SEGURIDAD EN AMÉRICA

M36

Año 23 / No.134
Septiembre-Octubre

www.seguridadenamerica.com.mx

Especial:
Seguridad en *Data Centers* y TI

Reportaje: Seguridad privada en la industria automotriz

SEGURIDAD EN AMÉRICA

CUMBRE DE SEGURIDAD CORPORATIVA

13 CONFERENCIAS MAGISTRALES
Con la participación de 29 profesionales en seguridad

Iliana Fernández, **Microsoft**

Brian Cooke, **Marathon**

Eduardo Téllez **Laboratorios Liomont**

L. Eugenio Latapi **Ethics Data Analytics**

Lourdes Morales, **Walmart**

Luis Fernando Rojas, **Walmart**

Dagoberto Santiago, **PepsiCo**

Enrique Sansores, **PepsiCo**

Adolfo Márquez, **Hoteles City Express**

Alberto Granados, **Hoteles City Express**

Maribel Cervantes, **HSBC**

Javier Hernández, **BANORTE**

José Manuel Díaz-Caneja, **BBVA**

Luis Meza, **Citibanamex**

Ciro Ortiz Estrada, **SEPROBAN**

Antonio Gaona, **CODERE**

Fernando Gómez, **Grupo Gentera**

Fernando Polanco, **CIE**

Carlos Seoane, **Seoane**

Ricardo Aníbal, **ONU**

Adolfo Quintana, **ONU**

Héctor Coronado, **Kavak**

Guillermo Hassey, **Daimler Truck**

José Luis Sánchez, **OXXO**

Oziel Ortiz González, **7-Eleven**

Gerardo de Lago, **Timur | Galeam**

José Aguilar, **DHL**

Luis Constantino, **Universidad Iberoamericana**

Eduardo Jiménez, **FedEx**

30 – 31 de agosto 2022

En seguridad no hay competencia, porque unidos somos más fuertes.

Centro Citibanamex CDMX

evento presencial

SEGURIDAD EN AMÉRICA

Es una publicación con 23 años de presencia en el mercado. Nuestra misión es informar a la industria de seguridad, tecnología de la información (TI) y seguridad privada, así como al sector de la seguridad pública. Distribuidos 40 mil ejemplares bimestrales en más de 15 países de Latinoamérica.

Año 23 / No. 134 / septiembre-octubre / 2022

Portada:
Monitoreo 360

Síguenos por

Seguridad-En-América
@Seguridad_En_Am
@seguridad_en_america
SeguridadEnAmerica
revista-seguridad-en-america
@seguridad_en_america
www.seguridadenamerica.com.mx

Apoyando a:

Socio de:

CÁMARA NACIONAL DE LA INDUSTRIA EDITORIAL MEXICANA
CANIEM

COMPARTE ESTA REVISTA
COMPARTIR ES RECICLAR

Conmutador: 5572.6005
www.seguridadenamerica.com.mx

Seguridad en América es una publicación editada bimestralmente por Editorial Seguridad en América S.A. de C.V., marca protegida por el Instituto de Derechos de Autor como consta en la Reserva de Derechos al Uso exclusivo del título número: 04-2005-040516315700- 102, así como en el Certificado de Licitud de Contenido número: 7833 y en el Certificado de Licitud de Título número: 11212 de la Secretaría de Gobernación. Editor responsable: Samuel Ortiz Coleman. Esta revista considera sus fuentes como confiables y verifica los datos que aparecen en su contenido en la medida de lo posible; sin embargo, puede haber errores o variantes en la exactitud de los mismos, por lo que los lectores utilizan esta información bajo su propia responsabilidad. Los colaboradores son responsables de sus ideas y opiniones expresadas, las cuales no reflejan necesariamente la posición oficial de esta casa editorial. Los espacios publicitarios constantes en esta revista son responsabilidad única y exclusiva de los anunciantes que oferten sus servicios o productos, razón por la cual, los editores, casa editorial, empleados, colaboradores o asesores de esta publicación periódica no asumen responsabilidad alguna al respecto. Porte pagado y autorizado por SEPOMEX con número de registro No. PP 15-5043 como publicación periódica. La presentación y disposición de **Seguridad en América** son propiedad autoral de Samuel Ortiz Coleman.

De esta edición fueron impresos 12,000 ejemplares. European Article Number EAN-13: 9771665658004.

Hecho en México. Se imprimió en los talleres de Esténtor Impresos, Calle Virgen de Chiquinquira 706, Col. La Virgen, Ixtapaluca, Estado de México, C.P. 56530.

EDITORIAL

Las cifras oficiales arrojan alrededor de 30 mil muertes al año en México, esto como resultado de la violencia, de acuerdo con El País. La inseguridad que los últimos meses ha vivido la población, con negocios y transporte público y privado incendiados en varias entidades como Baja California, Guanajuato, Michoacán, Jalisco y Chihuahua, motines carcelarios y balazos que dejaron 11 muertos en Ciudad Juárez, sí es algo que preocupa en un país anestesiado en torno a una idea: la violencia es entre delincuentes.

Las autoridades pronto se pusieron manos a la obra y comunicaron detenciones en esos territorios. Hasta 17 en Tijuana, Mexicali, Ensenada y Playa de Rosarito, entre otros. Se puso en marcha otra operación conjunta entre las fuerzas armadas de todos los niveles en Michoacán con un saldo de 164 detenidos y decenas de armas incautadas. El asunto está todavía con más preguntas que respuestas.

La seguridad de la población parece ser ahora la inquietud del Gobierno, que anunció que la Guardia Nacional pasará a estar bajo la dirección completa de la Secretaría de Defensa Nacional (Sedena), lo cual plantea cuestiones como la militarización de la vida pública, los beneficios o desventajas que eso pueda tener en el combate de la violencia, que los militares no están libres de pecado y eventualmente los abusos de poder.

Las elecciones presidenciales de 2024 están cerca y AMLO sostiene que esa fecha será el principio de su jubilación política, no sin antes haber demostrado que tanto él como su equipo de Gobierno "son diferentes".

Hasta ahora, el discurso ha sido el de que se matan entre ellos, que la violencia es cosa del narco y nada tiene que ver con la ciudadanía, como si el Estado no tuviera responsabilidad en lo demás. Pero lo ocurrido en Ciudad Juárez rompe los argumentos.

Parece que habrá que considerar posibles cambios en el discurso tradicional de "abrazos, no balazos". Mientras, el presidente sigue mostrando las estadísticas que lo sitúan arriba de la clasificación entre los mandatarios mejor valorados del mundo.

Como siempre, estimado lector, lo invitamos a la reflexión. ¿Usted qué opina?

23 ANIVERSARIO DE SEA

Por otro lado, este 28 de septiembre de 2022 celebramos 23 años de la fundación de esta casa editorial, **Seguridad en América** (**SEA**), por lo que no queremos desaprovechar la oportunidad para agradecer a todos los lectores, patrocinadores, colaboradores y amigos que han hecho posible esta revista desde 1999, que ha sido la base para desarrollarnos hacia otras vertientes como SEA Media Group y SEA Academy. ■

En nombre de todo el equipo, ¡muchas gracias por su preferencia!

RECONOCIMIENTO

Como es costumbre **Seguridad en América** distingue a quienes, gracias a su interés en nuestra publicación, han formado parte del cuerpo de colaboradores al compartir su experiencia y conocimiento con nuestros lectores.

En la presente edición, el director general de esta casa editorial, Samuel Ortiz Coleman, entregó un reconocimiento a Óscar Fredy Paredes Muñoz, magíster en Seguridad y Defensa, consultor en Seguridad Corporativa y Gestión de Riesgos, quien en generosas ocasiones ha presentado a nuestro público lector interesantes artículos que atañen a la industria de la seguridad en su conjunto.

Por tal motivo decimos: "Gracias por pertenecer a nuestro selecto equipo de especialistas". ■

Si desea conocer más del experto, consulte su currículo:

ENTREVISTA EXPRÉS CON

Karina Sánchez Ochoa,

gerente de Operación Nacional en GECSA (Grupo Empresarial Casa)

¿Cuáles considera que serán los beneficios y/o consecuencias del Registro de Prestadoras de Servicios Especializados u Obras Especializadas (REPSE) para la industria de la seguridad privada?

Uno de los beneficios es que con el REPSE se regulará a las empresas de manera correcta y se evidenciará a aquellas que no cumplen con lo solicitado por la autoridad y esto tiene como consecuencia que las organizaciones que cumplen con el "deber ser" son las que están sobresaliendo y tomando ventaja sobre las que son competencia desleal ante el cliente y la autoridad. ■

ÍNDICE septiembre-octubre 2022

VIDEOVIGILANCIA

CONTROL DE ACCESO

TRANSPORTE SEGURO

CONTRA INCENDIOS

CIBERSEGURIDAD Y TI

ESPECIAL

SEGURIDAD PRIVADA

CONOCE A TU ASOCIACIÓN

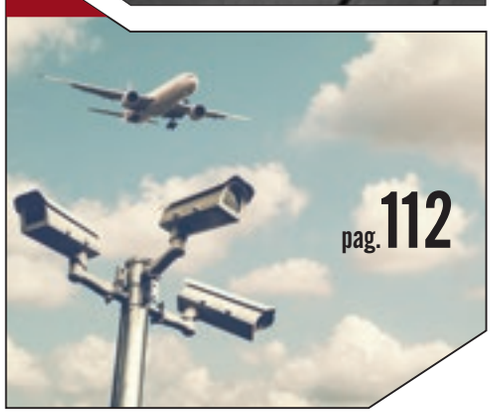
ÍNDICE septiembre-octubre 2022

PROTECCIÓN EJECUTIVA

LA ENTREVISTA CENTRAL

ADMINISTRACIÓN DE LA SEGURIDAD

SEGURIDAD PÚBLICA



EL PROFESIONAL OPINA

FOROS Y EVENTOS

NOVEDADES DE LA INDUSTRIA

TIPS

ENTREVISTA CON EL EXPERTO

DATA CENTER LOCAL Y EN LA NUBE: ¿CÓMO GARANTIZAR SU SEGURIDAD Y OPERACIÓN?

La seguridad de los Data Centers implica proteger la infraestructura crítica de amenazas o intrusiones que atenten contra las actividades de una empresa

Foto: Creativeart - Freepik

MÉXICO | Joel Alejandro Camacho Cortés

En la actualidad, todas las empresas —sin importar el rubro, sector e industria a la que pertenezcan— dependen de algún tipo de sistema e infraestructura, ya sean informáticos o de equipamiento crítico, para ejecutar y garantizar su correcta operación.

Los *Data Centers* resultan espacios sumamente estratégicos para las empresas y negocios, ya que hacen posible su continuidad al garantizar el correcto funcionamiento de los sistemas utilizados y el adecuado almacenamiento de los registros obtenidos.

DATA CENTER LOCAL Y EN LA NUBE

Un *Data Center* o centro de datos local es una infraestructura física que tiene la finalidad de alojar los activos requeridos para el almacenamiento, procesamiento y transmisión de información, además de todo lo necesario para que los equipos trabajen en óptimas condiciones.

Por su parte, un *Data Center* en la Nube se trata de un servicio provisto por un proveedor externo, quien gestiona el funcionamiento de los servidores virtuales, haciéndose responsable por el mantenimiento y las actualizaciones correspondientes.

Las plataformas de almacenamiento en la Nube admiten el pago bajo demanda, lo que significa que cada compañía tiene la posibilidad de contratar el espacio que necesite, ampliándola o reduciéndola de acuerdo con los requerimientos específicos de su negocio.

Además, el crecimiento de la digitalización empresarial y la aceleración tecnológica contribuyen a que cada vez sean más las organizaciones que apuestan por los *Cloud Data Centers*.

Los sistemas de videovigilancia son utilizados en estos espacios para monitorear las zonas de acceso, exteriores e interiores del *Data Center*, para lo que también pueden contar con alarmas encargadas de detectar incidencias

SISSA
DIGITAL

DESARROLLAMOS
SOLUCIONES DIGITALES

Para ***automatizar, controlar, monitorear y gestionar*** las plataformas, sistemas de seguridad y tecnologías de la información de su planta automotriz.

CONTÁCTENOS PARA
obtener más información
acerca de cómo elevar los niveles de seguridad y productividad en su planta automotriz o en cualquier industria a la que pertenezca.

55-1954.2832 55-6651-0200

Soluciones
totalmente personalizadas

Desarrollo
de software versátil y flexible

Integración de múltiples
equipos, dispositivos y PLC de diferentes marcas

Amplia suite
de drivers de comunicación

Soluciones hiperconvergentes
y sumamente escalables

¿QUÉ IMPLICA LA SEGURIDAD DEL *DATA CENTER*?

Los *Data Centers* son elementos fundamentales para cualquier tipo de organización, ya que ayudan a guardar, compilar y proteger todo tipo de información, así como a disminuir los riesgos de pérdidas de datos y a garantizar la continuidad de las operaciones y la rentabilidad del negocio. Es por ello que en estos espacios toma especial relevancia el tema de la seguridad.

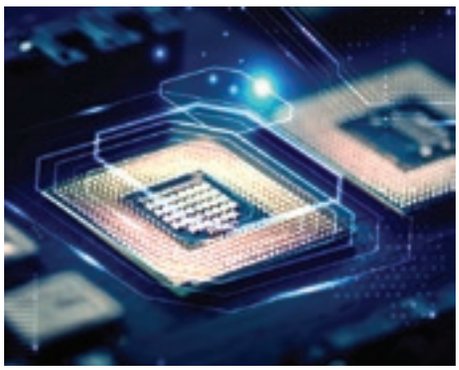
En este sentido, la seguridad debe contemplar más allá del perímetro de los *Data Centers* y abarcar todos los dispositivos posibles, como los servidores, los *switches* o los *routers*, ya que los ataques a las empresas y organizaciones se han vuelto cada vez más sofisticados y exploran nuevas vulnerabilidades tanto en *hardware* como en *software*.

Desde el punto de vista digital, la seguridad del *Data Center* depende de la definición e implementación de un plan de recuperación de datos ante cualquier tipo de desastre y de la protección de los archivos antes de ser almacenados.

SEGURIDAD DEL *DATA CENTER* LOCAL

Un *Data Center* local, además de conformarse por un conjunto de servidores físicos, integra diferentes sistemas de seguridad, como los sistemas de control de accesos encargados de validar la entrada del personal mediante tarjetas personales, a través de sistemas más complejos como los biométricos, e incluso con soluciones que integren ambos sistemas.

Los sistemas de videovigilancia son utilizados en estos espacios para monitorear las zonas de acceso, exteriores e interiores del *Data Center*, para lo que también pueden contar con alarmas encargadas de detectar incidencias o intrusiones lo antes posible.



De igual forma, los sistemas de protección contra incendios, los sistemas de respaldo de energía y los sistemas de climatización son de suma importancia para los *Data Centers*, ya que estos son los encargados de garantizar que todo el equipo activo resguardado en estos espacios esté operando sin dificultades ni problemas.

En lo referente al diseño de los *Data Centers* locales, aunque éste dependerá de su tipo, deben contar con elementos redundados, tales como los generadores de energía alterna a base de gas o diésel, los cuales son usados como plantas de emergencia a fin de suministrar energía eléctrica en caso de sufrir interrupciones por parte de la línea comercial.

SEGURIDAD LÓGICA DEL *DATA CENTER*

La seguridad lógica consiste en la implementación de barreras y procedimientos para la protección y conservación de los pilares de la seguridad de la información, que son: confidencialidad, integridad, disponibilidad, autenticidad y no repudio.

La encriptación de las transmisiones de datos se utiliza para asegurar los datos en Internet, para lo que dichos datos son cifrados y protegidos con ayuda del protocolo HTTPS.

Asimismo, el SSL, una de las encriptaciones más fiables que existen en el mercado hoy en día, garantiza a los usuarios de un sitio web que sus datos no serán interceptados de manera fraudulenta. No obstante, estos procesos deben adaptarse en función del tipo de información resguardada en cada centro de datos.

En cuanto a la seguridad de la red de un *Data Center*, es imprescindible contar con *Firewalls*, sistemas de detección de intrusos o IDS (*Intrusion Detection Systems*) para analizar y monitorear el tráfico de red en busca de posibles ciberatacantes, sistemas de prevención de intrusos o IPS (*Intrusion Prevention Systems*) para denegar de forma proactiva el tráfico de red en caso de que los paquetes representen una amenaza de seguridad conocida, basados en un perfil de seguridad.

Los ataques a las empresas y organizaciones se han vuelto cada vez más sofisticados y exploran nuevas vulnerabilidades tanto en *hardware* como en *software*

SOLUCIONES DE SEGURIDAD A LA MEDIDA

En SISSA Monitoring Integral no solamente nos especializamos en la consultoría, auditoría, ingeniería y diseño de centros de datos, sino que también garantizamos la seguridad de estos espacios mediante la implementación de diversos sistemas de protección.

