigilancia, a través de la integración en diferentes sectores como el residencial, gobierno, industria automotriz, retail y la banca, además de la Ciudad Inteligente.

Manuel Zamudio, Industry Associations Manager, de Axis Communications para el Norte de América Latina y el Caribe, responsable y coordinador del evento, nos dijo: “Este es un evento que hacemos cada dos años y lo que buscamos es traer propuestas diferentes en colaboración con los integrantes de nuestro ecosistema, de nuestros programas de socios, socios desarrolladores de aplicaciones de software, socios fabricantes de componentes de hardware, que nos ayudan a complementar soluciones para resolver necesidades específicas”.

“También tenemos una propuesta de soluciones cien por ciento AXIS y lo que queremos es mostrar cómo podemos convivir con todo tipo de aplicaciones e integraciones, plataformas unificadas para resolver los problemas de todos los componentes de una ciudad. Sabemos que dentro de poco tiempo la gran mayoría de la población del planeta viviremos en ciudades y entonces estamos preparándonos, estamos proponiendo pequeños componentes de un todo mucho más grande que es la ciudad, y ésta primero necesita ser segura antes de ser inteligente”.

“En AXIS tenemos propuestas para seguridad pública, para atender a la ciudadanía y darle servicios, combatir el crimen, pero también estamos haciendo propuestas para hacer más eficiente la movilidad de la gente en la ciudad, para que pueda desarrollarse mejor en su actividad diaria, en temas comerciales, residenciales, y de edificios inteligentes”.



El Axis Solutions Conference 2019 estuvo dirigido al público en general y alternó presentaciones de tipo comercial y técnico, con otras de análisis político e incluso de entretenimiento.

“Queremos mostrar que estamos agregando nuevas dimensiones tecnológicas a nuestro mundo, porque ya no son sólo soluciones basadas en imágenes, en video, sino también en audio, en lecturas de temperatura, o utilizando microondas, y diversas analíticas que generan una gran cantidad de información, de datos, que se convierten en información útil para la toma de decisiones, adecuadas y oportunas”.

Al evento asistieron más de 2500 personas a lo largo del día, y en algunos momentos se contó con la presencia de 900 personas de manera simultánea. Además de los stands de las 19 empresas asociadas, durante todo el día se impartieron diferentes conferencias, entre ellas: “Panorama de México 2018-2024 ¿qué podemos esperar?”, impartida por Javier Tello, reconocido analista político, y “Convirtiendo retos en oportunidades”, de Mario Flores y “El futuro de la tecnología y cómo ésta afectará la manera de generar y ejecutar los negocios”, de Vito di Bari.^{MS}



EN UN MERCADO
COMPETITIVO
ESTAR
CERTIFICADO
HACE LA DIFERENCIA

CURSOS ALAS



Alarmas



Video Vigilancia



Control de Acceso



Redes



Operadores



Gerencia y ventas



Incendios



Integración



Perimetral

También puedes armar tu grupo
y te llevamos el curso a la medida
de tus necesidades

¡Escríbenos HOY!

+57 321 615 33 67

cursos@alas-la.org

www.alas-la.org/cursos

Cursos certificados por la



ASOCIACIÓN
LATINOAMERICANA
DE SEGURIDAD



VIDEOVIGILANCIA Y ALARMAS: prevención del delito y tecnología

El uso de tecnología en materia de seguridad ciudadana es una práctica cada vez más aceptada y utilizada en México. En el país se invierten elevadas sumas del presupuesto público en la adquisición de estos productos que se consideran “eficaces” y menos intrusivos, sin embargo, aún no se cuenta con evaluaciones que permitan conocer sus diferentes efectos, tanto positivos como negativos, y ni siquiera se conoce con certeza la prevalencia de este tipo de tecnologías.

Paralelamente, los hogares mexicanos ante la inseguridad y el temor a ser víctimas del delito recurren a diferentes medidas de protección entre las que se encuentra el uso de la tecnología. Existen diferentes motivos por los cuales las familias deciden invertir en medidas de protección para sus propios hogares. Al respecto, uno de los principales cuestionamientos es si se invierte en éstas como una medida

preventiva, o como una medida reactiva cuando alguno de los miembros del hogar ha sido víctima del delito.

En el caso de la inversión que proviene de los particulares para proteger sus propios hogares, cuando la sociedad crea conciencia sobre los problemas de inseguridad que se manifiestan en su entorno, el instinto de protección a la familia es inminente e intenta resguardar el ámbito familiar. Este “instinto de

protección” se manifiesta en los hogares mexicanos de diferentes formas.

En los hogares el miedo que las personas sienten a ser víctimas de la violencia o delincuencia es tal que se ven en la necesidad de hacer algo para protegerse individual y familiarmente. En algunos casos se trata de acciones que podrían calificarse como positivas, pero también hay algunas medidas que generan efectos negativos.

Medidas de protección en los hogares y sus efectos socio espaciales

Existen diferentes medidas de protección que se toman en los hogares, ya sea como una forma de prevención para evitar ser víctima de un delito o como una disposición reactiva para reducir la posibilidad de volver a serlo.

En la Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE, 2017) es posible conocer si se han adoptado medidas de protección en los hogares mexicanos para evitar ser víctimas del delito. Los resultados evidencian que en el 42% de los hogares se ha tomado cuando menos alguna medida de protección para evitar ser víctimas de la delincuencia. En 14 entidades federativas, más del 42% (promedio nacional) de los hogares decidieron invertir en medidas de seguridad, entre éstas destacan los casos del Estado de México, Sonora y Tabasco donde el porcentaje de hogares es superior al 50%.

Las principales medidas de protección que se tomaron en los hogares mexicanos son: cambiar o colocar cerraduras y/o candados, cambiar puertas o ventanas, colocar rejas o bardas y realizar acciones conjuntas con sus vecinos. En menor medida (menos del 6% de los hogares) decidieron invertir en comprar un perro guardián u otras opciones como instalar alarmas o cámaras de videovigilancia, contratar vigilancia privada en la calle o colonia, contratar seguros, adquirir armas de fuego y otras precauciones.

El primer efecto que se genera es de tipo económico, que de acuerdo con los distintos tipos de medidas implica un gasto. En 2017 se estimó que las medidas preventivas representaron un gasto para los hogares que asciende a 82 mil millones de pesos. Para dimensionar el monto que está inversión representa, basta señalar que para el año 2018 la federación destinó 7 mil millones de pesos a las entidades federativas a través del Fondo de Aportaciones para la Seguridad Pública, y la entidad que recibió más recursos alcanza un poco más de los 502 millones de pesos.

Además de la inversión económica en estas medidas de prevención, su ejecución tiene distintos efectos socio espaciales. Aún y cuando se instalen o implementen al interior o en los límites de los hogares, estas medidas producen efectos en las personas que habitualmente transitan en la vía pública, a los vecinos y a los usuarios de los espacios públicos.



Asimismo, se contemplan las modificaciones en las fachadas con alambres de púas o cercas electrificadas, medidas que si bien, podrían considerarse como menos violentas que el cierre de calles en “conjuntos cerrados” al generar principalmente efectos disuasivos y de protección de los hogares, también transforma significativamente el entorno urbano. Visualmente este tipo de protecciones envían un mensaje al transeúnte de que ese hogar está protegido y que, muy probablemente, la zona fue o continúa siendo víctima de la inseguridad.

En suma, la instalación de rejas o bardas ya sea en los límites de los hogares o para conformar “conjuntos cerrados” son medidas que generan modificaciones en la trama urbana que a su vez conciben mecanismos de exclusión o discriminación hacia los otros.

La instalación de cámaras de videovigilancia y alarmas en los hogares para protegerse de la inseguridad se considera como parte de la política pública de prevención del delito cuyo objetivo principal es reducir las oportunidades e incentivos para los transgresores.

La instalación de estos dispositivos en México no ha sido fortuita y responde en gran parte a una demanda ciudadana que ante el temor de ser víctimas del delito o por la percepción de inseguridad solicitan la colocación de estas cámaras y alarmas a las instancias gubernamentales y por cuenta propia también lo realizan en sus hogares.

El auge de las alarmas

Una alarma es un mecanismo que es activado ante la presencia de riesgo o peligro para alertar a los vecinos, usuarios o incluso a la autoridad de una determinada zona. Existen diferentes tipos de alarmas, en la Ciudad de México, por ejemplo, se han instalado los “botones de auxilio” que se definen como “un intercomunicador de contacto directo con los C2, se ubican en los postes de diversas cámaras de videovigilancia y deben ser presionados por las y los ciudadanos que requieran el apoyo inmediato de algún servicio de emergencia. Quien presiona el botón es atendido y su reporte es canalizado de manera inmediata a los cuerpos de emergencia. En este caso las cámaras de videovigilancia y las alarmas están físicamente en el mismo espacio y a su vez conectadas a los Centros de Comando y Control.

También existen las alarmas vecinales financiadas con recursos públicos que se han instalado en los hogares con



Sistema de seguridad
autónomo para el
transporte de carga

Tu carga protegida

blu!

 tiLatina

info@tilatina.com

Tel: +52 55 6588 0400



la autorización de los residentes y pueden ser activadas desde el interior de la vivienda para alertar situaciones de riesgo o peligro. En el caso de las cámaras de videovigilancia, numerosos equipos se han instalado con recursos públicos, pero solicitadas directamente por la ciudadanía a través del programa de presupuesto participativo que se ejerce en la Ciudad de México.

También existen cámaras y alarmas financiadas e instaladas directamente por los particulares. En algunos casos, la operación de éstas depende de un tercero, a quien se le paga por un servicio que incluye el monitoreo y eventual atención de las emergencias o peligros detectados a través de las imágenes de las cámaras o la activación de las alarmas.

Detrás del auge de la instalación de las cámaras de videovigilancia, tanto públicas como privadas, hay un profundo razonamiento teórico que explica la potencialidad de la videovigilancia como política pública para la reducción y prevención de la criminalidad, que proviene fundamentalmente del urbanismo.

videocámaras de vigilancia registra porcentajes más elevados. Está por encima de medidas como “contratar vigilancia privada en la calle o colonia” o “contratar seguros” que implica un gasto permanente y sistemático para los hogares que en el tiempo puede ser mucho más alto que la inversión en una videocámara o alarma. De igual forma se observa que está por arriba de los hogares que decidieron “adquirir armas de fuego”, si bien el porcentaje de esta medida es de apenas 0.7% es preocupante, sobre todo por la gran cantidad de homicidios dolosos que se registran con arma de fuego.

En el caso particular de la Ciudad de México, que es la entidad en la que mayor porcentaje de hogares refiere haber invertido en cámaras de videovigilancia y alarmas, es importante enfatizar que esta demarcación fue la pionera en México en implementar con recursos públicos un programa de despliegue tecnológico en materia de prevención del delito. Concretamente en 2009 se inició el Proyecto Bicentenario Ciudad Segura cuyo objetivo se definió como “proveer sensores, comando, control y responder con las capacidades necesarias para intervenir masivamente en contra del crimen,



La instalación de cámaras de videovigilancia y alarmas, aunque se coloquen al interior de los hogares, en la mayoría de los casos están dirigidas hacia la vía pública, vulnerando el derecho a la privacidad de los vecinos y transeúntes. Al respecto, es importante señalar que en México se ha hecho muy poco para regular la instalación de cámaras por parte de privados, lo que implica que los datos que son captados pueden ser usados por particulares para los fines que a ellos convengan y no existe una protección de las imágenes de las personas que son grabadas.

La inversión en cámaras de videovigilancia y alarmas no está entre las primeras opciones de protección para los hogares mexicanos. Entre las diferentes medidas de prevención que se indagaron en la ENVIPE 2017, destaca que en primer y segundo lugar se encuentran las medidas relacionadas con “cambiar, colocar o reforzar cerraduras y/o candados” y “cambiar o reforzar puertas o ventanas” que respectivamente representan 27.5% y 22.5% de los hogares. La instalación de alarmas y/o videocámaras de vigilancia se ubica en el sexto lugar con 3.5% después de otras medidas como “colocar o reforzar rejas o bardas”, “realizar acciones conjuntas con sus vecinos” o “comprar un perro guardián”.

Sin embargo, en comparación con otras opciones de prevención en los hogares, la instalación de alarmas y/o

así como mejorar la habilidad del gobierno de la Ciudad de México para responder eficiente y eficazmente a las crisis”.

Como parte del proyecto se consideró inicialmente la instalación de más de 8 mil STV's, o sistemas tecnológicos de videovigilancia, conectados a una red primaria o anillo de fibra óptica implementada dentro del proyecto, usando los adelantos existentes en el mercado de las nuevas tecnologías de las comunicaciones y telecomunicaciones.

Actualmente, como parte de este proyecto, se han instalado en la vía pública de la Ciudad de México más de 15 mil cámaras de vigilancia, así como 6 mil instaladas en el Sistema de Transporte Colectivo Metro, con la finalidad de prevenir y alertar inmediatamente a las autoridades de seguridad y de emergencias capitalinas sobre cualquier situación de riesgo. Asimismo, con recursos del Presupuesto Participativo, más de 300 colonias de la ciudad decidieron implementar proyectos relacionados con la instalación o mantenimiento de cámaras de videovigilancia.

No obstante, de la implementación de medidas de prevención con el uso de tecnología que son financiadas con recursos públicos, la Ciudad de México ocupa el primer lugar a nivel nacional de hogares que decidieron invertir en cámaras de videovigilancia y alarmas. En suma, uno de cada diez hogares de la ciudad coincidió en esta decisión.

Por otra parte, la teoría de la victimización refiere que haber sido víctima del delito, o que una persona conocida haya sido víctima, incide en la sensación de inseguridad. Asimismo, se ha referido que una de las razones por las que en los hogares se invierte en medidas de protección es porque han sido víctimas del delito y lo que se pretende es reducir la probabilidad de volver a serlo, es decir es una reacción ante la victimización.

De acuerdo con los resultados de la ENVIPE 2017, en promedio el 28.8% de las personas en México fueron víctimas de al menos un delito, lo que equivale a aproximadamente a 24 millones de casos, en algunas entidades el porcentaje es mucho mayor, destacando el Estado de México con 47.6% de víctimas. Del total de las personas que fueron víctimas a nivel nacional, el 33.9% ocurrió en la casa.