Además, todas nuestras soluciones de TI, seguridad electrónica y telecomunicaciones responden a las necesidades específicas de cada uno de nuestros clientes y se adaptan a su presupuesto, razón por la cual en SISSA no sólo somos integradores de tecnología, sino que somos desarrolladores de soluciones diseñadas a la medida. ■

Fotos: SISSA Monitoring Integral

Joel Alejandro Camacho Cortés,
director de Desarrollo de Negocio y Preventa en SISSA Monitoring Integral.

Más sobre el autor:

GRUPO IPS

GARANTÍA EN SEGURIDAD

ÚNICA EMPRESA DE SEGURIDAD PRIVADA CERTIFICADA COMO UNA GPTW

Great Place To Work. Certificada Dic 2021 - Dic 2022 México

crese

ESR

Dignificamos al sector de la seguridad,

PARA CONSTRUIR EL MÉXICO QUE QUEREMOS

Síguenos

Tel. (55)5525 3242

grupoipsmexico.com

SISTEMAS DE VIDEOVIGILANCIA: EL FUTURO DE LA INDUSTRIA AUTOMOTRIZ

Ofrecer una solución completa e integral de videovigilancia se ha convertido en una "commodity" que todos los fabricantes deberían resolver

ESPAÑA | Raquel Elías Gutiérrez

La crisis económica generada por la pandemia agrava una situación que ya venía siendo delicada por los efectos de la nueva normativa medioambiental europea y que coloca a la industria automotriz en plena transformación tecnológica hacia la electrificación.

Con 3.1 millones de vehículos fabricados en 2021, México es el séptimo productor mundial. Las claves del éxito son la inversión en la innovación continua y la automatización de las plantas productivas que permiten generar una mayor producción, aprovechar los recursos y optimizar los tiempos.

En esta transformación tecnológica, los sistemas de video están jugando un papel fundamental. Con la incorporación de la Inteligencia Artificial (IA) en los sistemas de videovigilancia, las cámaras monitorizan la automatización de los procesos, detectan fallos y los previenen, verifican el control de la calidad, geolocalizan y visualizan activos en continuo movimiento y paralelamente, recogen metadatos asociados a las imágenes. Datos que, gracias a herramientas de *Big Data*, se transforman en información valiosa para generar cuadros de mando y gráficas que facilitan la toma de decisiones.

Este artículo tiene como objeto recoger algunas de las principales aplicaciones de uso que nuestros clientes hacen de los sistemas de video inteligentes en sus procesos productivos.

MONITORIZACIÓN DE PROCESOS AUTOMATIZADOS

Los sistemas de video son la clave para garantizar la excelencia en los procesos productivos. Integrados con los habituales sistemas de gestión son capaces de detectar un incidente (parada o avería de una máquina) y alertar en tiempo real al centro de control para resolver la incidencia en el menor tiempo posible.

La visibilidad completa de sus procesos en vivo optimiza flujos de trabajo, maximiza la producción, reduce los costos y garantiza la continuidad del negocio.

Foto: Creativeart - Freepik


ELLOS ENTRETIENEN.
NOSOTROS PROTEGEMOS.
GARRETT
Confía en los productos de seguridad para detección de metal y escaneo térmico Garrett.
PD 6500i
PINPOINT
DETECTION

Foto: SCATI

SUPERVISIÓN DEL CONTROL DE CALIDAD

Los sistemas de video son capaces de realizar inspecciones en la fabricación y ensamblaje de todas las piezas de un vehículo, detectar así defectos de estampación, mecanizado, presencia de componentes, calidad de pintura, metrología entre las piezas de la carrocería o alineamiento de las puertas, entre otras muchas.

VERIFICACIÓN Y TRAZABILIDAD DE MERCANCÍAS

Junto a la captura de imágenes del proceso productivo, los sistemas de video recogen la información asociada a cada mercancía (N.° de expedición, origen, destino, dimensiones, etc.) y almacenar esta información en el sistema, garantizando la trazabilidad.

El video es una herramienta versátil que se puede integrar con otros sistemas de lecturas de códigos QR o de barras, para completar la supervisión del proceso. Los sistemas de video permiten realizar búsquedas por los metadatos recogidos, visualizar el recorrido de cada mercancía y localizar cualquier momento y la imagen asociada.

Los sistemas de videovigilancia "inteligentes" se integran con *software* de geolocalización y control de tráfico (AGV- Vehículo de Guiado Automático) y seguir y localizar miles activos (operarios, toros mecánicos, pallets, etc.) con una gran precisión y visualizar las imágenes captados por las cámaras en tiempo real.

Además, los sistemas de videovigilancia permiten supervisar varias instalaciones dispersas geográficamente y controlar el estado de todo el sistema desde un único centro de control y en cualquier momento.

OPTIMIZACIÓN DE PROCESOS INDUSTRIALES Y LOGÍSTICOS

Nos encontramos ante la IV Revolución Industrial. Ofrecer una solución completa e integral de videovigilancia se ha convertido en una "*commodity*" que todos los fabricantes deberíamos resolver.

Sin embargo, en la IV Revolución Industrial, los sistemas de videovigilancia jugarán un papel fundamental para la resolución de problemáticas que no están ligadas a la seguridad: trazabilidad de mercancías, supervisión de flotas de vehículos y otros activos móviles, optimización del *stock*, etc.

A través del *Big Data*, seremos capaces de recoger información asociada a cualquier imagen para sintetizarla y disminuir los tiempos de administración, agilizar la operativa diaria y optimizar cualquier proceso empresarial.

Como hemos visto, el video se postula como una herramienta de innovación por la gran versatilidad que ofrece a la hora de resolver cualquier problemática y que marca la diferencia competitiva frente a otras empresas del sector. ■

Foto: SCATI

Con la incorporación de la IA en los sistemas de videovigilancia, las cámaras monitorizan la automatización de los procesos, detectan fallos y los previenen

Raquel Elías Gutiérrez,
Marketing Manager de SCATI.

Más sobre el autor:

SISSA
INFRAESTRUCTURA

SISSA INFRAESTRUCTURA EN
DATA CENTERS

Diseñamos, implementamos y gestionamos proyectos llave en mano de infraestructura para proteger todos los activos alojados en su Data Center y garantizar la continuidad de su negocio.

¡Conozca más sobre SISSA Infraestructura!

- **SISTEMAS DE DETECCIÓN** CONTRA INCENDIOS.
- **SISTEMAS** DE TIERRAS.
- **SISTEMAS DE RESPALDO DE ENERGÍA** (UPS).
- **AIRES DE PRECISIÓN Y CONFORT PARA DATA CENTER** (TIPO MOCHILA, INROW Y RACK COOLER).

Contáctenos para obtener más información sobre los servicios llave en mano de SISSA Infraestructura.

55-6651-0200

LA IMPORTANCIA DE LA SEGURIDAD FÍSICA EN *DATA CENTERS*

Los sensores pueden crear diferentes zonas de detección para proteger los diferentes racks de servidores y se pueden vincular al sistema de control de acceso

MÉXICO | René Cuenca

La creciente demanda de servicios en la Nube y la adopción de tecnologías digitales ha impulsado un tremendo crecimiento de los centros de datos y ha destacado aún más la importancia de mantener los datos seguros y protegidos.

Si bien hay un fuerte enfoque en la ciberseguridad, la intrusión física y el acceso no autorizado también representan una gran proporción de amenazas para un centro de datos y, ya sea un centro de datos a gran escala o un centro de datos operado por el propietario de una empresa más pequeña, el robo o daño de los datos podría convertirse en una interrupción significativa de los niveles de servicio.

Foto: Optex

Un enfoque de seguridad física de varias capas, que combina la protección en el exterior hasta la sala de servidores, puede ayudar a minimizar cualquier amenaza de seguridad y ayudar a mantener los datos seguros.

PERÍMETRO Y ENFOQUE DE CONSTRUCCIÓN

Las cercas perimetrales y las puertas proporcionan la primera capa de seguridad para la mayoría de las instalaciones del centro de datos y agregar tecnologías de detección de intrusiones puede ayudar a los equipos de seguridad a obtener una alerta temprana de una intrusión y evitar el acceso no autorizado. Una vez que alguien ha entrado en el perímetro, la detección volumétrica precisa y confiable alrededor del edificio puede admitir la videovigilancia y permitirá al equipo de seguridad rastrear la ubicación de la intrusión, y si se trata de una o varias personas.

ASEGURAR LA ESTRUCTURA DEL EDIFICIO

La mayoría de los edificios de centros de datos y ciertamente las salas de servidores no tienen ventanas exteriores y pocos puntos de entrada. Sin embargo, la protección de la estructura del edificio podría evitar una amenaza potencial, como perforar un agujero o acceder a través del sistema de ventilación. Los sensores de fibra óptica montados en la pared pueden detectar perforaciones o intentos de dañar la pared, el piso o el techo. La tecnología LiDAR puede proporcionar una capa de seguridad alternativa y adicional mediante la creación de paredes o techos virtuales para proteger el edificio.

SEGURIDAD DE ACCESO Y DETECCIÓN DE "*TAILGATING*"

Controlar el acceso al edificio o a las zonas seguras es de vital importancia. Uno de los riesgos es si una persona no autorizada sigue a una autorizada, ya sea forzada o accidentalmente. La instalación de un sistema "anti-*tailgating*" combinado con un sistema de control de acceso (lector de tarjetas, biometría, etc.) puede alertar a la seguridad y verificar el acceso al área segura.

Foto: Creativeart - Freepik

Si el acceso al edificio es a través de torniquetes, la tecnología LiDAR puede proporcionar protección adicional mediante la creación de una pared virtual sobre los torniquetes, establecer una zona de detección por torniquete y cuando se conecta al sistema de control de acceso, detectará a una persona que pasa por un torniquete sin deslizar su tarjeta de acceso.

SALAS DE SERVIDORES

En el corazón de los centros de datos se encuentra la sala de servidores, un área de acceso restringido, generalmente solo accesible para técnicos e ingenieros que necesitan mantener, actualizar o reparar el equipo. La seguridad de la sala implicará garantizar que solo el personal autorizado entre en la sala y que solo acceda a los bastidores de servidores que necesitan ser manipulados.

Los sensores LiDAR con su detección flexible son capaces de operar incluso en completa oscuridad y son la tecnología más adecuada para proteger las salas de servidores. Los LiDAR 2D pueden crear techos, pisos y paredes virtuales, lo que permite que las áreas de detección personalizables "protejan" efectivamente las unidades del servidor.

Foto: Optex

Los sensores también pueden crear diferentes zonas de detección para proteger los diferentes racks de servidores y se pueden vincular al sistema de control de acceso, por lo que en el caso de una persona que estaba autorizada a acceder al rack uno, pero estaba manipulando el rack dos, el sistema de seguridad se activaría y podría configurarse para activar el control de acceso y bloquear la habitación.

El tamaño del objeto objetivo también se puede personalizar para proporcionar una alerta si algo tan pequeño como una memoria USB pasa a través del haz de detección. Otro beneficio de usar sensor LiDAR de seguridad para la protección de salas de computadoras es que funcionan con iluminación variable, incluso en completa oscuridad y en ambientes fríos. ■

René Cuenca,
gerente de Ventas en México & Centroamérica de Optex Latin America.

Más sobre el autor:

GARANTÍA DE SERVICIOS

Múltiples casos de éxito donde a través de los C5 en un robo se recuperan las unidades y las mercancías de los clientes en menos de 30 minutos, una ventaja competitiva sobre muchas empresas

MÉXICO | Erick Martínez / *Staff* Seguridad en América

La afinidad de un destacado grupo de líderes en materia de Seguridad Privada y rastreo GPS los reúne en marzo de 2007 para crear la Asociación Mexicana de Empresas de Seguridad Privada e Industria Satelital, A.C. (AMESIS), comprometidos en identificar, desarrollar y solventar las necesidades que el mercado requiere para apoyar a las empresas del sector en la actualidad. Hoy, a más de una década de trayectoria, la AMESIS ha logrado consolidarse como un órgano referente del sector y participante activo en la evolución de la seguridad en México.

Ricardo Bustamante Medina, presidente y socio fundador de AMESIS, además de CEO de Grupo UDA, afirmó en entrevista con **Seguridad en América** (**SEA**), que la AMESIS está basada en valores de confianza, seguridad y respeto entre los socios, promoviendo la unión y cada día sumar a las empresas de rastreo satelital más serias y comprometidas en aplicar nuevas tecnologías, generar estadísticas, apoyar en recuperar pérdidas a nivel nacional, el compartir ideas e información útil para poder hacer crecer al sector, lo que ha sido un gran acierto para todos, pues han logrado un avance significativo.

LOS BENEFICIOS DE AMESIS

La AMESIS ofrece grandes beneficios a todos los socios que la conforman, vincula el rastreo satelital desde un equipo básico hasta en los remolques, chapas electromecánicas, sensores de combustible, y en el caso de *Safety* corroborar si el operador de la unidad de transporte se encuentra en las mejores condiciones, monitoreando su conducción, ritmo, estado de salud, etc., previniendo accidentes y delitos a través del monitoreo inteligente.

Una de las novedades de la asociación es su nuevo sitio web, el cual cuenta con una intranet, donde se puede consultar información estadística acerca de la recuperación de vehículos y mercancías robadas.

El objetivo es que las empresas que conforman AMESIS sumen información a la estadística y juntos ir construyendo datos que sean públicos para así conocer mejor a la delincuencia, qué tipo de mercancías roban más, los tramos carreteros más complicados, horarios, etc., para poder seccionar y atacar cada sector de delincuencia.

Ricardo Bustamante Medina,
presidente y socio fundador de AMESIS

Federico Cruz Ortega,
representante del Comité de Relaciones Públicas de AMESIS

Federico Cruz Ortega, director comercial de ISIS Seguridad Integral, integrados hace un par de meses a AMESIS y perteneciente al Comité de Relaciones Públicas, señaló que "el beneficio que se le puede dar a los clientes por pertenecer a AMESIS es la relación directa con las autoridades, en el sentido tener una pronta respuesta en caso de necesitarlo en los diferentes niveles federal, estatal y municipal".

EL IMPACTO Y COLABORACIÓN DE AMESIS

El impacto que esta asociación genera es muy grande, ya que es de las principales asociaciones que conforman a Agrupaciones de Seguridad Unidas por México (ASUME), la cual busca promover la Ley General de Seguridad Privada y la Cámara Nacional de la Seguridad Privada. Además, trabaja constantemente con asociaciones hermanas como son la Asociación Mexicana de Empresas de Seguridad Privada (AMESP), ASIS International, Asociación Nacional de Empresas de Rastreo y Protección Vehicular (ANERPV), Cámara Nacional del Autotransporte de Carga (CANACAR), lo que otorga una gran fortaleza para en el sector, poder apoyar al cliente final como un valor agregado a través de estas vinculaciones.

"Mediante estos vínculos estratégicos se busca que las empresas que se dedican a esto sean formales, ya que las empresas patito crean competencia desleal, posicionando al sector de manera negativa", afirmó Bustamante. Rodrigo Larracilla Godoy, secretario de AMESIS, director general de SKY Meduza y socio desde hace dos años, comentó que para pertenecer a la asociación se tiene que cumplir con una serie de filtros y requisitos, no sólo es la legalidad, sino el equipo y la robustez de infraestructura con la que se cuente, que pueda dar seguridad y confianza al cliente, que está contratando una empresa estable y un servicio adecuado respaldado por AMESIS. ■

Una de las novedades de la asociación es su nuevo sitio web, el cual cuenta con una intranet, donde se puede consultar información estadística acerca de la recuperación de vehículos y mercancías robadas

Rodrigo Larracilla Godoy,
secretario de AMESIS

Fotos: Erick Martínez / SEA

Columna de
Jaime A. Moncada, PE
jam@ifsc.us

Director de International Fire Safety Consulting (IFSC), una firma consultora en Ingeniería de Protección Contra Incendios con sede en Washington, DC. y con oficinas en Latinoamérica.

Más sobre el autor:

EUA

INCENDIOS EN PRISIONES

El 28 de junio de 2022 ocurrió otro gran incendio en una prisión en América Latina. En este caso en el Pabellón 8 de la Cárcel de Tuluá, en las afueras de la ciudad de Cali en Colombia. Hasta el momento de escribir esta columna, son 53 muertos y 8 en estado crítico. Aunque los hechos son todavía confusos, se dice que hubo un motín en horas de la madrugada, que la policía entró a controlarlo, que los prisioneros prendieron fuego a los colchones y se desencadena así esta tragedia. La prisión tenía sobrecupo y no tenía sistemas automáticos de supresión de incendios, el común denominador en estos incidentes a nivel regional.

En América Latina, en la últimas décadas, hemos estado padeciendo una epidemia de grandes incendios en prisiones. De los incendios con más de 50 muertos a nivel mundial, el 75% de ellos han ocurrido en una prisión latinoamericana. Todos han ocurrido en países en vías de desarrollo. La mayoría pasan desapercibidos, y debido a la población que muere en estas tragedias, la sociedad no se conmueve, ni pide cambios.