Videovigilancia en América Latina

Para muchos, la presencia de las videocámaras pareciera garantizar las condiciones adecuadas para la inversión, el comercio y el consumo. Su instalación respalda y cristaliza la idea que se tiene de una ciudad segura. En años recientes, los proyectos inmobiliarios han comenzado a incluir cámaras de vigilancia como parte del diseño de conjuntos arquitectónicos, a tal grado que casi cualquier proyecto de inversión urbana demanda la presencia de una red de videocámaras de vigilancia.

Actualmente, América Latina se ha convertido en uno de los nichos de crecimiento más importantes de la industria de estos dispositivos electrónicos a escala global. Según el reporte del IMS Research (2014), el mercado de la videovigilancia en América Latina mantuvo una tasa de crecimiento del 40.5% desde el 2008 hasta el 2013. Se espera que para el 2019 la venta de dispositivos de videovigilancia supere los 200 millones de dólares.

El crecimiento del mercado de la videovigilancia en América Latina se encuentra por encima de otras regiones del mundo, en parte apuntalado por Brasil como sede, en sólo diez años, de dos eventos deportivos globales. Más allá del caso brasileño, Argentina Colombia y México, encabezan los mercados con mayor crecimiento.

En el caso de México, la industria de cámaras de vigilancia incrementó sus ventas, entre 2011 y 2012, en un 60% y mantuvo un crecimiento moderado hasta 2014, cuando se detuvo sensiblemente por la introducción de las cámaras de vigilancia digital. Sin embargo, el mercado volvió a repuntar en el 2015, una vez que las entidades públicas y privadas ajustaron sus presupuestos para adquirir la nueva tecnología digital de videocámaras.



Hay que señalar, sin embargo, que el incremento de la videovigilancia en México -y en general en América Latina- no se ha hecho acompañar, como en otros lugares, de una evaluación sobre su efectividad para hacer frente a la inseguridad, lo que contrasta con el cúmulo de investigaciones al respecto en otros países, donde se han logrado establecer, por ejemplo, los límites y alcances de las cámaras de vigilancia en la prevención, reducción y reconstrucción de hechos criminales.

Además, estos estudios han mostrado que las cámaras de vigilancia tienen efectos en otros ámbitos de la vida social y no solamente en aspectos relacionados con la seguridad pública. Por un lado, tienden a desdibujar las fronteras que dividen la esfera de lo público y lo privado, colocando en no pocas ocasiones los datos personales que administran en un espacio de indeterminación jurídica.

Por otro lado, la videovigilancia genera procesos de clasificación social y espacial que derivan en formas de exclusión de grupos y sectores de población. Al separar espacios y zonas privilegiadas de aquellas que representan un riesgo, las cámaras de vigilancia resultan dispositivos que reproducen la desigualdad social y la segregación del espacio urbano.

Si bien es cierto existen regulaciones que dan soporte a la ciudadanía frente al uso de la videovigilancia, aquellas son pobres o débiles en el caso mexicano, lo cual mina en ciertos aspectos la capacidad de las personas y grupos para hacerse de espacios de autonomía y control frente a procesos de clasificación y discriminación social. Incluso ahí donde existen regulaciones a la videovigilancia se puede observar que dichas regulaciones centran su atención en los temas relativos a la privacidad y la protección de datos personales, pero dejan de lado los efectos sociales de la vigilancia.

Indefinición legal

La inseguridad y la necesidad de autoprotección en México, son el principal motor que mueve a la ciudadanía a adquirir soluciones de seguridad electrónica, por lo que los equipos de videovigilancia IP, seguido de alarmas y controles de acceso encabezan la lista de compras. La iniciativa privada, y sectores como el industrial, retail, banca, energía, transporte y hospitales ocupan el 45% de las ventas, residencial 15% y gobierno 40%.

En México la seguridad residencial, comercial y corporativa también ha ganado terreno en los últimos años. Los sistemas de protección contemplan la instalación en puntos estratégicos de dispositivos electrónicos como son sensores de movimiento, contactos magnéticos para puertas y ventanas, así como botones de pánico.

El Censo Nacional de Gobierno, Seguridad Pública y Sistema Penitenciario de 2015, reportó que veintinueve entidades federativas y la Ciudad de México tenían bajo su control 25,631 cámaras de vigilancia para el ejercicio de la función de seguridad pública, más del doble de las que reportó ese mismo censo en 2012. El 41% de las cámaras instaladas en el país se encuentran en la Ciudad de México, seguida por el Estado de México, Guanajuato y Michoacán.

Las cámaras de vigilancia no sólo funcionan como mecanismos para resolver y prevenir hechos criminales, son también dispositivos de gobierno que expresan reglas que buscan garantizar y gestionar el orden y la convivencia en las ciudades.

No obstante, la videovigilancia ha recibido críticas de diferente tipo. Por un lado, se le ha cuestionado su capacidad para resolver problemas de seguridad, y porque resulta una herramienta poco útil para enfrentar en tiempo real las acciones



coordinadas del crimen organizado. Además se ha criticado que las cámaras de vigilancia son utilizadas por las autoridades policiales en colusión con el crimen organizado. También han surgido cuestionamientos que señalan lo costoso de su administración. Pese a estas críticas, la videovigilancia goza de buena salud en la opinión pública.

Cuando la videovigilancia queda a la deriva, funcionando con reducidos mecanismos de regulación, opera en sí misma como ley, ya que queda a la discreción de quien opera las cámaras decidir qué tipo de personas o colectivos deben ser monitoreados, qué tipo de información se recoge de ellos y cómo se debe almacenar, así como el tipo de uso que se le da a esa información.

La clasificación social genera efectos en el ejercicio de los derechos humanos en la medida en que ciertas personas y colectivos entran en un proceso de escrutinio particular marcado por los prejuicios construidos a su alrededor, los cuales pueden derivar en la implementación políticas de exclusión social. El hecho de que una persona o un grupo de personas esté en el foco de atención de un sistema de videovigilancia por el lugar que ocupa en un sistema de clasificación social afecta el ejercicio de su ciudadanía ya que se le trata de forma diferente de aquellos que han sido clasificados o tipificados como grupos que no son una potencial amenaza a la seguridad o el orden social.

Videovigilancia no regulada

Son pocas las leyes y reglamentos estatales o municipales que regulan la videovigilancia en México. En términos generales, centran su objetivo en dos aspectos: a) garantizar que la información que recogen sirva como elemento de prueba para castigar faltas administrativas y penales, y b) evitar las posibles violaciones al derecho de privacidad.

Por otro lado, sin embargo, se resalta la obligación de cuidar que la videovigilancia no vulnere ciertas garantías individuales y derechos ciudadanos. En este sentido, se le define, aunque sólo sea de manera implícita, como una actividad que no es exclusivamente de orden administrativo, sino que pone en juego la relación entre el aparato gubernamental y el ejercicio de la ciudadanía.

La ley de la Ciudad de México se distingue de las otras en el país porque trata de definir los criterios de instalación de videocámaras de vigilancia a partir de la sistematización de


información criminal, dejando de lado, al menos en la ley, los criterios de proporcionalidad e intervención mínima. Considera, por tanto, las tendencias en la estadística delictiva -a nivel de vecindarios, manzanas, avenidas y calles-, las áreas con el mayor reporte de infracciones a automovilistas, y aquellas que presentan riesgos en caso de fenómenos de origen natural.

Particularmente en la Ciudad de México, destaca la existencia de un protocolo detallado denominado "cadena de custodia" de las grabaciones. Este es un documento oficial en el que se asienta la forma en cómo se obtuvo la información, qué funcionarios tuvieron acceso a ella y con qué objetivos. Esto permite establecer candados sobre la inviolabilidad e inalterabilidad de las grabaciones, garantizando su conservación y cuidado.

La operación de la videovigilancia está determinada por el carácter humano de los operadores, quienes orientan la vigilancia hacia aquellas personas y comportamientos que consideran como sospechosos o inusuales. Esto pone de relieve el hecho de que la operación de las cámaras se encuentra de cierta manera alimentado por prejuicios y tipificaciones anclados en texturas culturales específicas, lo cual sugiere que las cámaras no siempre funcionan observando de forma homogénea al conjunto de la sociedad.

Más bien, la vigilancia se acentúa en los sectores tradicionalmente considerados como posibles responsables de alterar o poner en riesgo el desarrollo normal de la vida social. Se ha podido observar este tipo de uso de las cámaras en otros espacios donde autoridades municipales, por ejemplo, establecen el monitoreo de personas de la comunidad lésbico-gay en plazas públicas, a quienes se les sugiere dejar el lugar o no comportarse de una forma "anormal" o "inadecuada".

A esto hay que añadir el hecho de que las imágenes que se recogen, almacenan y procesan en los centros de videovigilancia pueden ser reproducidas en la televisión, en distintas plataformas de internet -como Youtube- o en redes sociales. Esto genera una conexión particular entre medios de comunicación e imágenes recogidas por los sistemas de videovigilancia, en el que ambos se retroalimentan permanente.

La videovigilancia no puede ser expulsada de nuestra vida ni borrada del paisaje urbano porque sirve para proteger y cuidar a la población, pero es necesario imponerle límites. Saber quién vigila, con qué criterios y cómo se transforma esa observación sistemática en información es un paso esencial para fortalecer la democracia y evitar que la gestión de lo social termine siendo administrada por lógicas opacas de clasificación y tipificación de grupos sociales. 



ELECTRÓNICA Y TECNOLOGÍA



REVISTA DIGITAL

ESPECIALIZADA EN ELECTRÓNICA Y TECNOLOGÍA

www.electronicaytecnologia.com



AUMENTAR LA SEGURIDAD DEL PERÍMETRO, una prioridad en los aeropuertos

Cada año se notifican numerosos incidentes de violaciones de seguridad perimetrales en aeropuertos de todo el mundo. Con cada infracción, los directores de seguridad se ven obligados a examinar cómo asegurar y administrar mejor sus propios límites, por lo que prevenir estas brechas se convierte en un gran desafío, especialmente para los aeropuertos que tienen millas y millas de propiedad para asegurar.

Cada año se notifican numerosos incidentes de violaciones de seguridad perimetrales en aeropuertos de todo el mundo. Con cada infracción, los directores de seguridad se ven obligados a examinar cómo asegurar y administrar mejor sus propios límites, por lo que prevenir estas brechas se convierte en un gran desafío, especialmente para los aeropuertos que tienen millas y millas de propiedad para asegurar.

El aeropuerto de la CDMX es uno de los más grandes en cuanto a dimensiones se refiere, y también uno de los más transitados del país y de América Latina. Tan solo en 2018 dio servicio a más de 47 millones de pasajeros y se tiene un registro de poco más de 9 mil empleados que a diario ahí laboran.

En ese sentido, a medida que se acerca la temporada de vacaciones los operativos de seguridad tanto terrestres como aéreos se refuerzan.

Información dada a conocer por la Secretaría de Turismo; para este verano, serán 9 millones 187 mil 514 turistas tanto nacionales como extranjeros los que se transportarán vía aérea, lo que significa 4.1 por ciento más en comparación con lo registrado en 2018.

En lo que respecta a las medidas de seguridad aeroportuaria, el factor humano es fundamental, sobre todo en lo que conocemos como temporada alta, con la presencia de operativos de fuerzas policiales y militares, que junto con las soluciones tecnológicas y el equipo propio de cada aeropuerto tratan de

IP UserGroup®
Latinoamérica
 Foro Internacional de Tecnología en Seguridad

EXPO
SEGURIDAD & CONFERENCIAS
"IP-in-Action LIVE MONTEVIDEO"

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, networking y
 aprendizaje más exitoso de la industria

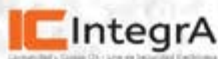


20 | MONTEVIDEO / URUGUAY
2019
 NOVIEMBRE | HOTEL NH COLUMBIA

COMPAÑÍAS EXPOSITORAS



ORGANIZACIONES ALIADAS



Tel.: +593 2 604 08 06 E-mail: pr@ipusergrouplatino.com

garantizar la seguridad de los usuarios y la operatividad de los vuelos.

Sabemos que ningún aeropuerto es 100 por ciento seguro. Por ello, los especialistas en evaluación de riesgos constantemente actualizan las pautas y estudian el panorama cambiante de las amenazas y la seguridad en estos lugares.

Para manejar las situaciones, los equipos de seguridad evalúan todas las variables de incidentes y cómo impactarían en las instalaciones, operaciones, personal y pasajeros. Sobre la base de estos criterios, los profesionales de seguridad aeroportuaria crean una amplia gama de planes de reacción y apoyo a las decisiones para responder rápidamente y mitigar cualquier interrupción. El objetivo es ayudar siempre a que las instalaciones regresen a operar de manera normal lo más rápido posible.

Y es que a diferencia de las zonas de abordaje donde los pasajeros pasan por controles de acceso, las zonas públicas y los perímetros se convierten en puntos críticos y es aquí donde la tecnología resulta un aliado para la seguridad de todos los usuarios.

El año pasado, por ejemplo, en el aeropuerto de Lyon en Francia, un hombre fue detenido tras forzar las barreras del aeropuerto y entrar con su automóvil a las pistas, obligando a suspender temporalmente las operaciones de los aviones.

Cuando se producen amenazas de este tipo como la intrusión en el perímetro o un comportamiento anormal, los operadores de seguridad deben coordinarse rápidamente y dar sentido a todos los datos que se presentan, pues estos nuevos datos en tiempo real se convierten en nuevos desafíos.

¿Qué se puede hacer?

Una plataforma de seguridad unificada y de arquitectura abierta proporciona una mayor conciencia situacional. De acuerdo con Jorge Sánchez, Gerente de Desarrollo de Negocios para Transporte de Genetec: "Al implementar un sistema de seguridad de arquitectura abierta, se puede unificar la vigilancia de video, el control de acceso y el reconocimiento de matrículas existentes para proteger y administrar mejor una terminal de pasajeros, el asfalto y el perímetro de un aeropuerto".

Empresas como Genetec, líder en sistemas de seguridad basados en redes IP con un portafolio de soluciones de seguridad unificadas, señalan que hay innovaciones constantes que llegan al mercado y que mejoran la intrusión y la protección de perímetros, como los sensores de microondas, de detección de cercas, sensores de detección de cables enterrados e incluso análisis de cables de conexión.