	PRISIÓN	PAÍS	FECHA	MUERTOS
1	Pen. Nal de Camayagua	Honduras	14 Feb 12	361
2	Cárcel de Higüey	Rep. Dom.	07 Mar 05	136
3	Prisión de Sabaneta	Venezuela	03 Jun 94	108
4	Cárcel de San Pedro Sula	Honduras	17 May 04	101
5	Cárcel de San Miguel	Chile	08 Dic 10	81
6	Cárcel de La Ceiba	Honduras	05 Abr 03	68
7	Calabozo Policía Carabobo	Venezuela	29 Mar 18	68
8	Prisión Al-Hair	Arabia Saudi	15 Sep 03	67
9	Prisión de Uribina (Barquisimetro)	Venezuela	24 Ene 13	63
10	Prisión Hasaka	Siria	24 Mar 93	57
11	Cárcel Tulúa	Colombia	28 Jun 22	53
12	Prisión Sidi Moussa	Marruecos	01 Nov 02	50

Lista compilada por Jaime A. Moncada de reportes peridísticos.

El incendio de la Penitenciaría Nacional de Comayagua, que ocurrió en Comayagua, Honduras, en febrero de 2012, donde 361 reclusos perdieron la vida, es el más trágico incendio que se tenga memoria a nivel mundial

EL PROBLEMA CARCELARIO LATINOAMERICANO

En años recientes hemos tenido los tres incendios de mayor relevancia a nivel mundial en usos carcelarios: Comayagua, Honduras; Higüey, República Dominicana; y la Prisión de Sabaneta en Venezuela. Luego del incendio de Comayagua, la más importante tragedia en una prisión a nivel mundial, la cual yo tuve la responsabilidad de documentar para la NFPA (National Fire Protection Association), yo escribí que "la probabilidad de morir en un incendio penitenciario en América Latina es más de 200 veces mayor que en los EE.UU."[1]. ¡Esto es increíble! Desafortunadamente, la gran mayoría de los incendios en usos carcelarios en nuestra región no han tenido una rigurosa investigación.

Una excepción es el incendio de la Penitenciaría Nacional de Comayagua, que ocurrió en Comayagua, Honduras, en febrero de 2012, donde 361 reclusos perdieron la vida. Tuve la oportunidad de visitar esta presión días después del incidente y documentar lo allí ocurrido para la NFPA. Durante mi visita encontré condiciones similares a otros incendios en la región: hacinamiento, uso de terminados interiores altamente inflamables, falta de apropiadas vías de evacuación e inexistencia de sistemas automáticos de protección contra incendios.

En este tipo de incendios resulta común ver cortinas y otros materiales combustibles rodeando las camas de los reclusos en las celdas (ver foto anexa). Lo mismo sucede con los artefactos eléctricos y sus tomacorrientes sobrecargados. En el incendio de 2004 de San Pedro Sula, los funcionarios del gobierno hondureño informaron la

presencia de 75 artefactos eléctricos en una celda de 10 por 15 metros. Los incendios como los de la prisión de Tuluá y la de San Pedro Sula a menudo son provocados por peleas entre reclusos, en las que el caos, sumado a una llama abierta, cableado eléctrico y abundantes materiales combustibles, puede generar incendios de desarrollo rápido.

FILOSOFÍA DE SEGURIDAD CONTRA INCENDIOS EN UNA PRISIÓN

La ocupación correccional utiliza la misma filosofía de seguridad humana y protección contra incendios que los hospitales, con el concepto de "defender en su lugar". En una prisión, los ocupantes son incapaces de velar por su preservación durante un incendio, no por razones médicas como en un hospital, sino por restricciones de seguridad, que previenen el movimiento libre y el acceso hacia las áreas adyacentes.

Sin embargo, la solución a esta problemática está en nuestras manos. En los Estados Unidos, el número de incendios en prisiones ha decrecido en un 88% desde 1980[2], mientras que la población carcelaria ha crecido en un 460%[3]. Esta increíble estadística ha ocurrido debido al uso riguroso de códigos modernos de prevención de incendios, como los de la NFPA. En este sentido, la norma NFPA 101, establece los criterios de seguridad humana y protección contra incendios para usos correccionales nuevos y existentes. En prisiones nuevas, excepto las clasificadas como "Condición de Uso I"[4], se requiere la protección de toda la instalación con rociadores automáticos, además de medidas de compartimentación, evacuación, y otros medios de protección contra incendios.

Cortinas altamente combustibles, utilizadas por los reclusos buscando privacidad

Foto: Cortesía Jaime A. Moncada

CRITERIOS DE SEGURIDAD CONTRA INCENDIOS

Tomando como ejemplo la Prisión de Comayagua, la normativa NFPA clasificaría esta instalación como Uso Condición V–Contenido, en donde el movimiento libre se ve restringido en los módulos y los guardias controlan manualmente la liberación de cada puerta. Una instalación correccional existente como la de Comayagua, con una construcción Tipo II (000), requeriría las siguientes características de seguridad humana y protección de incendio:

- **Protección de rociadores:** no se permiten módulos residenciales sin protección de rociadores. Los rociadores automáticos utilizados en este tipo de instalaciones son rociadores especiales, llamados "rociadores institucionales", los cuales son diseñados para prevenir el soporte de una carga[5] y con componentes que no sean fácilmente convertibles en armas. Los fabricantes de este tipo de rociadores también indican en su literatura que estos rociadores son "*tamper resistant*", o sea que alguien no los pueda cambiar o dañar, como por ejemplo, que resistan un golpe.
- **Detección de humo:** los módulos residenciales requieren un sistema automático de detección de humo.
- **Sistema de alarma de incendio:** el sistema de alarma de incendio requerido debe brindar notificación automática a los ocupantes.
- **Contenidos combustibles:** se necesitan controles adecuados para limitar la cantidad y combustibilidad de los combustibles disponibles para reducir la probabilidad de una combustión súbita generalizada en la habitación; se prohíben las decoraciones combustibles a menos que sean retardadoras de llamas; las cortinas para privacidad deben cumplir con los criterios de desempeño de propagación de la llama incluidos en NFPA 701, Métodos Normalizados de Pruebas de Incendio para la Propagación de la Llama de Textiles y Películas; aunque no se exija estrictamente, se recomienda que los colchones sean evaluados en relación a riesgos de incendio, y se brindan pautas para este objetivo en ASTM F1870, Pautas Estandarizadas para la Selección de Métodos de Pruebas de Incendio para la Evaluación de Mobiliarios Tapizados en Instalaciones Penitenciarias y Correccionales.
- **Colchones:** los nuevos colchones utilizados en ocupaciones penitenciarias y correccionales deben cumplir con ciertos criterios basados en la norma federal 16 CFR 1632, Norma para la Inflamabilidad de Colchones y Cubre Colchones (FF 4–72). También resulta aplicable una segunda norma de prueba, ASTM E 1537, Método de Prueba Normalizado para Pruebas de Incendio de Muebles Tapizados, cuando el colchón se utiliza en un edificio sin rociadores.
- **Separación entre módulos:** la separación entre habitaciones debe ser resistente al humo.

En los Estados Unidos, el número de incendios en prisiones ha decrecido en un 88% desde 1980, mientras que la población carcelaria ha crecido en un 460%

REFLEXIONES FINALES

Los incendios en prisiones tienen casi todos las mismas condiciones de riesgo, queriendo decir con esto que los riesgos presentes se repiten en cada uno de los incendios que han ocurrido en la región. Algo similar ocurre en los incendios en discotecas. Sin embargo, mi percepción es que la normativa internacional, como la de la NFPA, no se está utilizando en el diseño o rehabilitación de la mayoría de las prisiones latinoamericanas. Yo como consultor de seguridad contra incendios, muy rara vez he recibido una llamada de un operador de prisiones o una invitación a una licitación, donde se haga referencia a esta normativa o a la posibilidad de evaluar cómo mejorar las condiciones de seguridad contra incendios de prisiones nuevas o existentes. Es como si las tragedias de todas estas prisiones, donde miles de personas han perdido la vida, no le interesara a nadie. ■

REFERENCIAS

1 *Lecciones de Comayagua por Jaime A. Moncada, PE, NFPA Journal Latinoamericano, Sep. 2012, Año/Vol. 14, No. 3, Págs. 36-35.*
2 *Prisons and Jails, Jenniffer Flynn, NFPA Fire Analysis and Research, Marzo 2010.*
3 *US Bureau of Justice Statistics, US Department of Justice, 2010, Washington.*
4 *Condición de Uso I: Aquella bajo la cual está permitida la libre circulación desde las áreas con camas y otros espacios, hasta el exterior a través de medidos de egreso que cumplen los requerimientos de la NFPA 101 (NFPA 101-2021: Art. 22.1.2.1.1).*
5 *Como por ejemplo, que alguien ate una cuerda al rociador y con ella trate de ahorcarse.*

Foto: InSight Crime

EVOLUCIONA LA SEGURIDAD

Servicio a Nivel Nacional

DE TU HOGAR Y NEGOCIO AL SIGUIENTE NIVEL

EMPRESA ESPECIALIZADA EN
LA INSTALACIÓN, INTEGRACIÓN,
MONITOREO Y MANTENIMIENTO
DE LOS SISTEMAS DE SEGURIDAD
ELECTRÓNICA

PROTECCIÓN ELECTRÓNICA MONTERREY S.A. DE C.V.

INDUSTRIAL • RESIDENCIAL • COMERCIAL • GOBIERNO
FRACCIONAMIENTOS • PARQUES DE ENERGÍA • AEROPUERTOS

WWW.PEM-SA.COM

222 141 12 30

gerenciacomer@pem-sa.com

ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD
ALAS
SOCIO ALAS

SISTEMA DE GESTIÓN
ISO 9001:2015
BICERT, S.C.

REPSE
AR10508/2021

Achilles
No. 329,814

COPARMEX

REGISTRO FEDERAL DGSP/303-16/3302 PERMISO SSP PUEBLA SSP/SUBCOP/DGSP/114-15/109

EL COSTO DE LOS **CIBERATAQUES** Y EL ROI

Foto: ipopba - Freepik

Las organizaciones que adoptaron algún tipo de modelo de trabajo remoto pagaron un promedio de 1.07 millones de dólares por daños derivados de una brecha de seguridad en sus datos

MÉXICO | Jonathan Fridman

La pandemia mundial por COVID-19 parece estar llegando a un estado de relativa estabilidad. Si bien será algo con lo que tendremos que vivir el resto de nuestras vidas, las consecuencias más allá de los claros efectos en la salud y en la vida, también permanecerán con nosotros y podemos hablar de una época AC y DC (antes y después del COVID-19).

Definitivamente los principales héroes han sido los médicos y las vacunas que han logrado prevenir y salvar miles de vidas, sin embargo, hay un héroe del que poco se ha hablado y que había estado presente en nuestras vidas, pero de manera más discreta, la tecnología. Estas herramientas que nos permitieron seguir operando lo más normal o eficiente posible a pesar de estar distanciados. Bancos, compras, supermercados, educación y trabajo remoto son algunos ejemplos de servicios básicos que pudimos mantener en el encierro de manera relativamente eficiente. Aunque si bien es un hecho que no estábamos preparados para esta transformación digital, la realidad es que desde hace muchos años hemos venido evolucionando en esa dirección, la pandemia únicamente funcionó como el catalizador perfecto para potencializar esta transformación en nuestra vida diaria.

Prácticamente todos los aspectos de nuestra vida diaria, de nuestras familias y colaboradores se vieron afectadas por esta transformación digital y sus efectos todavía no terminamos de dimensionarlos. Lo que es innegable es que nuestros hábitos y forma de vivir el día a día cambió.

A pesar de los innumerables beneficios que hemos encontrado y que seguimos descubriendo al evolucionar a un mundo mucho más digital e interconectado, hay un elemento que también se potencializó como consecuencia directa del uso intensivo de tecnologías, los ciberataques. Básicamente un ciberataque es la explotación deliberada de sistemas informáticos, empresas y redes que dependen de la tecnología. Los ataques cibernéticos usan código malicioso para alterar el código, la lógica o los datos de los equipos, lo que genera consecuencias que pueden comprometer los datos y dar lugar a delitos cibernéticos, como el robo de información y de identidad.

Si no estábamos preparados para modificar nuestras rutinas y hábitos tecnológicos, mucho menos lo estábamos para protegernos y hacer uso de manera segura de esta tecnología. Esta brecha ha sido explotada por los ciberdelincuentes, para los cuales la pandemia convirtió un negocio que ya era rentable, en un campo fértil para explotar y aprovechar al máximo.

El gasto promedio anual en ciberseguridad por empleado se incrementó de 2 mil 337 dólares a 2 mil 691 dólares en 2020 aproximadamente 15%

De acuerdo con datos de Avantika actualmente existen tres elementos que explican el incremento en los ciberataques:

1.

Es negocio. Los daños infligidos por la ciberdelincuencia ascienden a un estimado global de seis trillones de dólares en 2021, si midiéramos la ciberdelincuencia en términos de un país, esto representaría la tercera economía más grande del mundo sólo detrás de Estados Unidos y China. Esta cifra representa 500 billones de dólares al mes, 115.4 billones de dólares a la semana, 16.4 billones de dólares al día, 684.9 millones de dólares cada hora, 11.4 millones de dólares al minuto y 190 mil dólares cada segundo. En resumen, es rentable.

2.

Hay mercado. Todos nos volvimos más vulnerables a partir de la pandemia y el trabajo remoto. El costo promedio de un ciberataque es de 1.07 millones de dólares más alto donde el trabajo remoto fue un factor. Las organizaciones que adoptaron algún tipo de modelo de trabajo remoto pagaron un promedio de 1.07 millones por daños derivados de una brecha de seguridad en sus datos. También se necesita más tiempo para que los colaboradores operando de manera remota contengan estos ataques. En promedio, las empresas con hasta el 50% del personal trabajando de forma remota tardaron al menos 58 días en identificar y contener las filtraciones de datos.

3.

Relación costo-beneficio. El anonimato que ofrece Internet y el incremento de sitios de ingeniería social hacen que las técnicas de ataque se vuelvan cada mes más accesibles. El elemento trasnacional, la existencia de "agujeros negros" informáticos como China o Rusia y la constante evolución de técnicas y modelos de extorsión y secuestro de información hacen que el rastreo de los ciberdelincuentes sea cada vez más complejo.

En estas condiciones de acceso a la información y anonimato, el beneficio potencial de realizar un ataque supera y por mucho la probabilidad de ser detenido. Sobre todo, cuando el uso de criptomonedas sin controles o supervisiones internacionales establecidas permite consolidar un modelo criminal rentable y de muy bajo costo. En Estados Unidos se estima que solamente el 0.3% de todos los cibercrímenes reportados son procesados por la autoridad y dado que la gran mayoría de los ataques no son reportados, este número podría disminuir a menos del 0.05%. Si a esto le sumamos el hecho de que muchas empresas que son vulneradas pueden no estar enteradas y ni si quiera reportarlo, menos del 1% de los ciberdelincuentes son atrapados y condenados.

INVERSIÓN EN CIBERSEGURIDAD

A primera vista parecería que la pregunta relevante para los directores y dueños de empresas debería ser ¿qué podemos hacer para protegernos? Sin embargo, la realidad es que la pregunta que realmente todos hacemos es ¿cuánto debemos gastar en ciberseguridad para evitar un ataque?

El gasto promedio anual en ciberseguridad por empleado se incrementó de 2 mil 337 dólares a 2 mil 691 dólares en 2020 aproximadamente 15%. Mientras que un negocio promedio en Estados Unidos destina tan solo alrededor del 6% de su presupuesto de TI en ciberseguridad. Estos números para América Latina son aún más preocupantes dado que las regulaciones de cumplimiento son mucho menos estrictas que en Estados Unidos, donde el incentivo a invertir en ciberseguridad se da principalmente por las regulaciones cada vez más demandantes y que abarcan prácticamente todos los sectores e industrias.

En términos del Retorno de Inversión (ROI), la mayoría de las empresas calculan la inversión en ciberseguridad de acuerdo al *benchmark* con el mismo sector y el riesgo potencial de los costos derivadas de la pérdida o secuestro de información. Sin embargo, pocas consideran cuál es la necesidad real al interior de la empresa. De aquí que al diseñar un Plan Anual de Ciberseguridad, si bien es importante considerar lo que se está haciendo en la misma industria, el componente fundamental es realizar un traje a la medida identificando los elementos con los que cuento, el valor de los riesgos asociados a una brecha de seguridad y alinear los procesos y objetivos del negocio en una misma dirección incluyendo a todos los miembros de la organización creando una cultura de ciberseguridad robusta e integral.

Finalmente, el cuestionamiento que todos debemos hacernos es el siguiente: hace tres años, ¿cuál era mi nivel de conciencia y preocupación por la postura de ciberseguridad en mi empresa y en mi entorno? Y hoy en día cuánto se ha incrementado ese nivel de conciencia y preocupación. Una vez definido este incremento, la pregunta crítica es si mi inversión en ciberseguridad se ha incrementado en la misma proporción. Una discrepancia en esta correlación es un claro indicador que debemos asesorarnos y ejecutar acciones, porque hoy en día somos vulnerables. ■

Jonathan Fridman,
director de Operaciones de Avantika.

Más sobre el autor:

Foto: tete_escape - Freepik

SEMICONDUCTORES, EL COMBUSTIBLE DE LA ECONOMÍA MUNDIAL

Los famosos semiconductores se han convertido en el combustible principal para que prácticamente todas las industrias puedan operar y así abastecer un mercado de consumo mundial que no deja de crecer. La crisis de semiconductores aún no termina y seguirá profundizándose durante 2022

ARGENTINA | Diego Madeo

Las empresas que desarrollan y fabrican se han convertido en expertos malabaristas de este gran circo que hoy tiene en vilo a todo el mundo. La búsqueda de nuevos proveedores asiáticos y de Estados Unidos, que aún manejan parte del *stock* remanente con precios que no dejan de crecer, sumada a la incertidumbre de fechas de entregas por parte de las fábricas, son algunos de los tantos problemas que día a día van mutando en este "sálvese quien pueda". Parece caótico, ¿no? y lo es, porque se avecinan para esta segunda mitad de 2022 más desafíos para resolver por parte de los fabricantes de productos terminados.

Miremos la problemática desde el punto de vista del consumidor final, ¿cuál es el impacto que está sufriendo? ¿Realmente está percibiendo qué es lo que sucede? El incremento del precio final de un producto tecnológico, ¿es significativo? Y la verdad es que se observa un gran desconocimiento del tema; el impacto por demoras en entregas o aumentos de precios difícilmente son comprendidos y relacionados con la crisis de semiconductores.

La escasez mundial de microcontroladores ha tenido efectos de gran alcance en la fabricación y el crecimiento económico de muchas compañías de seguridad electrónica. Pero sin dudas, la peor crisis se observa en los fabricantes de automóviles más grandes del mundo que han tenido que cerrar fábricas y recortar la producción debido a la falta de semiconductores necesarios para el normal funcionamiento del vehículo, ocasionando perdidas de miles de millones de dólares debido a la demora en las entregas, a pesar de la fuerte demanda.

Los fabricantes de automóviles se están preparando para un dolor de cabeza prolongado, los tiempos de espera de semiconductores se han alargado y los precios han subido. Este déficit de microcontroladores también se ha extendido a la industria de la seguridad que se encuentra en tasas de crecimiento sostenidas año con año. Cadenas de producción que se interrumpen provocando demoras en las entregas y aumento de precios en los productos finales.

Durante 2021, se estima que en Latinoamérica los precios de productos terminados de seguridad incrementaron en dólares entre un 15 y 20%, una situación inusitada teniendo en cuenta la estabilidad de las últimas dos décadas, donde inclusive se observaban decrementos en los precios de venta de ciertos productos que componen las distintas familias de seguridad electrónica.

¿CÓMO SE ESTÁ RESOLVIENDO ESTA GRAN CRISIS?

Los fabricantes de semiconductores alrededor del mundo comenzaron una carrera sin precedentes para aumentar la capacidad de producción. Pero los millones de dólares que se están invirtiendo aún no están dando sus frutos. Las plantas no comenzarán la producción en masa por lo menos hasta 2024, por lo que no ayudará a resolver la escasez inmediata.

FÁBRICA

Instalar una fábrica en Japón es el reciente plan de expansión para el jugador taiwanés más grande del mercado TSMC, que hoy cuenta con 51 mil empleados en todo el mundo, controlando la impresión de pastillas de silicio con un *Market share* mundial del 50% . La construcción de la nueva planta comenzará este año y la producción en masa a fines de 2024, mientras tanto, TSMC espera que su capacidad de producción se mantenga ajustada.

A principios de 2021 la compañía se comprometió a invertir 100 mil millones de dólares en esta nueva planta con

el desarrollo de nuevas tecnologías. Además, TSMC está construyendo otra fábrica de chips de 12 mil millones de dólares en Arizona y expandiendo la capacidad de producción en Nanjing, China, según indica el portal The Wall Street Journal.

Como comentamos anteriormente, las nuevas fábricas no estarán operativas durante los próximos años, pero la inversión promete impulsar la presencia de la producción estadounidense en la fabricación de chips avanzados después de décadas de ceder terreno a ubicaciones en Asia como Taiwán, Corea del Sur y China.

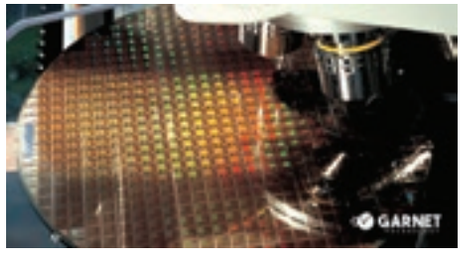
PERSONA EN FÁBRICA

La guerra geopolítica aumenta las apuestas para que los gobiernos, en particular en Estados Unidos y Europa, reduzcan su dependencia de los proveedores asiáticos y esto ha desencadenado una ola de inversiones récord en microprocesadores y ha llevado a los gobiernos a ofrecer incentivos financieros para asegurar estas nuevas fábricas. Pero Estados Unidos sigue con algunos problemas, los costos de poseer una nueva fábrica de chips son aproximadamente un 30% más altos que en Corea del Sur, Taiwán o Singapur, y son hasta un 50% más que en China, según el informe de la SIA.

Se proyecta que los fabricantes globales de chips destinarán 146 mil millones de dólares totales en gastos de capital este año, aproximadamente un 50% más que antes de que comenzara la pandemia y el doble del nivel de hace solo cinco años, según la consultora Global Gartner Inc.

LA TECNOLOGÍA AVANZA Y NO SE DETIENE

El mundo de los semiconductores se miden en nanómetros. Cuanto más pequeño es el transistor, más nueva y avanzada es la tecnología de proceso y mayor es la cantidad de microcontroladores que se pueden fabricar en una sola oblea de silicio. Los chips fabricados mediante el proceso de 28 nanómetros o más grandes generalmente se consideran chips heredados, y los números más altos indican tecnología más antigua. Los chips fabricados mediante procesos de nanómetros más pequeños se consideran avanzados y los chips más avanzados se producen en procesos de nanómetros de un solo dígito.



NANÓMETROS

Una oblea de cinco nanómetros para chips avanzados, que permiten que las aplicaciones se ejecuten en los últimos teléfonos inteligentes como el iPhone 13, se vende por alrededor de 17 mil dólares y este precio se compara con aproximadamente 3 mil dólares por una oblea de 28 nanómetros para semiconductores "heredados" que realizan funciones más simples, como conectar dispositivos a redes wifi.

La instalación de "salas limpias", necesarias para garantizar que los chips se mantengan libres de impurezas, puede costar 500 millones de dólares. Una sola máquina de fotolitografía, utilizadas en los diseños de chips en una oblea de silicio, puede alcanzar los 150 millones de dólares. Incluso los equipos de control de procesos pueden sumar 10 millones de dólares cada uno. Las últimas fábricas proyectadas pueden contener decenas de estas máquinas.

No es difícil concluir que sin microprocesadores se ralentizará la velocidad de avances en la economía mundial y una sólida inversión de capital será clave para garantizar que la recuperación de abastecimiento se mantenga firme en los próximos dos años. Mientras tanto, tendremos que aguardar la normalización de la situación, seguir resistiendo algunos aumentos de precios, administrar las demoras en las entregas y aguardar que la problemática en la logística mundial se regularice bajando nuevamente algunos costos que hoy están impactando negativamente en los precios de los productos terminados.

CHIP EN LA MANO

En simultáneo, las empresas proveedoras de seguridad electrónica tendrán el gran desafío de incrementar su eficiencia en los despachos de mercaderías, utilizando la tecnología de información de manera más agresiva, analizando más datos y pronosticando compras para abastecer en tiempo y forma a sus clientes. Por su parte, los compradores deberán estar atentos a la evolución de la crisis mundial durante este año, trabajar con *stocks* planificados y tener en cuenta los posibles incrementos de precios que puedan suceder durante 2022.

Sin dudas, el camino es acompañar la crisis minimizando lo más posible el impacto negativo que pueda ocasionar en cada uno de nuestros negocios. ■

Fotos: Garnet Technology

REFERENCIAS

- *https://www.wsj.com/articles/tsmc-to-build-chip-factory-in-japan-as-it-faces-surging-demand-11634207770*
- *https://www.wsj.com/articles/more-chips-will-be-made-in-america-amid-a-global-spending-surge-11637762400*
- *https://www.wsj.com/articles/tsmc-sony-to-open-7-billion-chip-plant-in-japan-in-2024-11636462339?mod=article_inline*
- *https://www.wsj.com/articles/semiconductor-industry-isnt-spending-big-on-scarce-old-tech-chips-11636453801?mod=article_inline*
- *https://www.wsj.com/articles/samsung-eyes-up-to-17-billion-u-s-chip-plant-investment-11611361050?mod=article_inline*
- *https://www.wsj.com/articles/the-world-relies-on-one-chip-maker-in-taiwan-leaving-everyone-vulnerable-11624075400?mod=article_inline*

Diego Madeo,
gerente comercial & MKT Latinoamérica de Garnet Technology.

Más sobre el autor:

GESTIÓN DE RIESGOS DE SEGURIDAD Y CIBERSEGURIDAD: ¿DESDE LA VÍCTIMA O DESDE EL ADVERSARIO?

"Cuando se combinan las dos visiones: víctima y adversario, se potencia un estado vigilante respecto de la comprensión y proyección de los riesgos y amenazas en el entorno cibernético, así como su evolución en el futuro próximo", Renaud & Ophoff

Foto: Creativeart - Freepik

COLOMBIA | Jeimy Cano

INTRODUCCIÓN

Los riesgos propios de la ciberseguridad y la seguridad de la información por lo general se atienden siguiendo los lineamientos de los estándares y buenas prácticas vigentes los cuales apuntan tradicionalmente al ISO 31000 de gestión de riesgos. Este ejercicio clave para asegurar los riesgos conocidos, se adelanta en perspectiva reactiva, toda vez que no sólo se conoce y hace el tratamiento de los riesgos, sino que se prepara a la organización cuando uno de ellos se materialice.

En este sentido, prácticas actuales como la del marco de ciberseguridad del NIST (identificar, proteger, detectar, responder, recuperar) (2018) se ubican en la perspectiva de la víctima que debe atender el evento adverso y donde el atacante tiene muchas certezas sobre el funcionamiento de su infraestructura y operaciones. Esto significa, que la aplicación de las prácticas estándares intrínsecamente buscan responder a los eventos adversos en la infraestructura sin considerar las intenciones o capacidades del adversario, análisis que se adelanta sólo si el ataque fue exitoso (si es que se hace).

En esta perspectiva pareciese que la organización sólo tuviese la opción de recibir y manejar los eventos adversos que le propone su atacante, dejando abierta la posibilidad de nuevos y novedosos ataques de sus posibles adversarios. Los marcos de trabajo en seguridad y ciberseguridad buscan prevenir los ataques, por lo general conocidos y documentados, lo que complica el ejercicio tradicional de la prevención, pues en la realidad, la innovación, la sorpresa y la novedad son la esencia de las propuestas de los adversarios.

Así las cosas, se hace necesario avanzar en plantear una gestión de riesgos cibernéticos desde la perspectiva del adversario. Esto es, comprender tanto las intenciones y sus capacidades (Martin, 2019) para salir de la zona cómoda de los estándares, y movilizar a la organización a otro marco de trabajo que busque detectar, disuadir, demorar, confundir y anticipar, para concretar una perspectiva más proactiva y prospectiva de la gestión, donde la organización estará más atenta a su contexto de operaciones, la protección de aquellos activos críticos que son de interés para un adversario, los comportamientos de las personas y sobremanera, una postura vigilante que mantenga una visión estratégica de la organización basada en su apetito de riesgo (Wucker, 2021).

Por tanto, esta breve reflexión desarrolla dos perspectivas de la gestión del riesgo de seguridad y ciberseguridad (desde la víctima y el adversario), con el fin de sintonizar los esfuerzos alrededor del tratamiento de los riesgos conoci-

Protectio

Seguridad Logística

NUESTRO PROVEEDOR DE CONFIANZA EN **SEGURIDAD LOGÍSTICA** ES PROTECTIO

"¡Pero es entre nosotros!
Porque la **Generación de Valor**
de Protectio a través de la Seguridad
es una ventaja competitiva
en el mercado."

EMPRESA SOCIALMENTE RESPONSABLE

COPARMEX
CIUDAD DE MÉXICO

AMESP

01 (55) 5639 1643 ó 5639 3574
contacto@protectio.com.mx
www.protectio.com.mx

dos y el desarrollo de capacidades para mantener una postura vigilante frente a los riesgos latentes y emergentes, que permita a la organización establecer una trayectoria en medio de los inciertos y la inestabilidad propia del contexto actual internacional.

DESDE LA VÍCTIMA

Esta es la perspectiva tradicional de la gestión de riesgos que busca ubicar una serie de sensores en la organización (que llamamos controles) los cuales se definen para que generen alertas de posibles eventos adversos y desde allí, iniciar la gestión del riesgo basado en la información que se genere por cuenta de los riesgos conocidos.

Esta lectura de la gestión de riesgos supone una reacción por parte de la empresa, para atender los posibles eventos que están ocurriendo y adelantar las acciones necesarias para su tratamiento. Nótese que mientras no se generen alertas el sistema de gestión no se activa para avanzar en el conocimiento de lo que ocurre en el entorno. Así las cosas, mientras más fino y mejor calibrado esté el control mejores alertas se pueden tener para avanzar en la identificación y aseguramiento del posible riesgo.

En la literatura especializada esta postura se denomina defensa pasiva (Cai et al, 2016). Un ejercicio basado en un conjunto de dispositivos y mecanismos tecnológicos que monitorean y se actualizan sobre las tendencias de amenazas y ataques con el fin de alertar a la organización sobre estas temáticas, y así mantener la confiabilidad de la infraestructura, basados en patrones conocidos, nuevas técnicas reportadas o actualizaciones de firmas en los "appliance" instalados en los centros de datos o en la Nube.

Cuando una organización sustenta su gestión de riesgos desde la perspectiva de la víctima es claro que estará preparada para enfrentar la inestabilidad y el evento adverso conocido. Podrá movilizar activar el protocolo identificar, proteger, detectar, responder, recuperar, y el equipo de atención de incidentes para identificar, contener, actualizar y erradicar el riesgo que se ha materializado, para luego de un examen forense de lo que ha ocurrido, poder capitalizar las lecciones aprendidas y efectuar los ajustes del caso tanto en la infraestructura como en los procedimientos de la organización.

La gestión del riesgo cibernético y de seguridad de la información en perspectiva de "atacado", reitera la vista del marco de calidad conocido como PHVA (Planear, Hacer, Verificar y Actuar), que si bien, permite mantener una vista repetible y previsible sobre un escenario con variables conocidas, es reactivo a las condiciones emergentes del entorno, donde no tiene otra opción que activar su protocolo de "análisis de causa-raíz", con el fin de entender lo que ha pasado, cómo ha afectado a la organización y qué correctivos debe hacer para incorporar a su práctica actual (Cano, 2020).

Avanzar en la gestión de riesgos y el marco de calidad, puede llevar a la organización a entrar en la zona de la "falsa sensación de seguridad", donde el adversario es capaz de desarrollar una inteligencia confiable sobre la dinámica de la organización, así como de la forma en que asegura los riesgos concretos de seguridad en sus diferentes productos y servicios. De esta forma, logra tener un cúmulo de información bien documentada y consistente desde donde puede estudiar rápidamente cómo crear la distracción y el engaño para crear la inestabilidad necesaria que le permita luego concretar su pivote de acción y desplegar el ataque concreto sobre un activo crítico específico (Cano, 2021).

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

ES VIABLE A TRAVÉS DE LA CONSTRUCCIÓN DE ESCENARIOS CREAR UNA VENTANA DE APRENDIZAJE, UNA "CAJA DE ARENA" DONDE ES POSIBLE EXPERIMENTAR Y EXPLORAR POSIBILIDADES SITUADAS EN LA DINÁMICA DE LA ORGANIZACIÓN, CON EL FIN DE AUMENTAR LA CONSCIENCIA SITUACIONAL CIBERNÉTICA

DESDE EL ADVERSARIO

Cuando se cambia la perspectiva de la gestión de riesgos ahora desde el adversario, la organización debe mantener lo que sabe hacer frente a los riesgos y amenazas conocidas, y salir a explorar nuevas posibilidades para comprender mejor quién es su adversario y qué capacidades tiene. Si bien esto no va, limitar o cambiar las intenciones del atacante, sí es viable crear una disuasión creíble que le permite moverse de un objetivo inicialmente previsto a otro (Martin, 2019).