El gerente de Genetec para transporte comenta que para complementar la detección del perímetro, deben colocarse cámaras de alta resolución en lugares estratégicos que capturen imágenes claras y de largo alcance. Con la configuración estratégica, la primera línea de detección de perímetro en el cerco generará alertas que activan a las cámaras para que realicen automáticamente el zoom y la inclinación en el área objetivo para la identificación visual.

Así, la videovigilancia se envía directamente al centro de monitoreo de seguridad, o incluso como una alerta móvil al teléfono inteligente del director de seguridad, para una verificación y respuesta inmediatas.

La administración de estos dispositivos y alarmas directamente desde un sistema de mapeo integrado también ayuda a los operadores a identificar rápidamente otras cámaras cercanas para obtener una visión más amplia de la situación y la ubicación confirmada. Las cámaras combinadas de detección de perímetro, de largo alcance y alta resolución, y las herramientas de mapeo de ubicación aumentarán el tiempo de respuesta y minimizarán el riesgo de brechas.

Adicionalmente, acompañar estos sistemas de seguridad de arquitectura abierta con herramientas para la toma de decisiones como Mission Control, permite que se estandaricen los procesos y que en momentos de estrés y angustia, los operadores dejen a un lado las emociones y tengan herramientas que los guíen en todo el proceso. En esta herramienta, los datos complejos y correlacionados se revisan y gestionan en un espacio unificado, donde los incidentes se reportan, califican, distribuyen, resuelven y auditan de forma coherente y eficiente. Esto brinda, en el caso de los aeropuertos, nuevos niveles de inteligencia situacional, visualización y capacidades completas de administración de incidentes. **MS**

“Este tipo de tecnología se ha instalado en más de 150 aeropuertos de todo el mundo, convirtiéndose en un estándar líder en seguridad y seguridad de terminales de aeropuerto”, concluyó el gerente de Genetec.



INSCRÍBETE
YA!

ImpoSI de EGURIDAD

2019

29 • 30 • 31 OCTUBRE CDMX

HOTEL MARQUIS REFORMA

La **OPORTUNIDAD** de **ACTUALIZARSE** en temas de vanguardia
y lograr **CONSOLIDAR ESTRATEGIAS** eficaces y de calidad

TEMAS de **VANGUARDIA**
por **EXPERTOS CONFERENCISTAS**



ENRIQUE ESPINOZA
El mapa del camino
en la protección de activos



MARCO SANMIGUEL
La Seguridad en Centros
de Distribución, Transporte T1 y T2



IVAN BARRERA
Improvisación



EDGAR ESCOBAR
¿Cómo el Smart Data, genera mejoras operacio-
nales en diferentes industrias?



JOSÉ LUIS SÁNCHEZ
Gestionar crisis e incidentes en el retail

Actualízate!

PROCESOS

TECNOLOGÍA

INFRAESTRUCTURA

CAPITAL HUMANO



SÍGUENOS!



ANTADMEXICO



@ANTADMx

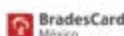
INSCRIPCIONES Y PATROCINIOS

☎ 5580 9900 Ext. 266

✉ bbrena@antad.org.mx

📞 5541887543

•••• Socios Estratégicos ••••



3 días
de
Conferencias
Networking
Dinámicas
y **MÁS!**

BIOMETRÍA MULTIMODAL

para combatir el robo



Uno de los grandes retos para cualquier negocio minorista en México es el robo hormiga. Esta clase de robo ocurre cuando las personas sustraen artículos pequeños, generalmente en pequeñas cantidades, de un establecimiento. Esta problemática se ha incrementado en 152% en los últimos 5 años, representando una merma anual para los negocios minoristas de México de hasta 160 mil millones de pesos.

Según datos de la Asociación Mexicana de Empresas de Seguridad Privada, el barniz, champú, lata de frijoles, perfumes, desodorantes, cervezas, dulces, quesos, bolillos, paquetes de jamón, tabletas electrónicas y audífonos son los artículos preferidos para el robo hormiga en el país.

Estos números han obligado a diferentes negocios a tomar diferentes medidas para asegurar su mercancía, tales como colocarla dentro de cajas transparentes con candado o cerrar los refrigeradores con llave. Métodos que a todas luces implican un gasto mayor de tiempo al momento de proporcionar la mercancía a los clientes.

Otro método utilizado con miras a disuadir este comportamiento es el uso de cámaras de seguridad. Es un método de protección especialmente útil cuando el robo ocurre por parte de algún

empleado. Este método también funciona para deslindar responsabilidades o para tener una imagen del ladrón posterior a la sustracción, pero no la evita.

Ante esta situación de inseguridad, muchas cadenas minoristas están optando por opciones tecnológicas que puedan evitar el robo en el instante en el que ocurre. Hoy en día esto es posible mediante el uso de biometría multimodal. Al combinar el uso de cámaras de videovigilancia con un software de reconocimiento facial y bases de datos de personas reincidentes o sospechosas. De esta manera, cuando una persona que se encuentra en esta lista accede al local se alerta a los empleados para que puedan tomar las medidas preventivas necesarias.

Si a esto le sumamos inteligencia artificial, el procesamiento de imágenes puede analizar más factores incluyendo expresiones faciales y movimientos oculares. Esta información se compara con patrones de comportamientos y expresiones sospechosas, lo cual permite al sistema lanzar una alerta para los empleados de modo que se prevenga un posible delito antes de que ocurra o antes de que el ladrón abandone la tienda.

La tecnología es el mejor aliado para ayudar a los comercios minoristas prevenir el robo hormiga y mitigar sus pérdidas. La necesidad de implementar la identificación biométrica para fortalecer las medidas de seguridad y personalizar los servicios del sector minorista crece de forma constante. Para ayudar en esta ardua tarea, NEC cuenta con un software de reconocimiento facial además de contar con 40 años de experiencia como integrador de tecnológico en el sector minorista. **XS**



✉ contacto@proyectosti.com.mx

☎ 01 800 58 10 689

🌐 www.proyectosti.mx



ROXTEC Líder Mundial en Sellado Pasamuros

Roxtec es una compañía sueca con más de 29 años en el mercado, creador de la tecnología Multidiameter y líder mundial en sellado pasamuros para infraestructuras críticas. Tiene presencia en más de 70 países.

A mediados del pasado mes de julio, Roxtec presentó a los medios de comunicación el Multidiameter, la invención de la empresa para la adaptación a cables y tubos de diferentes tamaños, basada en módulos de sellado de goma con capas desprendibles.

Roxtec ofrece soluciones de sellado completas para una amplia variedad de aplicaciones en muchos sectores. Los sellos de seguridad Roxtec se encuentran en tierra, mar y en aplicaciones subterráneas. También ofrece servicio y asistencia a clientes de más de 80 mercados a través de filiales y una amplia red de distribuidores.

Alfonso Guarneros, director de Roxtec para México y Latinoamérica, explicó que el interés de la empresa es trabajar con integradores que estén desde el principio de los proyectos, cuando se determina la ingeniería de estos para que desde el inicio se contemple la inclusión de una solución de sellado pasamuros.

“La solución modular de Roxtec permite un sellado perfecto, independientemente de la dimensión exterior del cable o la tubería. La solución simplifica el diseño y la construcción, acelera la instalación y reduce la necesidad de existencias, material y logística. También ofrece capacidad de repuesto para que las renovaciones y futuras actualizaciones sean más sencillas”, explicó Alfonso Guarneros.

En México y Latinoamérica existe poca consciencia de lo importante que es que cables y tuberías de instalaciones

de infraestructura crítica estén debidamente sellados y resguardados para evitar percances. Roxtec fabrica soluciones de sellado pasamuros que protegen los cables de polvo, vibraciones, pero también ante fuego en caso de incendio, lo mismo ante vibraciones en terremotos, pero sobre todo interferencia electromagnética.

De acuerdo con los resultados de un estudio realizado por Roxtec en 100 empresas mexicanas, el sector industrial registra 37 mil incidentes al año, de los cuales 40% no se informan de manera oficial, lo que indica que la seguridad no es prioridad en el momento de la puesta en marcha de los proyectos.

Karla Trejo, gerente de Mercadotecnia de Roxtec Latinoamérica, señaló que el 55% de las empresas considera importante colocar un sellado pasamuros multidiameter como el de Roxtec pero solo el 4% lo hace, por lo que la oportunidad de negocio es grande.

“En el 47% de los casos no se invierte en la solución principalmente por el precio inicial de la misma, por lo que el argumento de venta de los integradores deberá ser el ahorro del costo que representa una falla que eche abajo su infraestructura”, explicó.

Roxtec participó en la instalación del centro de datos del banco Santander en Querétaro, también trabaja con Banorte, el Sistema de Transporte Colectivo Metro de la Ciudad de México y con armadoras de autos. Otro de sus clientes es la Comisión Federal de Electricidad (CFE).XS



A SUME

Agrupaciones de Seguridad Unidas por México

PRINCIPALES OBJETIVOS

Fortalecer al sector en la cúpula empresarial.

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

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



asumeseguridad.org





Todo un éxito la trigésima quinta edición **“FERIA INTERNACIONAL DE SEGURIDAD E+S+S”**

Con la asistencia de más de 11,000 visitantes profesionales, la participación de 200 expositores de alrededor de 20 países, el desarrollo de más de 120 conferencias técnico - comerciales, la realización por primera vez del Foro de Pensamiento Estratégico de Seguridad y la generación de más de 4,000 millones de pesos en sólo el primer día de la rueda de negocios, de cuatro que duró el evento y en los cuales el intercambio comercial entre inversionistas y empresarios, fortaleció el desarrollo de oferta y demanda del sector, cerró sus puertas la trigésima quinta edición de la Feria Internacional de Seguridad.

Patricia Acosta, directora de la feria, precisó que “este año unimos a estos grandes escenarios, propuestas tecnológicas, productos y servicios de seguridad privada, centros de comando y control, ciberseguridad y vehículos interconectados, elementos claramente complementaron la red de soluciones en seguridad y protección para nuestros usuarios”.

“De igual forma, estamos muy felices con los resultados de la rueda de negocios, pues participaron compradores

internacionales provenientes de Ecuador, México, Nicaragua, Panamá, Perú, Venezuela y Colombia, con quienes se lograron efectuar 238 citas”.

Por su parte, Javier Villareal, Gerente Vertical de banca de HikVision, reveló que “logramos importantes contactos y clientes potenciales nacionales e internacionales. En esta edición aumentó el nivel de asistentes por las experiencias que generan nuestros productos, calculamos más de 1,800 personas que visitaron el stand en los primeros tres días de la feria, este dato fue obtenido por el sensor que se encuentra en el túnel del stand que nos ayudó a contabilizar las personas que nos visitaron”

Martín Otazo, Director de Mercadeo Latam Dahua Technology, manifestó que “las expectativas de sacar proyectos en la feria fue muy positivo, logramos contactos de Gobierno y verticales importantes, por lo que prevemos realizar proyectos muy grandes en especial con temas gubernamentales”.

En cuanto a Melexa, su gerente Alexandra González, indicó que “fue un espacio innovador que nos permitió presentar las últimas tendencias y las nuevas maneras

DISEÑO DE INGENIERÍA

SERVICIOS:

- Comissioning
- Desarrollo e Integración
- Instalación y Mantenimiento
- Administración de Proyectos

SISTEMAS:

- Inteligencia Artificial (IA)
- Incendio (Detección y Extinción)
- Control de Accesos (Biometría)
- CCTV (IP)
- Central de Monitoreo con reporte directo al C-4 en la Ciudad de México

Comexa Totalmente conectado a ti



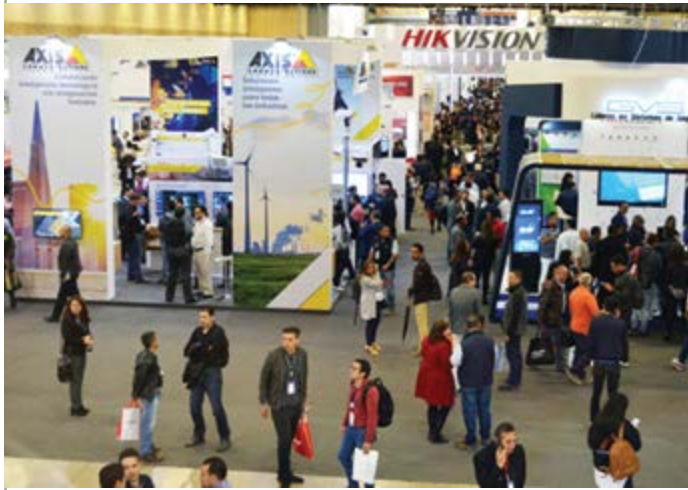
**Integradores de
Sistemas Electrónicos de
Seguridad**

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

Av. Universidad 989 – 401. Col. Del Valle, Benito Juárez, 03100. CDMX

Tels. 5685 7830 / 5685 7837 / 01 800 2 COMEXA

ventas@comexa.com.mx



de mostrar las soluciones para la seguridad laboral. Logramos un impacto grande con los tres lanzamientos que hicimos y las reuniones como el Smart Plays Solutions 3S, presentando las soluciones inteligentes en el suministro de consumibles para las empresas”.