Mientras la gestión de riesgos desde la víctima responde a una perspectiva mecánica de causa-efecto, la perspectiva desde el adversario es eminentemente sistémica, esto es, sensible al contexto, interconectado, interdependiente y con efectos en cascada. Es reconocer que el atacante desarrolla una mirada abierta y fina de la interacción y el acoplamiento de los diferentes elementos de la infraestructura, con el fin de producir el máximo daño con el mínimo de esfuerzo.

El adversario puede producir un evento adverso en el ciberespacio, como puede ser la liberación de código malicioso con capacidades inéditas: multiplataforma, polimórfico, cifrado, con mecanismos de autodestrucción (si es detectado) e hipercontagio, el cual llega a una infraestructura tecnológica (bien local o en la Nube) donde se propaga de forma acelerada, y que termina por penetrar todos los nodos visibles desde dicha infraestructura, quedando activo en unos equipos y pasivo en otros, con el fin de darle confianza al equipo de atención de incidentes por el tratamiento del evento, e invisibilidad posterior al adversario sabiendo que tiene pivotes disponibles para validar el comportamiento de la red y poder concretar una acción más silenciosa, anónima e invisible al radar de los controles instalados (Forscey et al, 2022).

En este contexto, la gestión de riesgos debe salir a explorar el entorno, consultar los datos disponibles del monitoreo actual, utilizar algoritmos de inteligencia artificial no supervisados para encontrar anomalías, reconocer y reflexionar los pronósticos de seguridad disponibles a la fecha, capturar las alertas tempranas de riesgos emergentes y sobremanera ubicar las tensiones geopolíticas que son relevantes para el desarrollo de los negocios de la empresa (Reeves et al, 2022).

Con estos insumos la gestión de riesgos de seguridad y ciberseguridad deberá avanzar en:

- **Detectar:** alertas tempranas basadas en la identificación de señales débiles del entorno que se deberán cruzar con las tendencias consolidadas y allí encontrar espacios en blanco desde donde pueden avanzar los adversarios.
- **Disuadir:** incorporando tecnología de blanco móvil o decepción con el fin de deteriorar la inteligencia previa del adversario y así aumentar su nivel de incierto, lo que obliga al agresor a repensar su estrategia frente a un objetivo inicial.
- **Demorar:** creando zonas de distracción para el adversario, donde este pueda perder mucho tiempo tratando de penetrar la infraestructura o cambiarle las prioridades en su plan de ataque.
- **Confundir:** cambiando la configuración de la infraestructura de forma dinámica, con el fin de crear mayor incierto en su modelo de riesgos y así, llevarlo a que pueda dar pasos en falso y exponer su identidad.
- **Anticipar:** habiendo aplicado las etapas anteriores se tiene un marco de trabajo donde es viable ver la trayectoria y el movimiento del adversario en la infraestructura, lo que habilitar un espacio concreto para interceptarlo antes de que tenga éxito.

VÍCTIMA Y ADVERSARIO

Si se establece una vista complementaria de las dos perspectivas de la gestión de riesgos, es necesario crear una zona de conversación convergente que permita tener voz y voto a los riesgos conocidos propios de la dinámica de la organización, así como para los riesgos emergentes. Esta zona la literatura la denomina diseño y análisis de escenarios. Un ejercicio de construcción colectiva donde la mirada está puesta no en los riesgos en sí mismos, sino en el contexto donde pueden ocurrir los eventos, para lo que se hace necesario reconocer los retos de la organización, los posibles adversarios y las buenas prácticas que se tienen a la fecha (Cano, 2020).

Desde la práctica de escenarios es posible convocar diferentes voces y perspectivas de los ejecutivos, de la gerencia táctica y el aseguramiento de la operación, como una vista consolidada que piensa en los posibles eventos y efectos que pueden tener para la organización. Desde esta perspectiva, se consolida una vista integral del riesgo que sale de la zona técnica y se traduce en posibilidades que terminan ocasionando impactos negativos en la organización. La ciberseguridad y la seguridad se traducen en narrativas que aumentan la consciencia situacional de la organización frente a un entorno cada vez más FANI: Frágil, Ansioso, No lineal e Incomprensible (Cascio, 2020).

Cuando se combinan las dos visiones: víctima y adversario, se potencia un estado vigilante (que puede alcan-

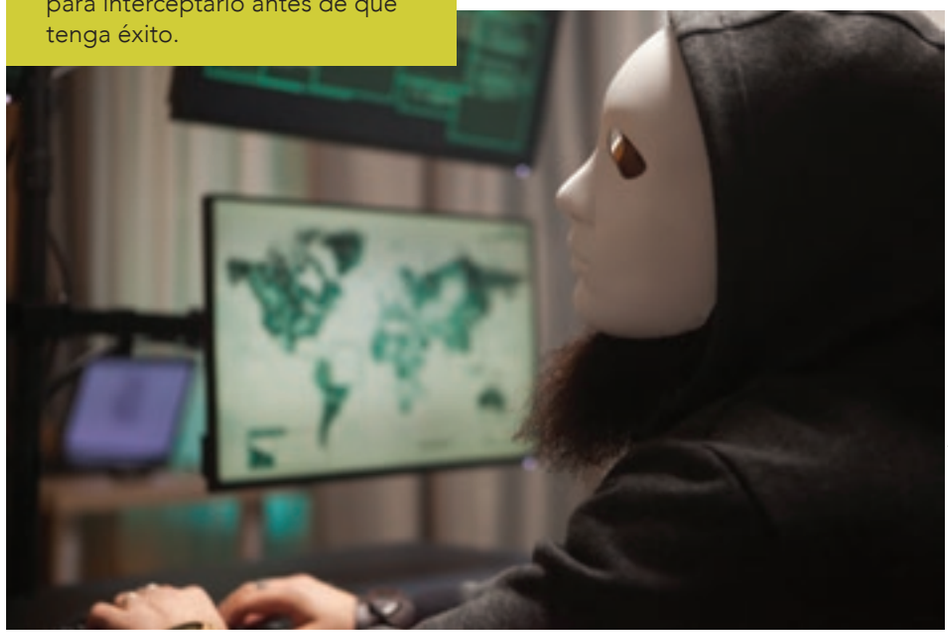


Foto: Creativeart - Freepik

zarse en un grado variable) respecto de la comprensión y proyección de los riesgos y amenazas en el entorno cibernético y su evolución en el futuro próximo (Renaud & Ophoff, 2021). Esto es, una apropiación del riesgo a nivel corporativo, que liderado desde los ejecutivos del primer nivel logra permear la organización en sus diferentes niveles. Nada de esto se puede concretar, sin una apertura a ver las cosas distintas, sin incomodar los saberes previos y experimentar el incierto como insumo para aprender/desprender.

Conectar las dos visiones permite no sólo establecer qué es un comportamiento normal y esperado de una plataforma tecnológica, sino reconocer los comportamientos y acciones de las personas frente a una amenaza, con el fin de crear conciencia y precauciones frente a posibles eventos que puedan ser reconocidos como anormales. La participación de múltiples perfiles y experiencias en el desarrollo de los escenarios habilitan espacios de reflexión y proactividad que desmitifican el riesgo de seguridad y ciberseguridad, para situarlo en la cotidianidad de las operaciones.

Adelantar el diseño y análisis de escenarios es habilitar una plataforma de aprendizaje/desaprendizaje donde todas las perspectivas suman, todas posibilidades son permitidas, con el fin de construir, desde los objetivos y retos estratégicos de la compañía, el filtro requerido que defina el marco de trabajo y discusión relevante para aunar esfuerzos en la defensa de la empresa frente a posibles adversarios conocidos y desconocidos, así como frente a contextos de inestabilidad posibles y probables donde la organización debe trazar un rumbo en medio de un mar de incertidumbres (Cano, 2020).

REFLEXIONES FINALES

Adelantar la gestión de riesgos de seguridad y ciberseguridad no es un ejercicio que tiene una sola mirada. Es una dinámica que requiere no sólo la perspectiva tradicional de la víctima que se prepara para un incidente, sino el reto que implica salir de la zona cómoda de los estándares, y situarse en el territorio del adversario para aumentar la incertidumbre en su modelo de riesgos. Si bien la gestión de riesgos en perspectiva del marco de trabajo logra identificar, proteger, detectar, responder, recuperar ha demostrado avances y logros sobresalientes en diferentes empresas a nivel global, se hace necesario movilizar los esfuerzos para complementar la vista desde las capacidades e intenciones del adversario, como una forma de mantener una postura vigilante y no sólo reactiva, que impulse la dinámica empresarial y desarrolle las capacidades necesarias de acuerdo con el apetito de riesgo de la empresa.

De esta forma, es viable a través de la construcción de escenarios crear una ventana de aprendizaje, una "caja de arena" donde es posible experimentar y explorar posibilidades situadas en la dinámica de la organización, con el fin de aumentar la consciencia situacional cibernética (Renaud & Ophoff, 2021) en la cotidianidad misma de la organización, sin sesgos tecnológicos o especializados, donde cada persona puede reconocer los impactos y los efectos de un evento adverso como parte de la forma como se deben entender y gestionar los riesgos de seguridad y control en el desarrollo de sus actividades.

Cuando se suman las dos perspectivas: la víctima y el adversario, la organización avanza en una posición de resiliencia organizacional, donde es capaz de definir sus umbrales de operación, reconoce cuál es su nivel de tolerancia al riesgo, qué tanta capacidad tiene para absorber la materialización de un evento adverso y sobremanera, cómo mantendrá las operaciones a pesar de haber sido impactado por evento adverso (Denyer, 2017). La preparación y exigencia para responder y recuperarse que se adquiere en la aplicación de los estándares y buenas prácticas, debe ser complementada con las capacidades necesarias para reconocer el adversario y enfrentarlo en su propio terreno.

Las organizaciones que quieran avanzar en medio de las tensiones actuales y enfrentar la incertidumbre propia del riesgo cibernético, no sólo deben atender las recomendaciones y exigencias de los estándares, sino abrirse a tomar riesgos de forma inteligente y calculada, lo que en el fondo implica "una capacidad para evaluar adecuadamente las probabilidades y posibilidades de la materialización de un evento no deseado y sopesarlo con las percepciones, teniendo en cuenta las alertas tempranas, las tendencias consolidadas y los mejores pronósticos, así como los aspectos emocionales que puedan influir en la decisión final"(Wucker, 2021). ■

CUANDO UNA ORGANIZACIÓN SUSTENTA SU GESTIÓN DE RIESGOS DESDE LA PERSPECTIVA DE LA VÍCTIMA ES CLARO QUE ESTARÁ PREPARADA PARA ENFRENTAR LA INESTABILIDAD Y EL EVENTO ADVERSO CONOCIDO

Foto: Creativeart - Freepik

Jeimy Cano, CFE, CICA,
miembro fundador del Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho de la Universidad de los Andes.

Más sobre el autor:

Tracking® Systems de México S.A. de C.V.

Recuperación 98.5%
Aviso en menos de 30 minutos*

Soluciones Integrales para RASTREO SATELITAL

EXPERTOS EN:

- Prevención y seguridad
- Logística
- Tráfico
- Reparto
- Cadena de suministro

- **24 años** de experiencia como líderes en el sector
- Más de **25 mil equipos** instalados
- Infraestructura sustentada por **AWS** y **Azure**
- Contamos con puntos estratégicos en todo el país
- Atención y soluciones personalizadas

Contáctanos
55-5374-9320

Socio Amesis
amesis.org.mx

amesis

*APLICAN RESTRICCIONES, ALGUNOS EQUIPOS /ACCESORIOS REQUIEREN ACTUALIZACIONES Y/O CONFIGURACIONES ESPECIALES.

TRUST ID

VERIFICACIÓN Y CERTIFICACIÓN DE PERSONAL

¿Estás seguro de quién maneja tu Logística?

EN 10 MINUTOS CERTIFICA A TU OPERADOR EN CONFIANZA

Somos una empresa dedicada a la validación de personal logístico como: **Operadores, Monitoristas y Técnicos Instaladores**. Nuestro proceso de verificación y certificación de los datos del personal es rápido y confiable.

- PROCESOS ULTRA RÁPIDOS
- ACEPTADA EN LOS PRINCIPALES CEDIS
- ID DIGITAL CON QR
- PROCESO EN LÍNEA DESDE TU SMARTPHONE
- LISTAS NEGRAS

- Análisis de datos de confianza en línea.
- Validación Fotográfica.
- Análisis de contenido en declaraciones.
- Estudio Socioeconómico / Sociolaboral.
- Validación de Antecedentes Laborales, Penales, Civiles y Mercantiles.
- Listas Negras a Nivel Mundial, entre otros.

DESCARGA LA APP

55 5374 9340 55 4141 6451 trustid.mx

SEGURIDAD EN *DATA CENTERS* Y TI

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Incendios, inundaciones, humedad, cambios de temperatura o diseño mal aplicado, son sólo algunos de los riesgos a los que están expuestos los Centros de Datos, sin dejar de lado los ataques intencionados

En la actualidad la vida se divide en dos categorías: física y virtual, lo que en ambas siempre debe estar presente es la seguridad, además de un espacio en donde habitar. Los *Data Center* (centros de datos), es la instalación física que resguarda y centraliza los sistemas informáticos de una empresa (ordenadores, redes, almacenamiento y otros equipos de TI). En todo el mundo existen distintos centros de datos, los cuales alojan información y equipo sumamente delicado e importante. Los Centros de Datos son también un facilitador para interconectar, de manera digital a los participantes de diversas industrias y sectores.

Los Centros de Datos, al ser infraestructura crítica, tienen diversos riesgos en materia de seguridad, mismos que se convierten en un reto que debe ser atendido.

Ya sean accidentales o intencionales, algunos de estos son: subidas o caídas de energía eléctrica, incendios, inundaciones, humedad, temperaturas incorrectas en los equipos, ya sea por instalaciones no adecuadas o mal diseño, vandalismo, uso inadecuado del equipo, entre otros.

Para mitigar algunos de estos riesgos es de suma importancia contar con un buen sistema eléctrico y de climatización. La información que en éstos se alberga debe estar protegida por equipo robusto, con mantenimiento constante y proveniente de una empresa que cuente con las instalaciones e infraestructura adecuada, de lo contrario, los riesgos se acrecientan.

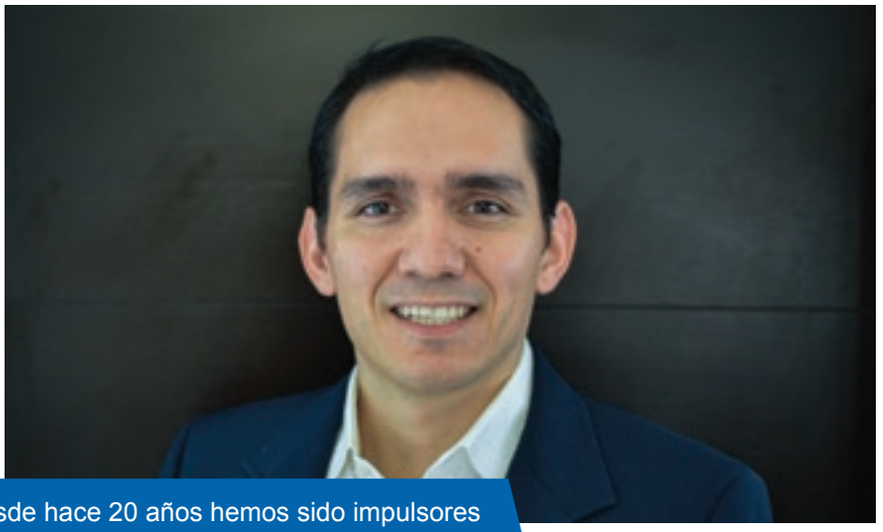
KIO NETWORKS

KIO Networks es una empresa referente en el mercado latinoamericano en Infraestructura de Centros de Datos y Tecnologías de la Información (desde 2002). Actualmente cuenta con más de 40 Centros de Datos distribuidos en México, Centroamérica, el Caribe y Europa, y su principal objetivo es "usar la tecnología para mejorar la vida de todos".

"Hemos desarrollado a un equipo de más de mil 900 personas altamente calificadas y certificadas que les permite brindar el mejor servicio basado en experiencia, mejores prácticas y conocimiento tecnológico, logrando una excelencia operativa", comentó Alejandro Ríos, director de Tecnología en KIO Data Center.