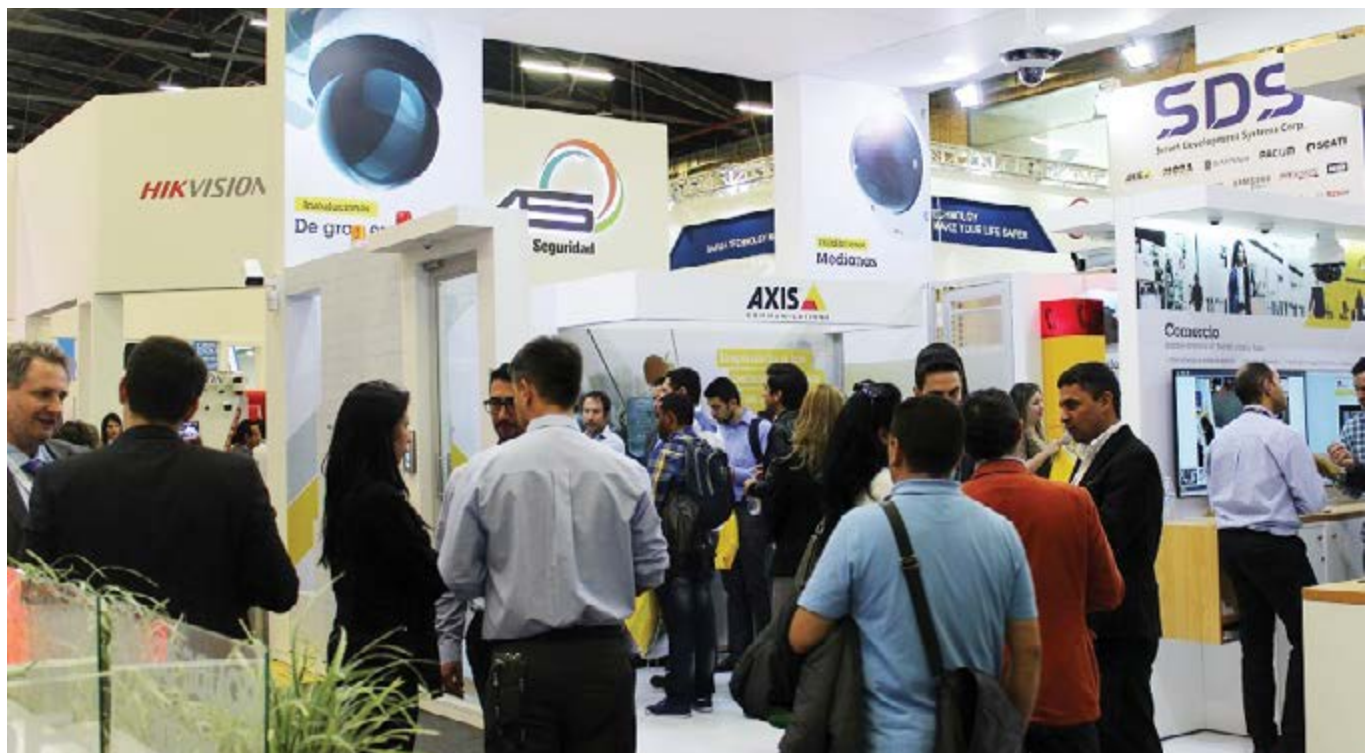
Camilo Peralta, gerente de Canales de Globaltex, reveló que “la comparación de la feria del 2018 al 2019 es en la cantidad de clientes o contactos que se lograron en esta. Estimamos que fueron alrededor de 250 potencialmente para proyectos y que las ventas aumenten en el próximo trimestre en un 82 por ciento”.

Mario Aguirre, Technical Manager de Ztkteco, argumentó: “llevo cuatro años en la feria y esta edición tuvo un éxito importante. Este espacio ha hecho que

se conozca aún más la marca, por lo cual calculamos que nos visitaron de alrededor de 1,500 personas”.

Romel Cetina, coordinador de ventas de Indexcol, precisó que “la revolución del mundo avanza rápido, por eso a nivel de protección contra incendios estamos desarrollando nuevos productos que han disminuido los riegos, los cuales pudimos exponer con éxito en la Feria Internacional de Seguridad”.

Finalmente, la directora de la Feria recalcó que “este año presentamos las más claras innovaciones acordes a las exigencias de los mercados que ven en la implementación de soluciones correctas de seguridad, el pilar de desarrollo de las organizaciones modernas, que con gran responsabilidad evolucionan en la mitigación de las amenazas tradicionales y emergentes”.



INTCOMEX

consolida su estrategia IoT Transporte

Con el objetivo de masificar su propuesta de transporte, dentro del negocio del IoT, Intcomex, presentó Mobileye una solución para la conducción autónoma de vehículos nivel 1, mediante la integración de un sistema de cámaras y sensores que se colocan en la parte frontal y lateral de los vehículos, capaces de identificar objetos cercanos para prevenir colisiones generando alertas pasivas para el conductor.



La marca cuenta con cerca de 20 años de desarrollo de negocio de visión artificial; hoy tiene casi el 90% del mercado y más de 30 millones de vehículos circulando con su tecnología. En el IoT Transporte busca integrar sensores, hardware y software dentro de plataformas que permitan a los usuarios finales tener mejor control de su operación, reducir los costos operativos y hasta la prevención de colisiones y accidentes.

Rafael Danon Sprits, director regional de la vertical IoT Transporte en Intcomex, explicó que la división ha crecido y ya comenzaron a trabajar con partners con los que están apoyándose, sobre todo en lo que a logística se refiere. Reveló que a la fecha ya cuentan con más de 100 socios que comercializan este tipo de soluciones en la región y en México existen cerca de ocho mil Mobileyes instalados; cifra que buscarán duplicar en menos de un año.

De igual manera, reconoció que el tema de financiamiento resulta vital para este tipo de soluciones por lo que hoy ya cuenta con esquemas de financiamiento y arrendamiento, con modelos para el usuario final que va desde 12 hasta 72 meses, de acuerdo a las necesidades del cliente.

Adicionalmente, la propuesta del mayorista integra la oferta de Amber Connect, solución de telemetría con GPS y portales por industria para control de flotas; la oferta de Hikvision para videovigilancia y reconocimiento facial en el segmento de Transporte; y próximamente presentará una nueva marca para el conteo de pasajeros.

Llevar aspectos tecnológicos de IoT a la industria del transporte puede derivar en diferentes beneficios, desde un mejor control en su operación, reducción de costos operativos, llegando a la prevención de accidentes, colisiones, siniestros, e incluso a salvar vidas.

La empresa está trabajando en conjunto con marcas como Hikvision y Dahua para el tema de videovigilancia interna en el transporte y con otros partners como Microsoft e Intel que apoyan a Intcomex con nuevas marcas para ampliar el portafolio.

La mayoría de los proyectos que tienen están en Europa y en Estados Unidos, pero la marca se interesó en México porque es un mercado estratégico y una de las economías más importantes del mundo en la industria automotriz. **MS**

INFOCOMM MÉXICO 2019

multiplicó por tres su exhibición comercial y oferta educativa

Ciudad de México.- La novena edición de InfoComm México llegó a su fin con un saldo positivo en el que destaca una mayor variedad de empresas exhibidoras, un robusto programa educativo con más de 70 conferencias especializadas y la realización simultánea de DataNet México y el Congreso TecnoTelevisión México; un par de eventos que complementaron, tanto la muestra de marcas, productos y servicios, como la disponibilidad de información y la posibilidad de generar nuevas relaciones comerciales entre los asistentes. InfoComm México 2019 se llevó a cabo del 14 al 16 de agosto en el WTC de Ciudad de México con una audiencia acumulada de 5,788 participantes.

Desde nuestra primera edición, el evento ha crecido a buen ritmo, tanto en el piso de exhibición, como en la cantidad y calidad del programa educativo. Trabajamos para ampliar el panorama del evento al atraer mercados de tecnologías complementarias como redes, datos y cableado estructurado con la oferta de DataNet México. Y este año, incluimos al mundo de la producción de video y broadcast con la realización de la primera edición de TecnoTelevisión México”, indicó Víctor Alarcón, gerente de Proyectos de InfoComm Latinoamérica.

Como es costumbre, el programa educativo despertó un gran interés, pues contó con la participación de expertos académicos y de asociaciones de profesionales, además de especialistas de diferentes compañías de la industria de integración audiovisual, TI, producción de televisión y medios digitales. En total, 1,675 participantes se dieron cita a las más de 70 sesiones de conferencias presentadas en las agendas de InfoComm, DataNet y TecnoTelevisión.

“La parte educativa ha sido medular, porque es una oportunidad para ponerse al día en cuanto a tecnologías y tendencias, lo que ayuda a entender cómo se comportará el mercado en un futuro cercano. En los últimos tres años, en conjunto con AVIXA, hemos puesto especial énfasis en los mercados y aplicaciones verticales como señalización digital, tecnología AV para templos religiosos, casa inteligente, comunicaciones unificadas, colaboración; centros y cuartos de control y monitoreo, añadió Víctor Alarcón.

Por su parte, DataNet México, la exposición y congreso de las tecnologías de Redes, Voz y Datos, enfocada a diseñadores,




instaladores, integradores, fabricantes y usuarios finales del sector TI; sumó un año más como parte del evento.

A decir de Alejandra García, gerente de Proyecto de DataNet México, la edición 2019 dejó muy satisfechos a los organizadores, pues se mejoró la exhibición en todos sentidos, creció la cifra y calidad de los expositores, inclusive el diseño de sus espacios. “Es la segunda edición del evento de manera independiente y en alianza con InfoComm. Desde el primer día tuvimos una excelente afluencia de asistentes con flujo constante, con una alta calidad en las conversaciones y contactos que han hecho nuestros expositores, apuntó la responsable de DataNet México.

“En lo académico, robustecimos el programa y llevamos las conferencias en el mismo piso de la feria, lo que facilitó que más participantes aprovecharan las trece charlas abiertas. Además, tuvimos cursos exclusivos de cuatro horas de especialización en centro de datos y redes ópticas pasivas, temas que están tomando fuerza para la capacitación, agregó Alejandra García.

Gracias a la buena respuesta de los expositores al reservar sus espacios para 2020, la décima edición de InfoComm México está asegurada. Se trata de nuestra feria más grande en la región y, aunque nos falta mucho por crecer, la estabilidad de la economía mexicana nos da confianza para seguir adelante. La industria de integración AV está en pleno desarrollo, tenemos el compromiso de mostrar sus beneficios a los nuevos clientes y usuarios, pues estas tecnologías nos ayudarán a ser más productivos, a comunicarnos y entendernos mejor, además de generar ahorros en muchos sentidos”, concluyó Víctor Alarcón de InfoComm Latinoamérica.

Bajo la organización conjunta de AVIXA (The Audiovisual and Integrated Experience Association) y la revista AVI Latinoamérica, la próxima cita del evento será InfoComm Colombia 2019, que se llevará a cabo del 23 al 25 de octubre, en el Gran Salón de Corferias, en la ciudad de Bogotá.

La décima edición de InfoComm México está programada para los días 19 al 21 de agosto de 2020, en el WTC de Ciudad de México. 



CONTROL

DE ACCESOS MX



REVISTA DIGITAL
ESPECIALIZADA EN CONTROL DE ACCESOS

www.controldeaccesosmx.com

CONTROL DE ACCESO

“La primera línea de defensa”

Por Rafaela Silva, Security Supplier Relation Manager, Anixter Caribbean & Latin America

Dentro de la tecnología de seguridad electrónica, el control de acceso está en la cima de la pirámide en términos de criticidad, junto con los sistemas de detección y alarma contra incendios. Por ejemplo: Si comparamos el control de acceso con circuito cerrado de televisión o con detección de intrusos, si una cámara o sensor no estuviera funcionando, incluso el usuario común del sistema podría notar este fracaso. Sin embargo, si hay alguna falla de funcionamiento en el control de acceso, se darían cuenta de inmediato, debido a que el usuario no podría entrar en el sitio protegido. Y lo que es peor, ¡no podrá salir! Y en caso de una situación de emergencia como el comienzo de un incendio, esto puede ser crítico.

De ahí la importancia de elegir una solución de control de acceso segura, confiable y estable.

El control de acceso electrónico ha surgido para resolver algunos problemas relacionados con el uso de llaves, cerraduras y cerrojos mecánicos. El uso de la llave metálica convencional, tal y como la conocemos hoy, tiene varios factores negativos. Los principales se discuten a continuación:

- **Las llaves pueden ser copiadas:** Al portar una llave, se puede ir a cualquier cerrajería y solicitar una o más copias;
- **No hay un histórico:** No es posible saber la fecha y hora en que un portador de una llave entre o salga de un lugar específico, ni el número de veces que lo hizo.

- **Pérdida de llaves:** Cuando esto ocurre, es necesario el intercambio de juegos de cerraduras y cerrojos para mantener el lugar seguro.
- **No hay tiempos de restricción:** El portador de la llave puede entrar en el sitio protegido en cualquier día y hora determinada, incluyendo fines de semana y días festivos.
- **Gestión de la posesión de llaves:** ¿Con quién está cada llave? Esta es una pregunta difícil de responder si no hay un control eficiente de las llaves.
- **Llaves Múltiples:** Para cada puerta se requiere una llave separada. Esto lleva a que los gerentes tengan que portar diferentes llaves.

El control de acceso electrónico resuelve todos los problemas anteriores. En lugar de una llave de metal, que se puede copiar fácilmente, ahora se utiliza una tarjeta electrónica que puede tener distintos mecanismos de cifrado y protección contra la duplicación, garantizado por los fabricantes. Además, los lectores biométricos pueden ser programados para prevenir que un usuario utilice la tarjeta de otra persona.

Con el control de acceso se puede restringir fácilmente días y horarios de acceso y emitir informes detallados de la actividad del usuario. Una sola tarjeta puede abrir todas las puertas desde que, obviamente, tenga los permisos de acceso para hacerlo.



Hoy en día, con la creciente adopción de equipos tercerizados de seguridad, el control de acceso ha tenido un papel muy importante para las empresas. Como la rotación de este personal de seguridad es alta, el personal de seguridad no es capaz de reconocer a todo el personal y saber si una persona pertenece o no a ese lugar en particular. Con el uso de un sistema de control de acceso electrónico, cada usuario debe utilizar su tarjeta, contraseña o biométrica para entrar en el espacio protegido. Por lo tanto, el criterio de autorización es impersonal, es decir, es realizado de forma automática por el sistema de control de acceso.

La primera variable que se fijará a la hora de elegir un sistema de control de acceso es la tecnología del lector y tarjeta. En la actualidad hay varias tecnologías como código de barras, magnética, Wiegand, Proximidad de 125 Khz, Smart Card (de contacto y sin contacto) o lectores biométricos. Muchas de estas tecnologías ya están obsoletas, y las que todavía están vigentes son: Tarjeta inteligente (Smart Card) con cifrado de clave propia y los lectores biométricos.

El control de acceso es la parte principal de la pirámide de criticidad de sistemas de seguridad. Así que la elección de una solución fiable es clave.

En cuanto a la topología, los sistemas de control de acceso se pueden clasificar como: Autónomo "Stand Alone" Con base en el servidor "Server based" o híbrido con Inteligencia Distribuida. A continuación hay una breve descripción de la operación de cada uno:

Sistemas Autónomos "Stand Alone": Se trata de sistemas que tienen su propia inteligencia y no requieren de software para operar. Toda la base de datos de usuarios y los permisos se almacenan en su memoria interna. Por lo general se trata de sistemas con capacidad limitada y no permiten la administración remota. Pueden ser auditables o no.

Sistemas en línea: En esta topología toda la inteligencia está en el servidor que es responsable de la liberación del acceso. Cuando una solicitud de acceso viene a través de un lector (proximidad, magnético, barras, biometría, etc.), se envía a un servidor, que va a revisar el nivel de otorgamiento de autorización, dando o no el acceso y devolviendo el comando de liberación.

Sistemas con Inteligencia Distribuida: En esta topología toda la inteligencia se encuentra en el controlador que es responsable de la liberación de acceso. Tras la liberación, el evento se envía al software en el servidor para el seguimiento y presentación de informes. En caso de pérdida de comunicación con el servidor se libera el acceso y se almacena el evento. A continuación se muestra un diagrama que muestra la topología de un sistema de control de acceso con inteligencia distribuida:

Los sistemas de control de acceso de inteligencia distribuidos son los más recomendables, ya que garantizan un funcionamiento incluso en caso de una caída de la red de comunicación o de fallo del servidor.

En resumen, a continuación encontramos algunas recomendaciones técnicas para la elección de una solución de control de acceso confiable y seguro:

El sistema de control de acceso debe:

- Tener su funcionamiento basado en la topología: Inteligencia distribuida;
- Permitir la integración con otros sistemas como CCTV, alarma contra intrusos, detección y alarma contra incendios, automatización, etc.;

- Utilizar tecnología de tarjetas inteligentes con cifrado para lectores/tarjetas y/o lectores biométricos en las zonas más restringidas;
- Tener arquitectura IP de comunicación entre los controladores y el software, con cifrado.

Además, es esencial elegir una empresa integradora certificada en la solución y con experiencia en el control de acceso.

Optar por una solución de control de acceso abierta que no se comercialice exclusivamente por una sola empresa. Con esto, el usuario final será libre de cambiar el instalador, en caso de que no esté prestando un buen servicio. **MS**



El control de acceso es la parte principal de la pirámide de criticidad de sistemas de seguridad. Así que la elección de una solución fiable es crítica. El uso de tecnologías de control de acceso ha crecido enormemente en los últimos años. Sin embargo, existen en el mercado muchas soluciones que no cumplen con los requisitos mínimos de seguridad, confiabilidad y estabilidad que estos sistemas requieren.

CONTROL DE ACCESOS

en oficinas bancarias



Las continuas fusiones entre entidades financieras, la reducción del número de oficinas de atención al público y el cambio en su modelo, unido a las nuevas formas de delito, obligan a los bancos a extremar la seguridad de las oficinas adaptándose a la evolutiva normativa vigente. Estas entidades están obligadas por ley a contar con medidas específicas de seguridad – que pasan tanto por su protección tecnológica como por el diseño de sus instalaciones, un exhaustivo mantenimiento de sus sistemas y la obligatoriedad de tener un director de seguridad que vele por su correcta implementación.

Los riesgos en las sucursales de banca han ido cambiando con los años: si hasta ahora los atracos en horario de atención al público eran los peligros más frecuentes, últimamente están proliferando los “atracos a la espera”, consistentes en realizar un butrón para esperar dentro de la oficina la llegada del primer empleado que cuenta con las claves para desbloquear la caja fuerte. A éstos, hay que sumar el fraude tecnológico que sigue en aumento y se puede llevar a cabo sin la intromisión física en las oficinas.

Incremento de la seguridad para el acceso a la cámara acorazada

En espacios que requieran una seguridad especial, como las cámaras acorazadas, se puede requerir el acceso por doble

custodia que implica la presentación de 2 tarjetas de usuarios autorizados dentro del horario especificado, o doble custodia con escolta, en la que uno de los dos usuarios autorizados ha de tener el nivel de escolta, o bien asignar calendarios de apertura y cierre.

Control remoto del acceso a las cajas de depósitos nocturnos

Asegura que solo los empleados que dispongan de dicho control remoto podrán acceder a la zona donde se resguardan los sobres con dinero en efectivo que los clientes han depositado en las cajas de depósitos mientras la oficina estaba cerrada.

Reducción de costos por pérdidas y duplicados de llaves

Los costos asociados a los cambios de cerraduras y llaves, sumados a los tiempos de inproductividad y falta de seguridad que provocan, se solucionan sustituyendo las llaves por tarjetas magnéticas que se pueden dar de baja y reponer de forma rápida con el mínimo costo.

Restringir el acceso por horarios y calendario

Aplicar la restricción en función de los diferentes tipos de usuarios o bien por el nivel de seguridad del área protegida



y los diferentes niveles de puertas asociados a dicha área, pudiendo requerir acceso mediante Nip + Tarjeta, en función del tipo de área, puerta, calendario y horario.

Interbloqueo automático entre cajeros

Configurar el interbloqueo de modo que no se permite la apertura de uno de los cajeros, hasta que todos los demás están cerrados.

Exclusión del acceso externo

Prevenir el acceso externo de los empleados o clientes a la sucursal ante eventos críticos, como un atraco.

Reducción de los costos derivados de la formación del personal

Menos formación del personal en el manejo del sistema de seguridad, al crearse un entorno de seguridad más automatizado.

Incremento de la seguridad de los cajeros

Aumentar la seguridad mediante su conexión automática al cerrar la puerta, la detección del fallo en el cierre de la misma o al exceder el tiempo de apertura programado.

Control automático de los sistemas de esclusas

Este sistema se basa en encadenar dos accesos consecutivos en los que la persona debe acreditarse. La apertura de los accesos es retardada para permitir decidir qué actuación debe realizarse en caso de ataque a la seguridad de la oficina bancaria.

Control del personal

Un control efectivo sabiendo en todo momento quién accedió dónde y cuándo, también impidiendo el acceso a ciertas áreas o a zonas restringidas o con información confidencial. **XS**



Familia XBIO

Terminales de tiempo y asistencia y control de acceso con biometría integrada.

Pantalla táctil*

Pantalla a color de 4.3 "con resolución de 480x272 píxeles ofrece una reproducción detallada y bien definida para que las transacciones se puedan mostrar y se puedan ingresar razones seleccionables con un simple toque.

Teclado

Las terminales de la familia XBIO están equipadas con un teclado numérico que permite identificar al usuario con: solo el código escrito en el teclado o el código asociado con la huella digital.

Biometría integrada

La terminal puede almacenar hasta 9,500 huellas dactilares y gestionar hasta 9,900 usuarios. También es posible memorizar la huella digital en la tarjeta del usuario (tarjeta inteligente, por ejemplo, Mifare) que permite superar los límites de las huellas digitales y también evitar el almacenamiento de datos biométricos sujetos a reglas de seguridad especiales.



CONTACTO:
Iztaccíhuatl #158 Col. Florida Del. Álvaro Obregón
C.P. 01030 Ciudad de México
TEL: +52 55 6308 4067
EMAIL: info@rodhe.com.mx

@RodheMx rodhe.com.mx
/RodheSeguridad store.rodhe.com.mx
/RODHESEGURIDAD360

* Disponible solo para X3BIO.

EL LADO OSCURO DE LAS BARRERAS DE SEGURIDAD:

encontrando el equilibrio dispositivos

Por Kurt Measom

Los torniquetes y las puertas giratorias de seguridad están diseñados para funcionar perfectamente y sin problemas, de modo que las personas puedan atravesarlos sin tener que entrar nunca en contacto no deseado con las barreras. Cuando las personas están bien capacitadas, que es un componente necesario para una implementación exitosa, las entradas de seguridad son muy efectivas para mitigar la posible pérdida catastrófica de propiedad, vida, continuidad, etc., como parte de un plan general de seguridad física.



El lado oscuro de las barreras: Contacto

Sin embargo, ahora hay algo en qué pensar antes de instalar cualquier tipo de entrada de seguridad. Todos los tipos de entradas automáticas tienen barreras que se mueven: estas se balancean, giran, deslizan o caen. Cuando las personas atraviesan barreras móviles, existe la posibilidad de contacto y lesiones potenciales.

La buena noticia es que las entradas de seguridad de hoy vienen equipadas con tecnología de sensores avanzada que se coloca estratégicamente para evitar el contacto. Sin embargo, la verdad es que las personas pueden caminar directamente hacia las barreras o pueden moverse tan rápida e impredeciblemente que los sensores no pueden responder lo suficientemente rápido.

Como ocurre el contacto de barrera

¿Cómo sucede el contacto?

A veces las personas se distraen o se apresuran, y pueden presentar su licencia de

conducir en lugar de su tarjeta de proximidad y caminar directamente hacia las barreras. O bien, están hablando por teléfono o enviando mensajes de texto y no viendo lo que hacen las barreras: en una puerta giratoria de seguridad, una persona está en el teléfono y entra en el siguiente compartimiento de la puerta después de un usuario autorizado; la puerta siente que es un intruso y deja de girar y el usuario se pega en el vidrio del ala de la puerta.

Un lector de tarjetas altamente encriptado tarda una fracción de segundo más de lo previsto para leer las credenciales de alguien. La barrera también tardará una fracción de segundo más en abrirse, y la persona puede caminar y pegarse en la barrera antes de que realmente se abra.

Si una persona se apresura en un carril de torniquete óptico para ir detrás de un usuario autorizado, podría haber contacto dependiendo del tiempo. La barrera puede simplemente cerrarse justo en frente de ellos o pueden acercarse a ellos desde los lados (barreras deslizantes).

Estas cosas pasan. Entonces, ¿qué puede hacer usted al respecto?



Diagrama 1

Balanceando la seguridad, la protección y el flujo de usuarios

El contacto de barreras es algo que claramente desea evitar, pero ¿cómo? La clave es encontrar un equilibrio entre la seguridad y el nivel de seguridad que necesita, así como un nivel de flujo de usuarios de la entrada que funcione para usted. Si observa el diagrama 1, verá que describe la relación entre seguridad, protección y flujo de usuarios cuando se trata de implementar una entrada de seguridad. Usted querrá encontrar su "punto óptimo" donde dirigir los tres al mejor grado posible; esto se muestra con el punto donde los círculos se superponen.

Aquí hay algunos ejemplos extremos que describen las partes externas de cada círculo en el diagrama:

- **Si usted solo deseara la Seguridad:** las barreras solo se moverían muy lentamente y nunca tocarían a un usuario. Se equivocarían por precaución y se abrirían, incluso para los intrusos, para evitar el contacto.

- **Si usted solo deseara la Protección:** entonces las barreras se cerrarían sin importar lo que impidiera que la gente entrara. La gente podría verse afectada y el flujo de usuarios probablemente sería más lento debido a un mayor número de usuarios rechazados.
- **Si usted solo deseara el Flujo de Usuarios:** entonces la gente podría volar a través de las entradas y nunca habría una acumulación, pero alguien podría salir lastimado o entrar sin que lo vieran.

Con un análisis cuidadoso de sus necesidades, puede encontrar el mejor equilibrio entre la seguridad, la protección y el flujo de usuarios. Si bien todos son importantes, cada implementación es única y hay productos y configuraciones específicas que funcionan mejor para optimizar cada situación. Sobre todo, siempre que sea posible, capacitar al personal sobre el uso correcto de las entradas de seguridad puede ayudar a minimizar los errores que podrían causar cualquier problema, permitiéndole maximizar los tres factores importantes. **MS**

INTERTRAFFIC MÉXICO

se asocia con ITS México



De izquierdo a derecha: Laura Barrera (Tarsus Mexico), Ing. José C. Azcárate Beltrán (ITS México), Editha Hoogenberg-Derksen (Intertraffic Mexico / RAI Amsterdam)

Nos complace anunciar nuestra nueva alianza con ITS México. Gracias a esta asociación podremos agregar un valor extra tanto a nuestra exposición como a nuestro programa de conferencias. Estamos muy contentos de combinar nuestras fortalezas, conocimientos y contactos. Juntos aceleraremos la transición de la movilidad en Latinoamérica. ITS México será parte de nuestro Consejo Consultivo y del jurado del Intertraffic Award Latin America.

Intertraffic México, hace la invitación a su exposición los próximos 12, 13 y 14 de noviembre; este evento tiene como propósito reunir en un mismo lugar a expositores y personas interesadas en movilidad, infraestructura, gestión del tráfico, seguridad y estacionamientos.

En este espacio se podrá hacer intercambio de ideas para que los asistentes mejoren su 'know-how', establezcan negocios rentables y tengan acceso al mercado de movilidad en México.

La invitación está dirigida al público en general, pero principalmente a visitantes con perfil del sector público como la Secretaría de Comunicaciones y transportes, autoridades del transporte público, autoridades del aeropuerto, instaladores de sistemas de gestión de tráfico y de estacionamientos, empresas de mantenimiento de carreteras, operadores de transporte público y privado, entre otros.

Los expositores tendrán un perfil relacionado con la fabricación de equipos y soluciones de gestión de estacionamientos, desarrollo de infraestructura, fabricación de equipo de seguridad de tráfico, instituciones financieras públicas, agencias federales y de gobierno central en busca de inversión privada, integración de sistemas de gestión de tráfico urbano e interurbano, y más.

El evento se llevará a cabo en Centro Banamex de la Ciudad de México ubicado en Av. Del Conscripto 311, Colonia Lomas de Sotelo, en un horario de 12:00 a 19:00 horas. El registro es gratuito y se puede realizar en: <https://www.intertraffic.com/es/mexico/> **MS**

ASIS CAPÍTULO MÉXICO

“Seguridad en parques eólicos”

El pasado 6 de agosto se realizó la reunión mensual de ASIS Capítulo México, en el lugar de costumbre, la Hacienda de Los Morales, en la Ciudad de México.



Alberto Frieddman, director general de PROSA

Pedro Sanabria, presidente del Capítulo, presentó su informe mensual de actividades, en el que destacó el crecimiento constante en el número de socios y los reconocimientos que otorgó ASIS Internacional al equipo del Capítulo México. En esta ocasión se reconoció la labor de Enrique Tapia Padilla, CPP, presidente del Capítulo en 2011.