"Hemos desarrollado a un equipo de más de mil 900 personas altamente calificadas y certificadas que les permite brindar el mejor servicio basado en experiencia, mejores prácticas y conocimiento tecnológico", **Alejandro Ríos**

Foto: Creativeart - Freepik



"Desde hace 20 años hemos sido impulsores de ecosistemas digitales caracterizados por su alcance y diversidad", **Alejandro Ríos**

SERVICIOS DE TI DE MISIÓN CRÍTICA Y ALTA DISPONIBILIDAD

- **Centro de Datos:** cuenta con más de 40 Centros de Datos con características en 11 campus tecnológicos con servicio de alta disponibilidad y clase mundial para el acceso a múltiples ecosistemas de interconexión. "Nuestro objetivo es proporcionar los más altos niveles de disponibilidad en el servicio de cualquier empresa, bajo un ambiente de redundancia operativa y máxima seguridad. Nuestros Centros de Datos están ubicados en cinco países: México, Guatemala, Panamá, República Dominicana y España con infraestructura de la más alta tecnología".

- **EDGE Data Center:** son centros de datos distribuidos estratégicamente en diferentes territorios para acercar la información de la empresa a sus clientes, reduciendo la latencia, mejorando el desempeño y logrando experiencias más rápidas y eficientes. EDGE *Data Center* está diseñado para las empresas que requieren tener su información en diferentes ubicaciones para estar más cerca del usuario y de las zonas de alta transaccionalidad.

- **Soluciones de Nube (pública, privada e híbrida):** esta es una herramienta indispensable para mantener almacenada, disponible y a salvo la información que el negocio genera día con día. Debido a sus características, una de sus aplicaciones es que permite el trabajo colaborativo, ya sea a través del correo electrónico, plataformas de trabajo en línea y acceso a otras nubes geográficamente dispersas y nubes globales, por mencionar algunos de los ejemplos.

- **Ciberseguridad:** KIO Networks está enfocado en ofrecer servicios preventivos para el cuidado de la información que van desde el diagnóstico hasta la consultoría, para ofrecer respuestas proactivas y reactivas ante la posibilidad de una amenaza, que incluyen aspectos como administración de *firewalls* (WAF), administración de antivirus, administración de web; todo con el respaldo de los más altos estándares y el apoyo por parte de ingenieros expertos en ciberseguridad.

- **Automatización Robótica de Procesos (RPA):** reducen la dependencia necesaria del talento humano hoy aplicado en operaciones rutinarias programables. Muchas herramientas de inteligencia artificial y robótica están disponibles para repensar las funciones del negocio.

- **Plataformas de *e-commerce*:** enfocadas en incrementar la densidad de clientes y aumentar las ventas a través de servicios como: consultoría para establecer la correcta estrategia y plataformas más adecuadas para cada negocio. Dentro de este contexto, más y más negocios requieren moverse al comercio electrónico y resulta que hasta un 70% de ellos no tiene una plataforma de *e-commerce* para hacerlo.

- **Inteligencia Artificial:** contamos con soluciones de Inteligencia Artificial (IA) que permiten identificar en tiempo real anomalías, predecir eventos y tomar acciones en servicios, aplicaciones, infraestructura y sistemas físicos. Éstas analizan bitácoras, métricas y sensores por medio de algoritmos de Machine Learning.

VALORES AGREGADOS

"Desde hace 20 años hemos sido impulsores de ecosistemas digitales caracterizados por su alcance y diversidad, lo que nos permite ofrecer diferentes ventajas de interconexión con otros jugadores del ecosistema, mejor desempeño de redes, en un entorno seguro, eficiente y ágil", señaló Alejandro.

El contexto actual muestra la importancia de la infraestructura tecnológica para una organización, por eso KIO Networks ofrece soluciones de acuerdo a las necesidades específicas de industrias e instituciones: desde Colocación, soluciones Multi-tenant, así como facilitar la interconexión entre operaciones de mismas o diferentes empresas, de manera rápida, óptima, segura y con una baja latencia, lo que se traduce en mayor eficiencia a menores costos.

Algunos de los beneficios de la firma son:

- ✓ **Alta disponibilidad:** ofrecemos continuidad de negocio, disponibilidad y seguridad, a través de arquitecturas redundantes, una excelencia operativa al gestionar infraestructura de clase mundial y ubicaciones con la más alta tecnología.
- ✓ **Neutralidad:** contamos con un modelo enfocado en la neutralidad, permitiendo que todo tipo de industria y/o cliente sea bienvenido a nuestro ecosistema.
- ✓ **Ecosistemas digitales y *marketplace*:** gracias a la neutralidad en nuestras operaciones, ofrecemos el más grande y diverso ecosistema de proveedores de servicios hospedado en nuestros Centros de Datos, lo que nos permite ofrecer diferentes ventajas de interconexión con otros jugadores del ecosistema, las principales Nubes públicas y líderes de la industria.
- ✓ **Certificaciones y estándares internacionales:** contamos con una serie de certificaciones que nos permiten generar confianza entre nuestros clientes, por ejemplo: ICREA 6, nivel que certifica tanto de forma individual como grupal a una robusta red de *Data Centers* de alta disponibilidad interconectados entre sí para garantizar una redundancia distribuida.
- ✓ **Protección contra desastres.** Contamos con un plan de recuperación ante desastres que nos permite restablecer los sistemas y la información de la empresa cuando se produce un incidente que afecta a cualquier servicio.

DELL TECHNOLOGIES

Dell Technologies es otra de las firmas que desarrolla soluciones para los centros de datos que ayudan a sus clientes a automatizar la TI (Tecnología de la Información), obtener flexibilidad, movilidad del ecosistema de nubes múltiples e innovar de manera segura.

"Nuestro portafolio comprende diferentes productos de *hardware* y *software* de almacenamiento, servidores, infraestructura convergente, protección y respaldo de la información que se adecuan a las diferentes necesidades de los clientes para darles la velocidad, calidad y eficiencia necesaria para enfrentar los desafíos del mercado. De igual forma, contamos con servicios de consultoría y con soluciones integradas de tecnología para el Centro de Datos que ayudan a nuestros clientes a integrar ambientes multinube; gestionar sus datos en el borde; contar con una gestión más inteligente y ágil de sus datos; entre otros, todo siempre considerando un ambiente de seguridad de los datos", compartió Mario Huelga, director de Ventas de Centro de Datos en Dell Technologies México.

"Nuestro portafolio comprende diferentes productos de *hardware* y *software* de almacenamiento, servidores, infraestructura convergente, protección y respaldo de la información que se adecuan a las diferentes necesidades de los clientes", **Mario Huelga**

Recientemente, Dell incorporó el portafolio APEX que ofrece tecnología como servicio o as a Service (aaS) en donde el cliente paga únicamente por la tecnología que consume, de esta forma se reducen los costos de inversión y la empresa va definiendo la tecnología que requiere de acuerdo con sus necesidades.

"En México contamos con el brazo financiero que proporciona Dell Leasing México, mejor conocido como Dell Financial Services, lo que nos permite apoyar a nuestros clientes para que puedan adquirir la tecnología que requieren del portafolio de Dell Technologies con opciones de financiamiento y soluciones de consumo flexibles: los clientes pueden utilizar tecnología que requieren en servidores, hiperconvergencia, almacenamiento y protección de datos*", explicó Mario.

Foto: Creativeart - Freepik

> "En México contamos con el brazo financiero que proporciona Dell Leasing México, mejor conocido como Dell Financial Services, lo que nos permite apoyar a nuestros clientes para que puedan adquirir la tecnología que requieren del portafolio de Dell Technologies con opciones de financiamiento", **Mario Huelga**

RIESGOS DE SEGURIDAD

El experto nos compartió los principales riesgos de seguridad a los que están expuestos los *Data Centers*:

- **Ciberdelincuencia:** el objetivo de los cibercriminales es acceder a los datos, hoy son el activo más valioso de las organizaciones.
- **Obsolescencia de los equipos y sistemas:** es decir, no modernizar los equipos o soluciones del Centro de Datos incluyendo almacenamiento, servidores, sistemas de administración y/o de climatización, soluciones de conectividad y seguridad.
- **Errores del personal (factor humano o *humanware*):** cuanto más complejo es el sistema, más vulnerable se vuelve el "elemento humano" y más capacitación/aprendizaje se requiere para operar la instalación.
- **Fallas en el acceso o disponibilidad de la información:** esto es un riesgo que además conlleva grandes pérdidas económicas debido al tiempo de indisponibilidad y que se puede ocasionar debido a errores de configuración, mal funcionamiento de los equipos o a causa de distintos tipos de ataques (DDoS) o *malware*.

VENTAJAS COMPETITIVAS

De acuerdo a Mario Huelga, una de las ventajas competitivas más grandes de Dell Technologies es su sólida cadena de suministro y la amplia red de canales que permite llegar a más empresas para ayudar a las organizaciones a acelerar su Transformación Digital sin importar su tamaño. Es importante tener conocimiento y toda la información necesaria al momento de seleccionar un aliado tecnológico para el Centro de Datos, a continuación el experto nos comparte los 5 tips para contratar sin errar en el intento:

1. **Alinear el área de TI con los objetivos de negocio:** es muy importante tener claridad en los objetivos que el negocio busca alcanzar para que con base en ellos se defina qué tecnología es la más adecuada para su Centro de Datos.
2. **Determinar el tipo de aplicaciones que se utilizarán por el negocio:** esto ayudará mucho a definir los equipos de *hardware* y *software* que se requerirán para que las aplicaciones corran de manera eficiente, ágil y segura.
3. **Definir la infraestructura más adecuada para el Centro de Datos:** es muy importante considerar dónde estará localizado en Centro de Datos; las necesidades de energía y enfriamiento que requieren; considerar los sistemas de respaldo de energía necesarios en caso de falla, considerar los equipos necesarios de respaldo en caso de fallas o de daños por desastres; así como tener un buen diseño de cableado para evitar futuros contratiempos o interrupciones.
4. **Establecer una estrategia de seguridad y protección de la información:** es importante establecer estrategias de seguridad tanto física como lógica para el *Data Center*: en cuanto a seguridad física, considerar el control de acceso a las instalaciones, sistemas de videovigilancia, protección contra incendios y asegurarse de que esté ubicado en una zona con poco riesgo de desastres naturales. Respecto a la seguridad lógica, es necesario contemplar un plan de recuperación de archivos, así como la seguridad que debe abarcar desde el perímetro de los *Data Centers* hasta los dispositivos en el Edge como PCs y estaciones de trabajo, pasando por *switches* y *routers*.
5. **Actualización constante del Centro de Datos:** debido a las exigencias del mundo digital y el ritmo con el que nuevas tecnologías se desarrollan, es importante contar con equipos y soluciones que ayuden al negocio a mantenerse operando a su máxima capacidad, en un entorno de máxima seguridad y lista para admitir e implementar nuevas aplicaciones y mayores cargas de trabajo. Para esto es necesario contar con el equipo, infraestructura y soluciones de vanguardia. ■

**Soluciones de financiamiento a través de Dell Leasing México S. de R.L. de C.V. ("DLM") entidad comercial, no autorizada a actuar como institución financiera en México.*

Columna de
Enrique Tapia Padilla, CPP
etapia@altair.mx

Socio Director, Altair Security Consulting &Training.

Más sobre el autor:

LATINOAMÉRICA

¿TENEMOS A NUESTROS EJECUTIVOS PROTEGIDOS?

(PRIMERA PARTE)

Hace unas semanas me invitaron para dictar una conferencia en el *Roadshow* de **Seguridad en América**, misma que denominé como el título de esta entrega. Disfruté mucho esta intervención. A la vez que disertas, también miras con nuevos ojos, es un aprendizaje continuo.

En nuestro día a día, es poco placentero pensar en los riesgos que existen a nuestro alrededor, pero dejar de pensar en ello no va a hacer que los riesgos se vayan. Al momento de proteger a una persona es entender lo extenso que abarca el término seguridad: proteger la integridad de las personas, el patrimonio y la imagen, así como garantizar la continuidad de las operaciones.

Es claro que al hablar de proteger a la alta dirección, tenemos que referirnos a la conformación de un Plan de Seguridad para ellos. Para ello y para marcar el rumbo propondría un objetivo principal que pudiera ser, brindar un soporte de protección ante los diferentes riesgos a los que pudiera estar expuesta la persona, otorgando medidas de prevención y protección, evitando así ser víctimas de la delincuencia y/o, en caso de suceder, minimizando los impactos consecuenciales.

EVALUACIÓN DE RIESGOS COMO INICIO

Por supuesto que todo punto de partida comienza con un levantamiento de información, análisis, evaluación y diagnóstico, para estar claros en dónde estamos parados y de qué los tenemos que proteger.

En este caso iniciar con una evaluación de riesgos (de la residencia y oficina, así como sus entornos; del ambiente familiar, traslados y lugares de visita frecuente), considerando al menos los siguientes tópicos:

- **Ubicación geográfica:** es claro que los riesgos no serán los mismos dependiendo de las locaciones donde se encuentran las personas y/o las instituciones que representan. Si la persona está en España o en México; si está en México, si sus movimientos

> Valorar el *modus operandi* de los delincuentes y sus motivos, será de gran apoyo para definir adecuadamente los riesgos a los que están expuestos

Foto: Creativeart - Freepik

por ejemplo, son principalmente en Yucatán o en Quintana Roo, incluso dentro de las mismas ciudades en Latinoamérica, donde con el paso de áreas geográficas pueden cambiar drásticamente y con ellos las condiciones de seguridad.

- **Naturaleza del ejecutivo y/o empresa:** ¿Es funcionario público o ejecutivo de un corporativo global? ¿Cuál es la naturaleza de la institución donde opera? ¿tiene familia o no, es soltero o casado? ¿cuáles son sus pasatiempos y sus intereses?

- **El adversario:** valorar el *modus operandi* de los delincuentes y sus motivos, será de gran apoyo para definir adecuadamente los riesgos a los que están expuestos:

  - ¿Quiénes lo hacen?
  - ¿Cómo operan?
  - ¿Cuándo lo hacen?
  - ¿Dónde lo hacen?
  - ¿Cuáles son sus fines?
  - ¿Qué les interesa de nosotros?

- **Análisis del personal actual:** incluir al menos el análisis de colaboradores cercanos (personal doméstico, jardineros, choferes y escoltas u otros), así como el análisis de los colaboradores de oficina cercanos al ejecutivo.

- ***Benchmarking:*** este tema es medular al momento de estar en la planeación del dispositivo. Acercarnos con nuestros similares a nivel nacional e inlcuso internacional para conocer las mejores prácticas, que nos permitan un marco de referencia.

Los riesgos no serán los mismos dependiendo de las locaciones donde se encuentran las personas y/o las instituciones que representan

- ¿Cuáles son los Programas Corporativos/Institucionales en temas de protección de personas?
- ¿Están utilizando vehículos blindados, vehículos convencionales o de bajo perfil?
- ¿Utilizan conductor, escoltas, personal armado y/o desarmados?
- ¿Incluimos a la familia o no en el esquema de protección?
- ¿Qué niveles jerárquicos son los que incluimos en nuestro plan y bajo qué consideraciones?
- ¿Cuáles son los criterios que utilizan para la protección de la residencia/oficina y otros inmuebles frecuentados?
- Entre muchos otros más.

Con todo lo anterior, emanará la detección de necesidades de seguridad, así como una serie de recomendaciones y estrategias de prevención y protección en el orden de infraestructura, recursos humanos y procesos, mismos que darán pie al Plan de Seguridad del Ejecutivo y su familia, para lograr así un Sistema Integral de Seguridad Personal. Pero esto será tema de nuestra siguiente edición, nos leemos pronto.

¿Cuál es tu opinión? Cuéntamelo en mi correo: *etapia@altair.mx* o a través de LinkedIn: *https://www.linkedin.com/in/enriquetapiapadilla/*. ■

Columna

EL TIGRE TIENE RAYAS

ballesteros.barrera@hotmail.com

Más sobre el autor:

Omar A. Ballesteros, director general y CEO de Ballesteros y Barrera Servicios de Protección.

ASOCIACIÓN NACIONAL DE EMPRESARIOS DE SEGURIDAD PRIVADA

MÉXICO

Foto: Cortesía Omar Ballesteros

¡Saludos, amigos! Siempre es un placer hacerles llegar otra vez mi columna "EL TIGRE TIENE RAYAS", que como bien saben son temas de liderazgo en la superación de sus empresas y siempre enfocado a que logren sus metas mediante la orientación de sus equipos de trabajo.

En esta ocasión les comparto una entrevista que me hicieron los amigos de MEGACABLE TV acá en la ciudad de León, Guanajuato.

Reportera Fátima (RF): ¿Cuál es su nombre y cargo dentro de la asociación?
Omar A. Ballesteros (OB): mi nombre es Lic. Omar Alejandro Ballesteros G., presidente de la Asociación Nacional de Empresarios de Seguridad Privada.

RF: ¿Cuántas empresas conforman la A.C.?
OB: 30 empresas y contando.