Para finalizar, Pedro Sanabria, invitó a los asistentes al próximo evento de seguridad integral que se realizará del 13 al 17 de octubre en el centro Citibanamex, el Security Week, lo que antes era el Congreso Latinoamericano de Seguridad ASIS. En esta ocasión, además de las conferencias en diferentes formatos y la zona de la Expo, se busca la realización de sesiones de networking, y generar espacios de aprendizaje y diálogo.

La empresa patrocinadora de la reunión fue Procesos Automatizados, S.A. de C.V. (PROSA), por lo que Alberto Frieddman, director general adjunto de la empresa, dio la bienvenida a los asistentes y realizó una breve reseña de la historia de esa empresa.

Por otra parte, Armando Zúñiga Salinas, director general de Grupo IPS, invitó a los asistentes al Diplomado en Desarrollo de Empresas de Seguridad Exitosas y Sustentables, organizado por Agrupaciones de Seguridad Unidas por México (ASUME), la Universidad Panamericana y el High Potential Development Center. También rificó una beca para ese diplomado.

La conferencia de este mes estuvo a cargo de Eduardo González Martínez, DSI, gerente de seguridad corporativa para Latinoamérica Norte de Siemes Gamesa, y que llevó por título “Seguridad en parques eólicos y los retos sociales que implica”.

“En México, los parques eólicos generan el 6% de la electricidad, por eso es vital que los colaboradores conozcan a la perfección las buenas prácticas y la autoprotección, dentro y fuera de los proyectos. La implementación de estudios y de programas de seguridad, así como una mayor concientización social son elementos clave para su seguridad”.

Afirmó que el sector busca implementar programas de concientización entre las comunidades e impulsar las actividades económicas de las poblaciones. Los proyectos también tienen el objetivo de tener una mayor capacidad de gestión de seguridad, pues una mala administración puede llevar a la cancelación del proyecto.

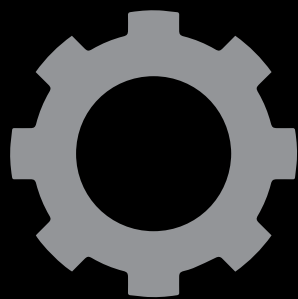
Otros retos que enfrenta este sector son de tipo logístico y de transporte para la movilización de materiales de construcción y montaje, desde que llegan a los puertos y hasta su destino final. Actualmente existen 59 parques eólicos en México, distribuidos en Baja California, Zacatecas, Chiapas, Jalisco, Nuevo León, Oaxaca, San Luis Potosí, Tamaulipas y Puebla. **XS**



Eduardo González Martínez, DSI, gerente de seguridad para Siemes Gamesa



Pedro Sanabria, Presidente de Asis Capítulo México (izquierda) y Enrique Tapia Padilla, CPP



SEGURIDAD INDUSTRIAL



REVISTA DIGITAL

ESPECIALIZADA EN SEGURIDAD INDUSTRIAL

www.seguridadindustrialmx.com



**ENTRE EL 20 Y 33 % DE
LOS POLICÍAS Y CIVILES**

viven con problemas ergonómicos



SafeStart es un programa de concientización de seguridad laboral de gran éxito en el mundo, cuenta con un portafolio de capacitación, enfocado al Factor Humano, así como un segmento direccionado a la Ergonomía personal, busca disminuir los daños en columna, cadera u hombros provocados por la utilización de chalecos antibalas o armamento de más de 5 kilos de peso.

Nelson Gutiérrez, Master Training de SafeStart, dijo que en México y en el resto de los países es común padecer daños en la salud por malas posturas “Según datos de la Organización Mundial de la Salud, las afecciones musculoesqueléticas son el segundo mayor contribuyente a la discapacidad en todo el mundo, y el dolor lumbar es la principal causa de discapacidad a nivel mundial. Si bien la prevalencia de las afecciones musculoesqueléticas varía según la edad y el diagnóstico, entre el 20% y el 33% de las personas en todo el mundo viven con una afección musculoesquelética dolorosa”.

Por ejemplo, si un policía o militar, por complacencia o exceso de confianza, se agacha de la misma manera que siempre lo ha hecho, doblando el tronco y no flexionando las piernas, los 5 kilogramos de peso del chaleco, aumentan considerablemente los kilogramos fuerza, que debe soportar su espalda baja o región lumbar para levantarse.

Si esto lo hace muchas veces durante el día, con el paso de los años, va a experimentar alguna dolencia. Por tal razón es clave, mostrarle lo valiosos que pueden ser los buenos hábitos relacionados con la ergonomía.

Este tipo de lesiones impactan fuertemente no solo los índices de frecuencia de incidentes, sino el ausentismo laboral, así como los costos directos e indirectos asociados.

En términos muy sencillos busca ayudar a las personas en utilizar Técnicas de Reducción de Errores críticos (TREC), para evitar lesiones por trauma acumulativo o trastornos musculoesqueléticos, que en un buen porcentaje, son causados por los estados de Prisa, Frustración, Fatiga y Complacencia.

Apoya a las personas a conocer la mecánica corporal, para así adoptar muy buenos hábitos de higiene postural, así como levantamiento manual de cargas, pausas activas, calentamiento previo a la tarea, la importancia del descanso, entre otros.

“Nuestro enfoque es amplio, aplica las técnicas no solo para el personal operativo, sino administrativo y lo más importante, reforzamos la importancia de adoptar buenos hábitos en el hogar también, porque este tipo de lesiones por trauma acumulativo, son el resultado de la suma de muchos factores tanto dentro como fuera del ambiente laboral”, destacó Gutiérrez.

Proporciona herramientas muy sencillas, para que las personas en primera instancia comprendan cómo funciona su cuerpo, posterior a ello, se les brinda técnicas muy claras y prácticas para adoptar las mejores posturas, sumado a hábitos relacionados con el descanso, las pausas durante la jornada, la importancia del fortalecimiento junto con el estiramiento.

Pero para ello, requerimos que las personas reconozcan que los estados (Prisa, Frustración, Fatiga y Complacencia) son peligrosos y hagan algo al respecto, porque muchas de las lesiones son causadas por tener dichos estados y no hacer nada para minimizar sus consecuencias o probabilidad de cometer errores. **XS**



CASCOS INTELIGENTES

mejoran seguridad de obras de tren

Beijing. - Las obras de construcción de ferrocarriles de alta velocidad de China comenzaron a utilizar cascos de seguridad inteligentes para mejorar la seguridad y la eficiencia, informó el Diario de Ciencia y Tecnología.

El casco inteligente, empleado en algunas obras en la provincia central de Hubei, fue desarrollado por el Grupo del Buró de Electrificación de Wuhan y está equipado con una cámara de alta definición, una antena de telecomunicaciones y un chip de control.

Además de proteger la cabeza, el casco sirve como terminal para distribuir la información por los recintos y se ha integrado en un sistema de gestión de seguridad basado en la tecnología del Internet de las cosas.

El casco también puede grabar videos sobre las labores de construcción y hacer sonar alarmas de seguridad. La información será recopilada por el sistema de gestión de seguridad y estará disponible en una aplicación de teléfonos móviles.

El aparato es útil en muchas situaciones, tales como la construcción de líneas eléctricas y proyectos de minería, y será actualizado en el futuro para las obras de construcción inteligentes, según el periódico. **XS**



KIMBERLY-CLARK

relanza su marca de seguridad industrial

España.- La multinacional Kimberly-Clark opera con dos negocios independientes: uno de consumo masivo, en el que vende sus productos a los consumidores finales por medio de los canales de retail, y otro institucional, en el que les vende directamente a las empresas. Esta unidad, conocida como Professional, en el país se surte con su planta de Barbosa, Antioquia. La empresa está relanzando su marca Kleen Guard, que abarca elementos de seguridad en el trabajo, como guantes, gafas o uniformes. Alejandro Guerrero, country manager de Kimberly-Clark Professional, dice que el mercado de productos de protección está muy atomizado. Ellos tienen 8% de participación y la meta es duplicar esa cifra en dos o tres años. Sus principales clientes son firmas mineras y petroleras. **XS**





ESTOS SON LOS 3 SECTORES

más riesgosos para el trabajo industrial

Las inversiones en seguridad no son un gasto, de eso depende que las empresas mantengan su seguridad en estos sectores riesgosos en el trabajo industrial.

En el país cada 75 segundos ocurre un accidente laboral y cada ocho horas un trabajador muere por un accidente en su empleo, de acuerdo con cifras de la Secretaría del Trabajo y Previsión Social (STPS).

Además, solamente 40% de las empresas que manejan maquinaria cumplen con las normas oficiales, por lo que aquellas que no lo hacen incrementan notablemente los riesgos de accidentes laborales.

En el mundo de la seguridad industrial son muchos los requisitos que deben cumplirse para evitar accidentes físicos, pero en los hechos todavía se registran en México un alto número de accidentes laborales, con decesos y un altísimo costo en la productividad de las industrias mexicanas.

Los sectores con más accidentes

En México los sectores industriales más peligrosos para trabajar son:

- La construcción
- Transformación-manufactura
- Transportes y comunicaciones

Existe un punto ciego en prácticamente todos los ramos descritos: las empresas no sellan el paso de cables y tuberías de manera adecuada lo que deriva en un alto número de accidentes laborales. Esto es porque en México no existe normatividad al respecto lo que ocasiona que la protección de

la infraestructura crítica sea realizada de manera improvisada; por ejemplo, con materiales sustitutos que no pueden garantizar la protección contra incendios, inundaciones, fauna nociva, explosiones, descargas electromagnéticas o incluso en acciones de sabotaje.

Protegen con “trapitos” áreas de alto riesgo

“Usualmente el paso de cables y tuberías se protege con espumas, trapos, gomas y otros materiales que pueden poner en riesgo las operaciones y la vida humana. El 84% de las empresas en México así protegen el paso de cables y tuberías”, explicó Alfonso Guarneros, director general en Roxtec, proveedor mundial de sellado modular para cables y tuberías flexibles.

Esto por supuesto no es lo más profesional ni lo idóneo, se incrementan los riesgos por ahorro en costos que no deben ser ya que las compañías dejan de invertir en algo tan valioso como su propia infraestructura y su activo de recursos humanos.

Conciencia y previsión, claves para abatir muertes por accidentes laborales

La conciencia de las empresas y sus administradores en el sentido de que es necesario proteger con los materiales adecuados las áreas de alto riesgo de sus empresas, así como la previsión constante, son factores que ayudan a disminuir los accidentes y los costos para las compañías.

“Es necesario difundir la seguridad industrial física en México, en particular la importancia que tienen el sellado de pasamuros, cortafuego del paso de cables y tuberías”, dijo Guarneros. **XS**

**“TECNOLOGÍAS NO LETALES,
TECNOLOGÍAS MENOS LESIVAS”**



**PISTOLA NO LETAL
MODELO TIGGER**



**PISTOLAS
ELÉCTRICAS NO
LETALES**



**ESCUDO
ELÉCTRICO**



**Soluciones
para el Sistema
Penitenciario**

Correo: ventas@aprinosa.net

Tel: (52) 333 6412350

Tel: (52) 333 6415684

Whatsapp: (52) 333 7007721

EMPRESA 100% MEXICANA

www.aprinosa.net

MOCHILAS ANTIBALAS

lo más comprados en el regreso a clases de EU



Antes de empezar su primer año en la Universidad de Connecticut, J. T. Lewis recibió un regalo poco común de su madre: una mochila a prueba de balas.

Lewis, quien está por empezar el segundo año de la carrera, proviene de una familia destrozada por la violencia relacionada con las armas: su hermano menor, Jesse, fue asesinado en un tiroteo ocurrido en 2012 en la primaria Sandy Hook en Newtown, Connecticut. Cuando su madre, Scarlett, le dio la mochila color gris oscuro, se la entregó sin tener que decir una palabra, mencionó Lewis.

“Simplemente había un entendimiento mutuo”, recordó Lewis, de 19 años y quien también es candidato al Senado estatal de Connecticut.

Lewis usa la mochila blindada en el campus porque lo hace sentir más seguro, aunque signifique sudar un poco más por llevar esa carga pesada.

“No sé si tendrá algún efecto”, comentó Lewis. “Pero podría tenerlo si me disparan por la espalda”.

A medida que los tiroteos masivos se vuelven un hecho trágico de la vida en Estados Unidos —en las escuelas, las tiendas, los cines y los templos—, las familias de las víctimas no son las únicas que están invirtiendo en equipo para protección.

En un acontecimiento distópico, una cantidad cada vez mayor de empresas está vendiendo mochilas a prueba de balas en las ofertas de regreso a clases; las cuales promueven para los padres que están desesperados por proteger a sus hijos de los tiradores.

“Es muy deprimente”, opinó Igor Volsky, el director de Guns Down America, una agrupación que defiende

el control de las armas. “El mercado intenta resolver un problema que nuestros políticos se han negado a solucionar”.

La demanda de las mochilas a prueba de balas aumentó después del tiroteo en un bachillerato de Parkland, Florida, ocurrido en febrero de 2018. Ahora que la temporada de regreso a clases está a la vuelta de la esquina, los tiroteos recientes en El Paso, Texas, y en Dayton, Ohio, han generado una atención renovada en estos productos.

Hay reportes de que en otras ocasiones las mochilas se han agotado en tiendas, con precios que suelen estar entre 100 y 200 dólares. Meses antes del tiroteo en Parkland, una escuela privada cristiana de Miami también vendía paneles protectores para insertar en las mochilas como escudos antibalas, por 120 dólares.

Este año, ArmorMe, una empresa de defensa personal dirigida por Gabi Siboni, quien fuera soldado en Israel, comenzó a vender una mochila a prueba de balas que se podía desdoblar para convertirse en una protección más grande.

“Primero que nada, la mochila está diseñada con un estilo muy moderno y atractivo”, dijo Siboni. “Además, tiene paneles que te protegen de las balas. Aumentará tus posibilidades de supervivencia”.



ACCESO GRATIS AL PISO DE EXPOSICIÓN CON PRE-REGISTRO



EXPO FIRE PROTECTION MÉXICO 2019 & INTERNATIONAL CONGRESS

1 Y 2 DE OCT. WTC, CDMX

Organizan:

AMRACI
Asociación Mexicana de Registros de Protección contra Incendios A.C.

CONAPCI
Comisión Nacional de Protección contra Incendios

SUPRESIÓN / DETECCIÓN Y ALARMA / PROTECCIÓN PASIVA / SEGURIDAD HUMANA



5ª Campaña Nacional
de Protección
Contra Incendios

EXPOSICIÓN Y CONGRESO
ESPECIALIZADOS EN SOLUCIONES PARA
LA PROTECCIÓN CONTRA INCENDIO
Participan Congresistas Nacionales e Internacionales

**COSTO DE ENTRADA AL
CONGRESO INTERNACIONAL**

PRECIO PREFERENCIAL
Antes del 20 de Septiembre

CÓDIGO EFPI
\$1,800.00

Los costos ya incluyen IVA



Contra
Incendio

XTREM SECURE

MIS

SEGURIDAD



EQUIPAR

ESPECIFICAR

INM•BILIARE

REVISIA
CONSULTORIA

01(55) 7098-5809 / 7098-6818

contacto@fpimexico.com

www.fpimexico.com

Otra empresa, Guard Dog Security, comenzó a vender mochilas a prueba de balas poco después del tiroteo en Sandy Hook. Los productos están disponibles en Office Max, Office Depot y Kmart, y la firma hace poco lanzó un modelo que cuesta menos de 100 dólares.

“Podría ser la diferencia entre la vida y la muerte”, señaló Yasir Sheikh, el director de Guard Dog.

En el pasado, algunas empresas fueron criticadas por haber afirmado en falso que sus mochilas blindadas estaban certificadas por el Instituto Nacional de Justicia, organismo que supervisa la calidad de los chalecos antibalas que usan las fuerzas del orden. La agencia, una rama del Departamento de Justicia, no ha certificado —ni siquiera probado— las mochilas a prueba de balas y no tiene planes de hacerlo, aseguró Mollie Timmons, una vocera del departamento.

No obstante, según Sheikh, la mochila de Guard Dog está diseñada para cumplir con la norma Nivel IIIA de rendimiento para chalecos antibalas de la agencia, por lo tanto, resistiría balas de escopetas y pistolas de mano. Las mochilas son probadas en una instalación en Oregon, mencionó Sheikh.

Sin embargo, Sheikh reconoció que las mochilas eran menos efectivas para bloquear disparos de armas semiautomáticas poderosas, como las que se usaron en Sandy Hook. Además, los defensores del control de las armas aseguran que no hay ninguna evidencia de que las mochilas blindadas sean seguras para los niños durante un tiroteo, sin importar el cuidado con el cual las hayan probado.

“Les estamos pidiendo a los niños que hagan frente a hombres armados porque los legisladores tienen demasiado miedo de hacerle frente al grupo cabildero a favor de las armas”, denunció Shannon Watts, la fundadora de Moms Demand Action for Gun Sense in America (Madres estadounidenses que

exigen acciones sensatas sobre las armas), una organización comunitaria a favor del control de las armas. “No hay un solo padre en este país que no esté aterrorizado. Estas empresas están capitalizando ese sentimiento”.

Siboni, quien dirige ArmorMe, dijo que era injusto acusar a su empresa de explotar los temores sobre la violencia que producen las armas a nivel nacional para obtener una ganancia.

“Lo que sea que hagas estarás capitalizando algo”, opinó. “Solo respondemos a una necesidad”.

Kamala Harris, senadora de California y precandidata demócrata a la presidencia, ha puesto de ejemplo a las mochilas a prueba de balas como un símbolo del problema más grande de la violencia relacionada con las armas en Estados Unidos.

“No debería ser necesario que los padres compren una mochila a prueba de balas para que sus hijos estén seguros en la escuela”, tuiteó en julio. “Esto no debería ser normal”.

Para Celeste Green, una estudiante de 22 años que cursa el último año en la universidad College of Charleston en Carolina del Sur, las mochilas son una precaución necesaria.

El 2 de agosto, un día antes del tiroteo en El Paso, Green supo que un adolescente de su ciudad natal, Columbia, Carolina del Sur, había amenazado con “acribillar” una escuela local. Cuando vio las noticias, pensó en su hermana menor, quien empezará el bachillerato en otoño. Green le envió a su madre videos y enlaces a sitios web con información sobre las mochilas a prueba de balas.

“De inmediato me preguntó: ‘¿Dónde debería buscarlas?’”, dijo Green. “No hubo la menor duda de que debía conseguir una”. **XS**





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



SEGURIDAD



PREVENCIÓN



CONFIANZA

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

Telefónos:

5207 6828 / 3603 3189

www.seguridad-privada.com.mx

BOSCH LLEVA LA SEGURIDAD INDUSTRIAL A UN NUEVO NIVEL

Bosch, una empresa de amplia tradición en el mercado, que se distingue por su gran calidad y sus soluciones de vanguardia, impulsa la seguridad industrial con soluciones que van mucho más allá de los tradicionales sistemas de alarma, videovigilancia y control de acceso.



Bosch desarrolla tecnología para la vida porque entiende que la evolución tecnológica debe traer consigo un impacto positivo para la gente. La seguridad industrial es un ejemplo de cómo esta transformación puede mejorar los productos y servicios aplicados para garantizar la integridad de los colaboradores de toda empresa y optimizar sus procesos.

Tecnologías que conectan seguridad y protección industrial

Como líder global en la provisión de seguridad, el trabajo de Bosch está guiado por las necesidades de sus clientes, con la idea siempre en mente de ofrecer perfección. Esta experiencia permite que ayude a sus clientes empezando por determinar y comprender sus necesidades. Más que aportar soluciones inteligentes, Bosch busca ser el socio ideal.

El objetivo de la compañía es la satisfacción de sus clientes, para ello ha optimizado sus soluciones de seguridad industrial de forma personalizada. Los sistemas de video, por ejemplo, van más allá de la generación de imágenes; cuando se integran al análisis de video y software de gestión en almacenes pueden hacer mucho más que monitorear y generar alertas.

Es posible utilizar estas soluciones para el seguimiento de envíos urgentes o prioritarios, el inventario virtual en tiempo real y la implementación de áreas de seguridad que funcionan como divisiones invisibles. Este es un ejemplo de una aplicación en un ambiente complejo: una solución inteligente Industry 4.0.

La compañía cuenta también con cámaras para ambientes oscuros y con visión limitada, capaces de detectar llamas y humo. Su tecnología identifica con rapidez el foco del incendio y evita los percances durante el proceso. Esta solución forma parte de los sistemas de detección de incendios y se utiliza en

ambientes con partículas en suspensión o techo alto, evitando incidentes. Y, si es necesario, su sistema de sonido y alarma por voz reproduce mensajes personalizados para una evacuación tranquila.


Las posibilidades no paran ahí. Las soluciones pueden recibir configuraciones de varias reglas y, cuando alguna de ellas no se cumple, se envía una alerta al operador del sistema de seguridad. Una aplicación práctica está en la seguridad perimetral con la identificación de objetos abandonados o retirados.

Y aún en entornos restringidos, donde la entrada es controlada, se puede utilizar la doble verificación y, además, sensores de intrusión con tecnología capaz de identificar cuando el equipo ha sido cubierto o violado.

Lo que distingue a Bosch

Bosch combina la tradición alemana y la calidad latina para innovar y ofrecer seguridad y protección en las condiciones más exigentes. Su experiencia de más de 133 años y una amplia cartera de clientes le permite ofrecer diferenciales únicos, como por ejemplo la precisión de los análisis y el bajo nivel de falsas alarmas.

Independientemente del giro de una empresa o de la complejidad que demande, esta compañía está en capacidad de satisfacer las especificaciones de seguridad que esta requiera, con eficiencia superior. Para Bosch es un gran orgullo su capacidad de desarrollo, de adaptación, personalización e integración de soluciones.

Hacer un monitoreo más eficiente contribuye a la prevención de incidentes y permite una respuesta rápida a las potenciales situaciones de riesgo. 

CIBERSEGURIDADMX



REVISTA DIGITAL
ESPECIALIZADA EN CIBERSEGURIDAD

www.ciberseguridadmx.com

La **SEGURIDAD** **INFORMÁTICA:**

— un tema de todas las
áreas



WatchGuard Technologies, líder mundial en seguridad e inteligencia de red, Wi-Fi seguro y autenticación multifactor, tuvo una destacada presencia en ISEC Infosecurity Tour 2019, realizado en Buenos Aires.

El evento reunió a las principales empresas de seguridad informática para mostrar las últimas tendencias aplicadas a diversos mercados.

WatchGuard, que participó junto a dos canales, NetGuard y Codic, abordó en su conferencia los motivos por los cuales la seguridad debe ser un tema que compete a todas las áreas de la empresa.

Al respecto, Leonardo Cesario, Sales Engineer Brazil de la compañía de seguridad informática, detalló los problemas de seguridad en las empresas y cómo las soluciones de administración centralizada pueden facilitar la implementación y gestión de los procesos.

“En el caso de las PYMES, por ejemplo, hay que ver las mixturas de los procesos que tienen, junto con las soluciones de seguridad que están implementando.



Las empresas pequeñas se enfrentan a un conjunto único de desafíos de seguridad informática debido a las limitaciones de recursos. Aun así, representan más de la mitad de las incursiones de seguridad que se observan cada año”.

En relación a los aspectos a tener en cuenta a la hora de implementar medidas de seguridad informática en las empresas, el ejecutivo comentó que “siempre hay que tener un firewall para proteger la infraestructura física, pero también se deben proteger los procesos que la compañía tiene para ofrecer servicios a los usuarios”, comentó Cesario.

Según el vocero, si la firma trabaja con sistemas remotos hay que poner una fuerte autenticación, con sistema de multi factor. “Recomendamos mecanismos como la autenticación vía ‘push’”, ejemplificó el vocero. Y agregó que, sin dudas, para las empresas, el mecanismo de ataques de mayor riesgo es el phishing.

En su reciente informe de Seguridad en Internet de Q1 2019, la compañía destaca la necesidad cada vez más importante de un enfoque de seguridad en capas, debido al avanzado panorama de amenazas de hoy.


“Los delincuentes cibernéticos están aprovechando diversos métodos de ataque, razón por la cual es necesario implementar una plataforma que ofrezca una gama completa de servicios de seguridad”, aconseja Cesario.

“También, las redes inalámbricas presentan un punto de fallas muy grande en varias compañías. Por eso es muy importante securizar la parte de red”, dijo.

Cesario comentó que el WiFi puede ser un punto de acceso para tomar una contraseña de un administrador y realizar un ataque, por lo que hay que proteger esta parte de la compañía.

En el evento, la firma presentó la solución AuthPoint, ideal para todo tipo de empresas, que ofrece autenticación multifactorial (MFA). Gracias a esto, según destacan desde la marca, cuando haya un intento de inicio de sesión externo la app crea una notificación de inserción segura en el teléfono inteligente del usuario, mostrando quién intenta autenticarse y desde dónde. Luego, se genera un mensaje que forma parte de su propio proceso de inicio de sesión, donde el usuario acepta y obtiene acceso rápido a los recursos de red y las aplicaciones en la nube que se hayan autorizado.

La firma ofrece una solución integral a través de una plataforma unificada de seguridad, la cual comprende tres productos: Total Security, Cloud-Managed Wi-Fi seguro y Authpoint.

Además tiene Firewalls Virtuales y Cloud, administración de Cloud, Wireless Intrusion Prevention (WIPS) y más. 



SECURITY WEEK

LATAM ASIS 2019

13 AL 17 DE OCTUBRE
CENTRO CITIBANAMEX

**¡APARTA
TU
LUGAR!**

FASE 2

SOCIOS	\$9,042.00
NO SOCIOS	\$10,270.00 +IVA
SOCIOS OTROS CAPÍTULOS Y OTRAS ASOCIACIONES	\$9,042.00 +IVA

*SHOOTING CHALLENGE | WEBINARS | ASIS TALKS | ASIS SIMS
ASIS LABS | CSO SUMMIT | ESCUELAS SEGURAS
COCKTAIL | WELCOME KIT | CONSTANCIA DE ASISTENCIA
DESAYUNO INAUGURAL | COMIDAS DE NETWORKING
ZONA DE EXPO

*Evento no incluido en el costo del Congreso

• TRANSFORMANDO LÍDERES •



FIRSTCALL



REGISTRATE HOY A SECURITYWEEK@ASIS.ORG.MX | SECURITYWEEKLATAM.COM



MÉXICO

es el país más afectado por ciberataques a nivel mundial

Sophos, firma especializada en ciberseguridad, dio a conocer los resultados de su encuesta global "The Impossible Puzzle of Cybersecurity", y reveló que México es el país más afectado por ataques cibernéticos con un 82 por ciento, mientras que Japón es el menos impactado con un 24 por ciento.

De acuerdo con la encuesta, más del 55 por ciento de las empresas mexicanas fueron víctimas de los ciberdelincuentes en 2018. Los ciberataques más representativos a nivel mundial y en México sucedieron principalmente a través de phishing propagado en correos electrónicos y por sitios web maliciosos. También destacó que las memorias USB y dispositivos externos son la fuente de uno de cada cuatro asaltos en el país.

Las industrias que presentaron más ciberataques en el último año a nivel mundial fueron de tecnologías de la información (TI), tecnología y telecomunicaciones (15.9 por ciento); empresas de retail, distribución y transporte (13 por ciento); manufactura y producción (13.7 por ciento); y servicios financieros (11.6 por ciento).

Sophos señaló que los gerentes de TI de cada organización están saturados de irrupciones provenientes de todas direcciones y luchan por mantenerse al día debido a la falta de experiencia en seguridad, presupuesto y tecnologías actualizadas. En México, más del 27 por ciento de los administradores no conoce cómo, ni cuánto tiempo estuvo presente el ataque en el entorno de su organización.

Además, el 95 por ciento de los encuestados en México declararon que desearían contar con equipos más fuertes para detectar, investigar y responder adecuadamente a los incidentes de seguridad. Así mismo, el 30 por ciento afirmaron que pierden más de una cuarta parte de su tiempo para administrar la seguridad de su organización.

Según el 75 por ciento de los administradores de TI, los software maliciosos, las vulnerabilidades sin parches y las amenazas de día cero son los principales riesgos de seguridad a los que se enfrentan los negocios en México. Sin embargo, solo un 10 por ciento consideran la cadena de suministro como una amenaza, exponiéndolo como un punto débil adicional para que los ciberdelincuentes puedan agregarlo a su repertorio de vectores de ataque.