RF: ¿Cuál es el principal reto que tienen las empresas de hoy?
OB: siempre es un gusto participar en las entrevistas de los amigos de Megacable, y hoy más que nunca es la situación económica del país, donde la presencia de un panorama desalentador en el desarrollo y crecimiento de nuestros clientes, lleva a que nosotros ajustemos nuestros precios a costos menores absorbiendo la inflación y disminuyendo nuestras utilidades, además de que la competencia desleal de empresas del ramo que no están regularizadas y se encuentran fuera de la ley y reglamento en cualquier nivel del gobierno.

RF: ¿Por qué la situación económica del país les afecta?
OB: nos afecta, porque nuestros costos deben estar ajustados conforme las leyes fiscales y ahora con el *outsourcing* (REPSE - Registro de Prestadoras de Servicios Especializados u Obras Especializadas), nos obliga a tener más gastos no previstos y esto lleva a aumentar nuestros precios para poder estabilizarnos, sin embargo, los clientes no quieren pagar nuestros precios ajustados a todo esto, y quieren y buscan más baratos, y las empresas gandallas aprovechan esto dando más baratos y de peor calidad. Afectan nuestra imagen y profesionalismo.

RF: ¿Cuántas empresas de la A.C. se encuentran fuera de norma o no están regularizadas?
OB: ninguna, es requisito estar en regla.

RF: ¿La fianza que establece el gobierno del estado y por ahora la ciudad de León, cómo les afecta o cómo consideran este requisito?
OB: es un requisito que marca la ley, en el caso del Gobierno de Guanajuato, se requiere tanto el refrendo como por primera vez, pero en el caso de la ciudad de León, solamente es el tramite de primera vez, aunque el Gobierno de León, mas en su representación de la Dirección de Regulación, hay errores de interpretación de su propio reglamento.

RF: ¿El REPSE está siendo un problema para las empresas de hoy, dentro de la A.C.?
OB: cada empresa tiene que hacer su trámite, las que tiene que solucionar los requisitos que marca la ley,

deben ponerse al corriente si tienen algún crédito, pero en realidad nadie de la A.C. se ha pronunciado con alguna dificultad en el tema.

RF: en días pasados el Secretario de Seguridad Pública de León, Mario Bravo Arrona, comentó que varias empresas no están cumpliendo con el registro en la ciudad, ¿usted qué opina de su declaración?
OB: las empresas registradas en la A.C. están al día y tenemos copia de sus permisos.

RF: ¿Ustedes representan a todas las empresas de la ciudad o el estado?
OB: representamos a quien quiere ser presentado.

RF: ¿Considera que la autoridad está sobrepasando sus funciones?
OB: sí, porque el reglamento municipal es muy claro en sus apartados, pero la Secretaría de Seguridad Pública de León trata de interpretar la ley conforme les conviene, pero no es el caso con el Estado, es muy clara.

RF: ¿Considera que hay favoritismos en la Secretaría de Seguridad de León, con algunas empresas?
OB: ¡Claro! Solamente hay que ver que en el Consejo de Seguridad Privada Municipal, solamente hay cuatro empresas y todas son parte del partido del municipio, nadie de la A.C. las conoce.

RF: ¿Qué están haciendo ustedes como A.C. para apoyar a sus agremiados?
OB: tenemos un departamento legal que nos está dando toda la asesoría, además de amigos dentro del municipio que nos apoyan en los temas relativos a nuestro giro, curiosamente no tenemos problemas en ningún otro municipio del estado, sólo León no quiere hacer equipo de trabajo, pero seguimos abiertos al diálogo.

RF: ¿Cómo les afecta la inseguridad actual?
OB: a todos nos afecta, pero si puedes ver las cifras, curiosamente están lesionando más policías que guardias de seguridad privada, nuestro personal no es motivo de agresión en la calle, como le pasa a la policía, ellos sí tienen muchos problemas en el tema, y digo verdaderos problemas.

Nosotros tenemos una red entre las empresas, donde todos nuestros supervisores dan atención a todos los clientes de todos nuestros agremiados en caso de incidentes, cualquier supervisor cerca de cualquier cliente de las empresas de nuestro gremio atiende la emergencia a cualquier hora, esto da la certeza del apoyo con una respuesta más rápida. En cambio, la policía tiene menos unidades que nosotros, y su tiempo de respuesta es superior a 20 min. mínimo.

En robos está desbordado, en las empresas de nuestra A.C. los robos no están altos, pero a empresas como calzado Charly, donde se robaron 30 millones de pesos (un millón 467 mil dólares) con tres tráileres cargados de mercancía, si pasa.

> Tenemos un departamento legal que nos está dando toda la asesoría, además de amigos dentro del municipio que nos apoyan en los temas relativos a nuestro giro

RF: ¿Cuántos elementos de seguridad tienen ustedes dentro de todas las empresas agremiadas?
OB: más de tres mil.

RF: ¿Pueden ustedes garantizar darle respuesta a sus clientes en caso de un incidente?
OB: claro que sí, ¡y siempre!

RF: ¿Las pruebas de control y confianza, les sirven a ustedes o les afecta, debido a que tienen que hacer un gasto exigido por la ley?
OB: en realidad, nos sirve.

RF: ¿Qué otros servicios otorgan las empresas de seguridad con ustedes? ¿Solamente personal privado?
OB: claro que no, tenemos empresas de todo: investigaciones, custodia de tráileres, guardias de seguridad privada en perfil básico sin armas, personal armado (registrado en la SEDENA – Secretaría de Defensa Nacional), cursos y capacitaciones en seguridad privada y prevención de accidentes, además de cursos de liderazgo en seguridad privada, asesoría-consultoría, inteligencia-contrainteligencia, y más.

RF: ¿Considera su Consejo que pueden haber empresas del ramo que tomen ventaja de ustedes?
OB: no hay forma, nadie puede ingresar a la A.C. sin primero ser aprobada su solicitud por el Consejo.

RF: hemos sabido que las patrullas de policía han levantado guardias por no estar registrados, ¿a cuántas de sus empresas les ha pasado eso?
OB: ninguna.

Nosotros tenemos una red entre las empresas, donde todos nuestros supervisores dan atención a todos los clientes de todos nuestros agremiados en caso de incidentes

RF: ¿Si hubiera un debate con la Secretaría de Seguridad Pública en relación al tema de la seguridad privada, aceptarían?
OB: si el debate fuera sobre las ventajas de hacer equipo de trabajo con nosotros en lugar de tomar su posición de inquisición, ¡claro que sí!

RF: ¿Los fraccionamientos se han quejado de las empresas de seguridad asegurando que son más problema que solución?
OB: los fraccionamientos privados o clústeres, tienen más problemas dentro de su estructura, que los que dicen que ocasionamos, no aceptan nuestras recomendaciones, y los mismos colonos ocasionan los problemas de robo, y muchos de los robos los facilitan ellos, por ejemplo, dejan las "bicis" de sus hijos en el frente de la casa sin protección y cualquiera las puede tomar. Y eso lo reportan al comité del fraccionamiento y queda como queja culpándonos a nosotros, donde hay problemas de personas externas queriendo robar se reportan siempre a la policía en tiempo, pero no tiene capacidad la autoridad y llegan siempre después de 30 minutos.

RF: ¿Cuál es la percepción de inseguridad de ustedes?
OB: superior al 80%.

RF: ¿Saben ustedes que vienen cambios en la ley federal y que serán ellos quienes lleven ahora la observancia del gremio?
OB: Sí, siempre es lo mismo, pero estaremos preparados.

RF: como siempre, presidente, es un gusto nos acepte nuestras entrevistas, ¿alguna declaración adicional de su parte?
OB: ¡Gracias a ustedes! Por tomarnos en cuenta y reconocer nuestra asociación, invitamos a todas las empresas del Estado y de la nación que busquen crecimiento y representación en el estado de Guanajuato, que se acerquen con nosotros, tenemos algo para solucionar sus problemas. ■

Foto: Creativeart - Freepik

FREEMATICA
Business technologies

El mejor software de gestión de horarios para Empresas de Seguridad Privada

Simplifica tu día a día. Descubre el ERP e-Satellite®

La elección de las grandes Empresas para la gestión y control de horarios.

El sistema líder de gestión end-to-end en formato Cloud y SaaS

Automatiza la planificación de horarios y cuadrantes con el software de gestión de cuadrantes y turnos *e-Satellite® de Freematica*.

¡Empieza la transformación digital de tu empresa; gestiona y organiza la rotación de tu personal para obtener mayor eficiencia y rentabilidad!

- + GESTIÓN
- + CONTROLES
- + AUTOMATIZACIÓN
- + USABILIDAD
- + FACTURACIÓN
- + PRENÓMINA
- + INFORMES
- + Kpi 's

freematica.com

EXPO SEGURIDAD MÉXICO 2022:
EL PUNTO DE ENCUENTRO MÁS SEGURO DE LATINOAMÉRICA

Los pasados 28, 29 y 30 de junio se llevó a cabo la décima novena edición de Expo Seguridad México, evento que reunió a más de 10 mil asistentes por día y un sinfín de tecnología e innovaciones de esta industria

MÉXICO

Mónica Ramos y Tania G. Rojo Chávez / *Staff* Seguridad en América

Con más de 300 expositores albergados en casi siete mil metros cuadrados del ya tradicional Centro Citibanamex (CDMX), Expo Seguridad México 2022, en su décima novena edición logró el éxito esperado por sus organizadores, entre ellos Jorge Hagg, director de dicho evento, y quien compartió escenario en la ceremonia de inauguración con Luis Wertman Zaslav, Comisionado del Servicio de Protección Federal; Myriam Urzúa Venegas, secretaria de Gestión Integral de Riesgos y Protección Civil, y el Comisario Jefe, Dr. Hermenegildo Lugo Lara, subsecretario de Inteligencia e Investigación de la Secretaría de Seguridad Ciudadana (CDMX).

Expo Seguridad México y Expo Seguridad Industrial se llevaron a cabo los días 28, 29 y 30 de junio, en ellas se mostraron los avances tecnológicos, soluciones y productos más novedosos, a los usuarios, integradores, distribuidores nacionales e internacionales y al público en general. Además de diversas conferencias impartidas por expertos en temas como control de accesos, videovigilancia, ciberseguridad, seguridad pública y privada.

Las marcas más reconocidas en el mercado, presentaron los avances tecnológicos y las tendencias a nivel mundial en este sector, además expertos en la materia, impartieron conferencias, hubo demostraciones, *networking*, y eventos especiales como la firma de Convenio entre la Asociación Mexicana de Blindajes Automotores (AMBA), y Agrupaciones de Seguridad Unidas por México (ASUME). Este año más los 10 mil 834 visitantes únicos, pudieron aprovechar todas esas actividades, RX Global organizador del evento, ya se encuentra alistando desde este momento la vigésima edición de Expo Seguridad México planeada para el mes de abril (2023). A continuación mostramos algunas de las marcas presentes este año.

Jonathan Avila, *Country Manager* para Everbridge en México y Centroamérica

"Mostramos nuestra plataforma de gestión de eventos críticos que tiene un alcance muy amplio para sumarizar: es inteligencia de riesgos, notificación masiva, gestión de crisis y seguridad física. Nuestra misión es unir el mundo físico de los dispositivos físicos con el mundo digital y fuentes de información. Al día de hoy, la mayor cantidad de clientes que están en el sector financiero, un 70% de las instituciones financieras en México, utilizan nuestra plataforma para distintos eventos. Nuestra plataforma es ágil, está lista en la Nube para ser utilizada".

Enrique Gonzalez, Gerente de Ventas en Securi-Mart

"Esta ocasión presentamos soluciones de detección de incendio de la marca Edwards Signaling; Control de Acceso con la marca Lenel; CCTV con la marca Pelco de Avigilon, y también manejamos los equipos de Alvarado con puertas giratorias y torniquetes".

Evamely Bravo, *Regional Sales Manager* de ISS para el centro y sureste de México

"Trajimos muchas soluciones nuevas porque nuestro *software* cambió de versión hace unos meses, de la 10 a la 11. En toda la historia de nuestro *software* SecurOS, es la primera vez que tiene tantas mejoras, una de ellas por ejemplo es Auditrel, que audita cada una de las transacciones hechas por un monitorista, entonces es un producto que ya viene embebido en la plataforma y permite que los supervisores puedan tener ese paso a paso en esta nueva versión, entre otras más".

Marcos Pérez, gerente de Cuentas Clave para la zona de Bajío de Moldex

"Nosotros somos la segunda empresa más grande del mundo en protección respiratoria y auditiva para la industria, hacemos lo que comúnmente llaman 'mascarillas', que no son más que filtros de aire para que el flujo de éste que está entrando al cuerpo humano, entre realmente bien filtrado. Por ejemplo, protegerlos de polvos, humos o neblinas, gases y vapores, sobre todo en la industria. El ruido también tiene que ser atenuado o bajado de frecuencias para que no lastime la parte auditiva, pueden ser tapones desechables o reutilizables y orejeras especiales, las cuales también trajimos a mostrar".

Camila Tapias, especialista en Resilience Global; y **Brian Kruzan,** *Senior Analyst*

"Nosotros tenemos tecnología para preparar a diferentes instituciones, tenemos una plataforma llamada Planet Reading, en donde hacemos capacitaciones y diferentes evaluaciones para universidades, empresas, gobiernos, para diferentes tipos de desastres, por ejemplo en México preparación en caso de terremoto; en general ofrecemos planeación para que sean resilientes y estén preparados para diferentes desastres".

Nelson Gutiérrez, gerente comercial para Latinoamérica y Centroamérica en Miguel Caballero

"Miguel Caballero tiene 30 años en el mercado, de los cuales 15 con presencia en México, desarrollamos, producimos e implementamos elementos de protección personal especializada enfocada a proteger la vida del ser humano. Tenemos una camiseta que se llama Armor T-Shirt, es una prenda patentada de uso interno, protege contra municiones de acuerdo a la N.I.J 0101.06, está certificada y es una prenda liviana que se adapta a la ergonomía de cada usuario".

Mauricio Guijarro, *Sales VP Latam & Caribbean* en Veri·das

"Nosotros presentamos soluciones bajo el concepto de Phygital, el cual consiste en la validación de información de los usuarios tanto en el mundo físico como digital, reconociendo tanto una cara, una voz, como una combinación entre éstos. Es decir, lo que nosotros hacemos es decirte que en el mundo digital y en el mundo físico de una manera voluntaria y segura, tú eres tú, y así evitar los ataques de tipo suplantación".

Jesús Armendáriz, departamento de Ingeniería en PTTPRO

"En PTTPRO ofrecemos soluciones desde equipos portátiles y económicos para cubrir pequeñas empresas hasta equipos digitales que se pueden utilizar para una consola de despacho, y equipos móviles que se pueden utilizar en vehículos, soluciones para emergencias o equipos de rescate. Actualmente en México tenemos en uso una solución en despacho en la iniciativa privada, además tenemos una mancuerna de radios y soluciones DMR, que está a prueba con Bomberos de la Ciudad de México".

GRUPO EMPRESARIAL CASA

SEGURIDAD PRIVADA

CUSTODIA

INTRAMUROS

CONSULTORÍA

SEGURIDAD PRIVIDAD | INTRAMUROS

www.gecsa.com.mx

info@gecsa.com.mx

www.facebook.com/gecsa

www.twitter.com/gecsa

www.youtube.com/gecsa

Tel: (55) 5373-1761 | (55) 5363-2868

Calle Limoneros 9-A,
Col. Valle de San Mateo,
C.P. 53240, Naucalpan de Juárez,
Edo. de México

Gustavo Estrada Rosales, gerente de Ventas en México de PG Products

"PG Products es una empresa fabricante de vidrio blindado, vidrio de resistencia balística y para Expo Seguridad México trajimos una camioneta BMW X3 blindada de origen con vidrios PG Products, también colocamos una exhibición de vidrios simulando cómo son montados dentro de un vehículo. Somos la única empresa que te puede ofrecer los vidrios blindados con acero incrustado en todos y cada uno de los componentes que forman parte del kit de vidrio, desarrollos tecnológicos en los parabrisas para que siga funcional toda la zona de sensores".

Carlos Santamaría, director de Ventas *Retail* de ZKTeco

"En esta Expo nos estamos enfocando en dos plataformas: la primera en la Nube es BioTime para gestión de asistencia, en lugar de utilizar un servidor como antes lo usábamos, estamos haciendo toda la centralización dentro de una Nube privada. Y la segunda sería la plataforma ZKBio CVSecurity, en donde estamos incorporando visión computarizada, son prácticamente los mismos módulos que manejábamos antes: control de acceso, asistencia, control de personal, acceso vehicular, inspección, visitantes, elevadores, pero ahora con integraciones de cámaras de vigilancia y paneles de control de acceso de otras marcas".