"Constantemente los ciberdelincuentes evolucionan sus métodos para entrar en una organización, ante esto los administradores de TI deberán priorizar la cadena de suministro como un riesgo de seguridad. Estos ataques también son una manera eficaz para que los ciberdelincuentes lleven a cabo robos automatizados y activos, donde seleccionan a una víctima de un grupo más grande de prospectos y luego hackean activamente a esa organización específica usando técnicas manuales y movimientos laterales para evadir la detección y llegar a su destino", comentó Chet Wisniewski, científico investigador en Sophos.

La encuesta fue realizada por Sophos, junto con la agencia Vanson Bourne, compañía especializada en estudios de mercado, entre diciembre de 2018 y enero de 2019. Se entrevistó a 3,100 tomadores de decisiones de TI en doce países y seis continentes que incluyen Estados Unidos, Canadá, México, Colombia, Brasil, Reino Unido, Francia, Alemania, Australia, Japón, India y Sudáfrica. **XS**

"Todas las empresas mexicanas, el gobierno e incluso la sociedad, deben reconocer la importancia de la ciberseguridad como un derecho y una responsabilidad. Con la información de la encuesta se podrá tener una mayor visibilidad que permita prevenir, resolver y detectar problemas de manera más eficaz y oportuna, y así evitar ser víctimas de ciberataques", dijo Alejandra García, Country Manager de Sophos en México.



NASA sufrió brecha de seguridad y robaron información sobre la misión a Marte

Por Tomáš Foltýn

La Administración Nacional de Aeronáutica y el Espacio, más conocida como NASA (por sus siglas en inglés), sufrió recientemente un incidente de seguridad en el que un atacante robó información sensible de la agencia relacionada a la misión a Marte, incluyendo detalles sobre el Curiosity rover.

La brecha, que afectó al Laboratorio de Propulsión a Reacción de la NASA (JPL, por sus siglas en inglés), permaneció sin ser detectada por 10 meses, detalla un reporte publicado por la Oficina del Inspector General de la NASA (OIG, por sus siglas en inglés).

“En abril de 2018, JPL descubrió que una cuenta perteneciente a un usuario externo había sido comprometida y utilizada para robar aproximadamente 500 MB de datos de uno de sus principales sistemas de misión,” explica el reporte, en el cual se atribuye la intrusión a un grupo de Amenaza Persistente Avanzada, más conocida como APT (por sus siglas en inglés).

Resulta que los cibercriminales explotaron un dispositivo Raspberry Pi, el cual estaba conectado a la red JPL sin autorización, y lo utilizaron como

trampolín para infiltrarse dentro de la red y moverse lateralmente.

No se especifica quien estuvo detrás de la intrusión, o más específicamente, quién conectó a la red este dispositivo, de una sola placa, que se puede comprar por aproximadamente 25 dólares.

Sin embargo, lo que sí está claro es que a la Oficina del Inspector General no le llamó la atención la postura en ciberseguridad que tomó la agencia espacial.

Problemas de seguridad de fondo

“Durante los últimos 10 años, el JPL experimentó varios e importantes incidentes de ciberseguridad que comprometieron grandes segmentos de sus redes TI”, afirma el reporte.

Además, no se detiene en este dato, sino enumera una serie de deficiencias en los controles de seguridad de la red de la NASA que ponen en riesgo sus sistemas de datos. *“Múltiples debilidades de los controles de seguridad de TI reducen la habilidad del JPL para prevenir, detectar y mitigar ataques dirigidos a sus sistemas y redes, exponiendo los sistemas y datos de la NASA a la explotación por parte de*

un atacante”, añade el informe.

Esto mismo quedó en evidencia en el incidente de Raspberry Pi, el cual fue habilitado en parte debido a su “visibilidad reducida en los dispositivos conectados a sus redes (de la NASA)”. Esto significa que nuevos dispositivos añadidos a la red no siempre fueron puestos a un proceso de evaluación crítica por un especialista en seguridad y que la agencia no sabía que el gadget (Raspberry Pi) estaba presente en la red.

Adicionalmente, la auditoría detectó una falta de segmentación de la red, algo que cual explotaron los atacantes para moverse lateralmente entre varios sistemas conectados a una puerta de enlace de red. La puerta de enlace ofrece a usuarios externos y a sus socios, incluyendo agencias espaciales extranjeras, así como contratistas e instituciones educativas, acceso remoto a un entorno compartido.

Además, la auditoría encontró que los registros de los tickets de seguridad, entre los cuales figuran solicitudes para la instalación de parches a un software o actualizar un sistema de configuración, en algunos casos permanecieron sin resolverse durante más de seis meses.



Esto a pesar de que los administradores de sistemas tenían un plazo máximo de 30 días para llevar adelante las medidas correctivas.

Esta clase de retrasos colaboró con que se pueda llevar adelante la intrusión de la Raspberry Pi, ya que “uno de los cuatro sistemas comprometidos no parcheó una vulnerabilidad en el tiempo que correspondía”.

También se vieron afectados sistemas vinculados con la Red del Espacio Profundo de la NASA (DSN, por sus siglas en inglés). Esto finalmente provocó que los equipos de seguridad del Centro Espacial Johnson, que administra la Estación Espacial Internacional, se desconectaran de la puerta de enlace por temor de que los “atacantes puedan moverse lateralmente desde la puerta de entrada a sus sistemas de misión, teniendo así la posibilidad de obtener acceso e iniciar acciones maliciosas que afecten a vuelos de misiones espaciales humanas que utilicen esos sistemas”.

El reporte también detectó que el JPL no implementó un programa de búsqueda de amenazas para “perseguir de manera agresiva actividad anormal en sus sistemas e indicadores de algún tipo de compromiso”, confiando en cambio en “un proceso ad hoc para la búsqueda de intrusos”.

El reporte destacó 10 recomendaciones y la NASA aceptó que todos, excepto uno, pusieran en marcha un proceso formal de búsqueda de amenazas.

Atacante accede remotamente a tu computadora a través de un **CABLE LIGHTNING**

En la edición 2019 de Def Con, la popular conferencia de seguridad que se celebra todos los años en Las Vegas, Estados Unidos, el investigador en seguridad conocido bajo el seudónimo MG, demostró que, adulterando un cable lightning de Apple con la instalación de un implante, un atacante puede tomar control de la computadora de una hipotética víctima de manera remota.

Se trata de un cable, apodado por el investigador como O.MG Cable, que con solo conectarlo a una computadora a través del USB y sin necesidad de conectar otro dispositivo como el teléfono en el otro extremo, permite al atacante ingresar de manera remota a la computadora y ejecutar una gran variedad de herramientas en el equipo comprometido, explica un artículo publicado en Vice.

El atacante abre cualquier navegador en su teléfono y coloca la dirección IP para ese cable. Ahí se despliega una lista de opciones, ya que con el cable vienen múltiples herramientas que permiten realizar distintas acciones en la computadora comprometida. “El cable viene con varios payloads, scripts y comandos que un atacante puede ejecutar en la computadora de la víctima. Un atacante incluso puede “matar” el implante USB en un intento de esconder cualquier evidencia de su utilización o existencia”, explica el artículo.

En relación a la distancia que debe estar un atacante para poder acceder a la computadora comprometida, MG explicó

que, por ejemplo, con un teléfono a una distancia de 90-100 metros es posible interactuar con el dispositivo afectado por el cable, aunque si fuese necesario se puede agregar una antena para ampliar el rango de distancia. Igualmente, también existe la posibilidad de configurar para que se conecte a una red Wi-Fi cercana y conectado a través de Internet el atacante podría controlar la computadora de la víctima prácticamente desde cualquier lugar.

El objetivo del investigador, que está comercializando el cable por USD200, es que pueda ser utilizado como una herramienta de seguridad legítima por equipos Red Team. **XS**



Empleados pueden comprometer la **SEGURIDAD DE LA EMPRESA**



"Se han presentado casos donde personal de confianza o ejecutivos de alta dirección y gerencia con acceso a información valiosa y sin mecanismos de control ni supervisión han estado involucrados en fraudes o ataques cibernéticos. Aquellos empleados que han sido despedidos y están enojados también representan una gran amenaza, ya que al conocer la operación del negocio y áreas sensibles, pueden aprovechar estos vacíos que los motiven a cometer algún daño", indicó el experto.

A pesar de las inversiones millonarias que se realizan para la protección de los activos valiosos de una organización, NETSCOUT SYSTEMS, INC., (NASDAQ: NTCT), proveedor líder de garantía de servicios, seguridad y análisis de negocios, informó que cada vez más crece el número de empresas que están enfrentando filtraciones de seguridad digital causadas por los mismos empleados.

Eliás Germán, experto en Ciberseguridad de NETSCOUT, dijo que es de vital importancia la supervisión del personal interno de la compañía ya que un comportamiento irresponsable, insatisfecho, descuidado o maligno, puede ser perjudicial para la organización. Las soluciones de seguridad tradicionales actuales no son capaces de impedir que un empleado provoque un robo o pérdida de datos confidenciales que luego podrían ser vendidos en el mercado negro.

A diario una gran cantidad de datos críticos se encuentra al alcance de los empleados, y sin los adecuados controles y privilegios, las empresas están más expuestas y vulnerables a sufrir algún acto delictivo. Hoy la amenaza es mayor, ya que se accede a la información a través de cualquier equipo de cómputo o dispositivo móvil, que puede o no ser propiedad de la empresa y por tanto en muchos casos no cumple con las políticas de seguridad implementadas para dispositivos internos, además de contar con la capacidad de acceder a recursos corporativos desde cualquier lugar y hora.


Una de las principales amenazas a la seguridad ocasionadas desde el interior de una compañía es causada por empleados disgustados sobre todo en áreas técnicas, que por la naturaleza de su trabajo tienen acceso a información confidencial, por ejemplo, un administrador de base de datos con acceso a datos personales de todos los empleados y clientes, o un administrador de Hypervisor que sabe exactamente como puede provocar un daño mayor a la infraestructura virtual de la empresa.

Otra situación de las más comunes, indicó Eliás Germán, es la falta de conocimiento acerca de los diferentes métodos utilizados para comprometer recursos de cómputo corporativo como laptops y smartphones. A menudo los usuarios de áreas no técnicas son más susceptibles a caer en campañas de phishing u otro tipo de actividad maliciosa que rápidamente otorga el control de sus dispositivos a un atacante remoto, convirtiéndose, aún de forma inconsciente, en el medio por el cual se produce la explotación desde el mismo recurso interno.

Eliás Germán mencionó tres prácticas frecuentes que en el ámbito laboral ponen en constante peligro a una organización:

- 1) Almacenamiento local de passwords en laptop/smartphone en archivo de texto. Si lo llegan a comprometer, un atacante podría obtener las credenciales de acceso a sistemas de misión crítica. Lo mismo aplica para almacenamiento local de información confidencial como "copia de seguridad".
- 2) Compartir información sensible por medios no seguros (correo, WhatsApp, etcétera).
- 3) Uso de sistemas corporativos desde redes no seguras (hoteles, aeropuertos, cafés, entre otros), sobre todo si la comunicación no es cifrada.

Eliás Germán opinó que la mayoría de las empresas pequeñas y medianas no cuentan con una política formal de seguridad, y si la tienen, en muchos casos no poseen las herramientas necesarias para implementarla de manera efectiva.

Ante dicha situación, el especialista destacó la importancia de contar con un modelo de seguridad que permita identificar de forma temprana los riesgos y amenazas para reducir de forma efectiva el impacto en la infraestructura y la reputación del negocio. 



Amenazas reales en un **MUNDO VIRTUAL**



El pasado 17 de julio se realizó, en el Centro Citibanamex de la Ciudad de México, el tradicional desayuno mensual de ALAS.

En esta ocasión el evento fue patrocinado por la empresa HID. Armando Cárdenas, gerente regional de ventas, aseguró que “ahora tenemos diferentes identidades. No somos simplemente personas, ya somos identidades a nivel digital y a nivel físico. La compañía HID está enfocada en conjuntar el hardware y el software para crear identidades seguras para la gente. Somos una empresa con casi 30 años en el mercado y estamos presentes en

más de 70 países. Nos identifican básicamente por las tarjetas y los paneles de control de acceso”.

En el evento también se llevó a cabo el taller “Amenazas reales en un mundo virtual: Cómo enfrentarlas y mitigarlas” impartido por el Ing. David Pereira, CEO de Secpro Security Professionals, especialista en diseño de estrategias de ciberseguridad, ciberdefensa y computación forense.

En tiempos de ataques virtuales cada vez más sofisticados y frecuentes, todos necesitan aprender a protegerse. Conocer las amenazas más comunes es el primer paso para reforzar la seguridad contra invasores y criminales cibernéticos.

Una infraestructura de seguridad debe estar preparada para incluir las tecnologías, procesos y usuarios involucrados, además de ofrecer protección de red, control y gestión de tecnología sin comprometer el desempeño del sistema o la productividad de los usuarios.

El ideal en el combate a los ciberataques consiste en combinar tecnologías con la responsabilidad de las personas, educando y concientizándonos sobre las situaciones de peligro existentes. **XS**



ÍNDICE DE ANUNCIANTES



MULTIPROSEG

2da. Forros / Pág. 3

RANGER SWAT MÉXICO

Pág. 88 -3ra. de Forros

GECSA

Pág. 7

LK SEGURIDAD PRIVADA

Pág. 11

IPS

Pág.15

CSCS

Pág. 19

MOSEG

Pág. 21

UNIFORMES JR

Pág. 23

SERRALDE

Pág. 25

ZN CORPORATIVO

Pág. 29

AXIS

Pág. 35

ALAS

Pág. 39

TI LATINA

Pág. 43

IP USERGROUP

Pág. 49

SIMPOSIUM ANTAD

Pág. 51

PROYECTOS TI

Pág. 53

ASUME

Pág. 55

COMEXA

Pág. 57

APRINSA

Pág. 73

EXPO FIRE PROTECTION

Pág. 75

ORIGINS

Pág. 77

ASIS

Pág. 81

SEPSISA

Contraportada



RANGER SWAT MÉXICO



Servicio de transporte a Ejecutivos



Servicio de Custodias



Servicio de GPS y Rastreo Satelital



Servicio de Escoltas



Servicio de Intramuros



Detecto, Visualizo y Actúo

52 (55) 5347 2741

contacto@rangerswat.com.mx



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



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