Flavio Domínguez, gerente de Desarrollo de Negocio de RedGPS

"RedGPS es una empresa de plataformas de *software as a service* marca blanca para empresas de rastreo y telemetría que ofrecen gestión de flotas y control de activos, por ejemplo flotas de camiones, generadores de energía, cualquier otro tipo de activos de puedan ser rastreables puede generar telemetría o posicionamiento. Traemos los últimos desarrollos que estamos liberando, por ejemplo un copiloto virtual, que es una aplicación puramente desarrollada para prevención de riesgos en minería y nuevas funcionalidades en nuestras *apps* móviles".

Luis Henrique Ribeiro de Placido, CEO de Fulltime México

"Para Expo presentamos una aplicación llamada FullCond para las centrales de monitoreo de condominios, la cual cuenta con Control de Acceso con amenidades conjuntas con paquetería. Desde la aplicación móvil usted podrá hacer uso y administrador de todas estas herramientas. Muchas veces se hace manual, entonces traemos un *software* con una aplicación para transformar este proceso en uno más automatizado. También presentamos Eficient para las ciudades inteligentes, con esta aplicación la municipalidad podrá ofrecer a sus habitantes de la zona, un aplicativo, una botonera electrónica que contiene botones de alerta".

Humberto Villegas Rizo, director general de Alse Mexicana

"Estamos presentando muchas soluciones para centros penitenciarios, tenemos las cerraduras en certificación penitenciaria y en esta ocasión especialmente presentando por primera vez al mercado la cerradura penitenciaria con tecnología IP, que dará mucha información a los usuarios de los movimientos de la cerradura, cuándo se abrió, cuándo se cerró, cuándo se abrió con llave, la temperatura, cuántas veces se ha usado para los mantenimientos, da un número muy grande de parámetros y de información. Y tenemos muebles de baño con un ahorro del 80% en el consumo del agua".

João Ilhéu, ejecutivo de Negocios Internacionales para Latinoamérica de VMI Security

"Tenemos nuestra línea de equipos de rayos X de inspección no intrusiva, trajimos un equipo con un túnel de 55 por 36 metros que tiene una integración de detección de metales Garrett, que un mismo operador pueda manejar los dos equipos en simultáneo, que en la pantalla de rayos X pueda ver la zona de inspección del detector de metales".

José Luis Rodríguez, ingeniero de Marca de la línea Bosch en TVC en línea

"Nosotros como empresa mayoritaria tenemos muchas marcas de todo tipo, como cámaras análogas, IP, analíticos, torniquetes, barreras, detectores de metal, etc. Traemos a la Expo un equipo contra incendio, es de la nueva serie de Bosch llamada Avenar de la serie 2000, sistemas de voceo de Bosch, tenemos los torniquetes de ZKTeco, barreras vehiculares, arcos detectores, soluciones de Dahua, sistemas de alarma, manejamos la marca DSS y Vivotek".

Luis Saavedra Sol, gerente regional de Ventas de Johnson Controls México

"Este año estamos presentando soluciones de seguridad integradas, en esta ocasión dándole más peso a las cámaras a la inteligencia artificial en video para poder clasificar personas, vehículos, objetos que tengan las personas, como maletas, pistolas, o alguna situación que pueda poner en riesgo la operación o a las personas que estamos protegiendo. En protección perimetral traemos radares con alcance de 250, 500 o hasta mil metros para poder detectar de forma preventiva intrusiones y poder reaccionar a tiempo antes de que la persona ya esté adentro o el vehículo. En control de acceso traemos reconocimiento de códigos QR para visitantes y reconocimiento de placas".

Mauricio Meza, director de Producto para América Latina en Hanwha Techwin

"Toda la tecnología y el *line up* de Hanwha para toda Latinoamérica, pero resaltando la Inteligencia Artificial dentro de las cámaras, ese es nuestro *core* de negocios hoy, porque estamos seguros que ese es el futuro de la videovigilancia, pero en general de las soluciones basadas en video. La aplicabilidad de las soluciones de Hanwha es tan diversa que puedes reinventarte y generar nuevos mercados, pero al día de hoy es muy natural pensar en *retail*, por ejemplo, en vigilancia ciudadana, transporte, educación y corporativos".

Mauricio Swain, director de Ventas para la región de Latinoamérica de Milestone Systems

"Presentamos nuestro *release* #2 que es X-Protect, todas las diferentes soluciones que ofrecemos y de las novedades más importantes que traemos para este año es el XProtect Rapid REVIEW, que es un plug-in que ayuda a que las búsquedas forenses sean mucho más inteligentes, por ejemplo si queremos detectar quién fue la persona que en su momento tuvo algún percance, con características como ropa, si es mujer u hombre; se puede hacer la búsqueda y el algoritmo te va a mostrar a todas las personas que cumplen con esas características".

Rogério Coradini, director de Ventas PACS en Brasil para HID Global

"Presentamos nuestra línea de lectores y soluciones de identidad seguras para HID para el mercado de México y Latinoamérica con un enfoque especial para la solución de Mobile Access, que transforma la credencial física en virtual, que puede utilizar su *smartphone* para acceder a las áreas seguras de la compañía o áreas que requieren un nivel de seguridad más alto".

Tatiana Bolívar, directora de Ventas de la División de Impresoras para América Latina de HID Global

"Presentamos dos productos: uno es una tecnología nueva de impresión para tarjetas o credenciales plásticas, esta nueva tecnología es impresión de inyección de tinta, puede imprimir en cualquier tipo de tarjeta y mostramos también nuestra solución de impresión en la Nube, es una solución que le da la funcionalidad de imprimir a plataformas de *software* que pueden ser de control de acceso o manejo de bases de datos de empleados".

Saúl Sebastián Salazar Lima, capitán de la sucursal de Querétaro, México, para PPA

"PPA (Puertas y Portones Automáticos) es una empresa brasileña especializada en soluciones de seguridad para cocheras, controles de acceso. Nuestro mercado principal es para herreros, alumineros, electricistas, integradores, arquitectos. Es un conjunto muy grande, desde personas que inician poniendo cámaras de seguridad y a la vez les piden la automatización, es la gente a la que nosotros queremos llegar. También manejamos cercas eléctricas e Internet de las cosas con varios equipos".

Arturo Flores Guadarrama, director comercial de OmniCloud

"Presentamos las soluciones de servicios en la Nube, como video y sistema de alarmas PSIM 100% *Cloud*. El producto estrella son los tótem, que son equipos para seguridad pública donde tenemos dos cámaras, una sirena y un botón de pánico para atención de incidencias al público en general conectadas al C5 de la Ciudad de México".

ASOCIACIONES DE SEGURIDAD

Además de los fabricantes y proveedores de soluciones de seguridad, en Expo Seguridad México también estuvieron presentes las diferentes asociaciones de seguridad, quienes acompañan, respaldan, benefician y capacitan día con día, a esta industria como ANERPV, AMESP, ALAS, ASIS Internacional, entre otras. A continuación algunas de las asociaciones que entrevistamos.

MSPV
SEGURIDAD PRIVADA

GUARDIAS INTRAMUROS

CUSTODIA DE TRASLADO DE MERCANCÍAS

GUARDIAS DE MEDIOS ELECTRÓNICOS

ISO 9001:2015

Contáctanos

55 5399 9937 ext. 846 | 800 2530717

ventas@mspv.com.mx www.mspv.com.mx

MSPVCorporativo MSPVSeguridad

Manuel Zamudio, presidente de Asociación Latinoamericana de Seguridad (ALAS) Comité Nacional México (2° periodo)

"En ALAS queremos retomar las actividades presenciales sin dejar de aprovechar lo que nos otorgan los medios digitales, es decir acercarnos de nuevo de forma física a nuestros socios y hacer ese *networking* de manera más personal, cercano y constante. Además, continuamos con los temas de capacitación, y todo el portafolio que tenemos en ALAS en seguridad electrónica, también aumentar nuestra participación con otras asociaciones".

Esteban Hernández López, presidente de la Asociación Mexicana de Blindajes Automotores (AMBA)

"El objetivo de la AMBA es dar un certificado de calidad, una garantía a los clientes de que compren vehículos que sean blindados por una de las compañías de AMBA, con la certeza de que son vehículos protegidos adecuadamente con materiales certificados con áreas de coberturas garantizadas con un contrato que respalde estos servicios".

Erika Rodríguez, supervisora comercial de Sistemas Información Satelital perteneciente a ANERPV

"Pertenecer a la Asociación Nacional de Empresas de Rastreo y Protección Vehicular (ANERPV) brinda además, la seguridad a nuestros clientes de que somos una empresa certificada, que contamos con el apoyo de una asociación tan importante y que con esto logramos tener el acercamiento con todas las autoridades a nivel nacional. Una de las grandes ventajas de pertenecer a la ANERPV es el contacto con las autoridades, la ANERPV nos brinda todo ese apoyo, y gracias a la plataforma Centinela hemos tenido más casos de recuperación de éxito a nivel nacional".

Herschel Schultz Chávez, director general de ASUME

"Estamos en una fase pos pandémica y esto involucró que las más de 30 asociaciones que representamos en todas las modalidades de seguridad privada, empezáramos a reactivar todas las actividades. Hemos trabajado con las autoridades para el tema de la coordinación específicamente en tres aspectos: uno, prevención del delito; dos, legislación, estamos impulsando la promulgación de la Nueva Ley General de Seguridad Privada que permita la homogenización de todas las reglamentaciones que hay a nivel municipal, estatal y federal, para combatir además la irregularidad e ilegalidad de las empresas que no cumplen con los requisitos de la ley. Y tres, la profesionalización, capacitación, dignificación y la Cámara Nacional de la Industria de la Seguridad Privada".

Héctor Manuel Romero Sánchez, presidente de Círculo Logístico

"Nuestra asociación está muy enfocada a toda la cadena de suministro: logística, distribución y transporte, desde que entra la materia prima hasta que llega a su lugar de destino. Estamos trabajando con parques logísticos, centros de distribución, dueños de mercancía, transporte, operadores logísticos. Nos enfocamos en la profesionalización del transporte, ya que está compuesto por el 80% hombre-camión, micro, pequeño y mediano empresario. Hoy estamos viendo un problema muy fuerte en la cadena de suministro, con diferencias de costos para los consumidores, cosa que no habíamos previsto, de ahí la importancia del análisis de riesgos y la continuidad del negocio". ■

Fotos: Mónica Ramos y Tania Rojo / SEA

Más que una empresa de seguridad...

SOMOS GRIP

- Traslados VIP
- Protección Ejecutiva
- Gripers (Especialistas en Seguridad Intramuros)
- Capacitación en Manejo de Armas de Fuego
- Auditoría y Consultoría
- Análisis de Riesgos
- Análisis de Confianza
- Vigilancia, Detección de Vigilancia y Contravigilancia

CERTIFICADOS ISO 9001:2015

redconocer · ASIS · CNS · AMESP · EXECUTIVE PROTECTION SUMMIT 2022

www.grip.mx

GRIPsecurity · soygriper · Global Risk Prevention

124 años OFRECIENDO soluciones

#SOYGRIPER

Río Frío 143, Colonia Magdalena Mixhuca, Alcaldía Venustiano Carranza C.P. 15850 CDMX

Tel. 55 5335 1632 / 55 4336 4090

¿SABES CÓMO SE HA EXTENDIDO LA SEGURIDAD PRIVADA EN MÉXICO?

Foto: Creativeart - Freepik

El sector de empresas de seguridad privada cuenta con alrededor de seis mil empresas en toda la república mexicana, integradas por al menos 500 mil elementos de seguridad

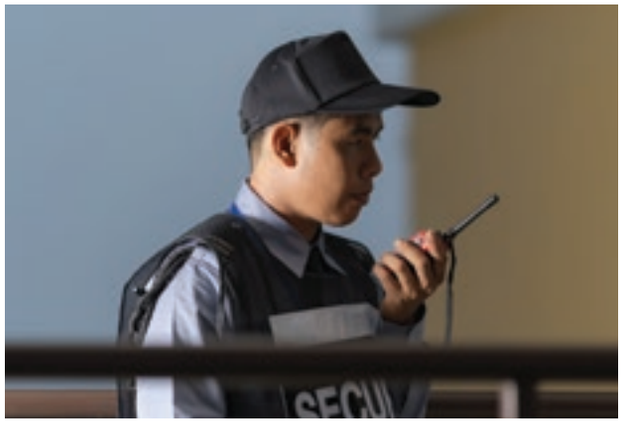


Foto: Creativeart - Freepik

MÉXICO

Angel Kociankowski

Fue allá por la lejana década de los años 70, cuando se registró el inicio de las empresas de seguridad privada en México con apenas cuarenta empresas, que buscaban atender la necesidad de protección que empezaba a expresarse por parte del sector privado, en vista de que la seguridad pública no contaba con recursos suficientes para enfrentar las nuevas modalidades de delito, y su aumento, y para resguardar a toda la sociedad.

Dando un gran salto en el tiempo, tenemos que en la década de 1990 la Ciudad de México aprobó un reglamento que responsabilizaba a la Procuraduría General de Justicia del Distrito Federal para gestionar el registro de los servicios de seguridad privada, con lo que empezaron las regulaciones para las empresas participantes.

Posteriormente, el sector inició su crecimiento a partir de la crisis económica de 1994, cuando se registró cierto aumento en el índice delictivo; en esa época se empezaron a registrar anualmente alrededor de 150 empresas de esta especialidad, aunque de dimensiones y calificaciones desiguales. Ya para el año 2000 había cerca de mil 400 compañías de seguridad registradas.

Después, en el año 2006 se publicó la Ley Federal de Seguridad Privada, aunque las entidades federativas empezarían a contar con sus propias regulaciones para las empresas de seguridad privada, y entonces empezó a impulsarse aún más este campo.

Pero es importante señalar que la seguridad privada ha ido evolucionando conforme se ha desarrollado la economía del país, y ha pasado a considerarse más que como un producto, como un servicio, el cual representa un segmento económico vital en la economía del país, ya que de acuerdo con el Banco de México, el segmento de servicios ha estado creciendo constantemente hasta lograr un registro del 14% del PIB (Producto Interno Bruto) en 2015, aunque en 2011 bajó a 11%, a partir de la pandemia.

LA ENTIDAD EN QUE SE CONTABILIZA EL MAYOR PORCENTAJE DE EMPRESAS EN EL REGISTRO ESTATAL ES LA CIUDAD DE MÉXICO, CON 18.63 POR CIENTO, Y EN SEGUNDO LUGAR EL ESTADO DE MÉXICO, CON 10.32 POR CIENTO

EVOLUCIÓN Y ADAPTACIÓN

La industria de la seguridad privada entonces se ha ido adaptando a las nuevas condiciones del país y a las nuevas tecnologías, aunque igualmente han ido evolucionando los siniestros y las distintas modalidades de crimen que afectan al país. Por ello, la seguridad configura una industria que no puede permanecer estática, y debe mantenerse en una constante evolución.

Además, se trata de una actividad que se va adaptando constantemente y se está integrando cada vez más al cuidado del valor humano, con aplicación de tecnología moderna y orientándose también a la gestión de las medidas de protección a la salud. Aunado a ello, se están agregando más elementos de protección a la industria de la seguridad privada, para cuidar a la persona ante cualquier amenaza o riesgo, se trate de asuntos de crimen, protección civil o salud.

Es en ese entorno de nuevas prácticas que se ha dado un incremento en el sector, lo cual se ilustra con el dato de que de 2017 a 2018, el número de empresas con registro estatal creció de cuatro mil 207 a cuatro mil 466, y el personal operativo estatal pasó de 87 mil 583 a 85 mil 230 de 2016 a 2018. Y en cuanto a las empresas y el personal con registro federal, se ha registrado un incremento sostenido y para 2017 se contabilizaban más de mil doscientas empresas, con ocho mil 671 elementos.

La entidad en que se contabiliza el mayor porcentaje de empresas en el registro estatal es la Ciudad de México, con 18.63 por ciento, y en segundo lugar el Estado de México, con 10.32 por ciento, y como ambas entidades configuran una zona conurbada, resulta que una de cada cuatro empresas de seguridad privada se encuentra en esa área.

Así, encontramos que el sector de empresas de seguridad privada cuenta con alrededor de seis mil empresas en toda la república mexicana, integradas por al menos 500 mil elementos de seguridad, pero se calcula que entre dos mil 500 y dos mil 900 empresas de esta especialidad no están reguladas.

DE 2017 A 2018, EL NÚMERO DE EMPRESAS CON REGISTRO ESTATAL CRECIÓ DE CUATRO MIL 207 A CUATRO MIL 466, Y EL PERSONAL OPERATIVO ESTATAL PASÓ DE 87 MIL 583 A 85 MIL 230 DE 2016 A 2018

PRINCIPALES ENTIDADES CON EMPRESAS DE SEGURIDAD PRIVADA CON REGISTRO ESTATAL

Entidad	Año 2017	Año 2018
Ciudad de México	760	832
Nuevo León	422	461
Jalisco	240	294
Baja California	238	246
Guanajuato	168	192
Chihuahua	224	178
Puebla	152	173
Quintana Roo	146	162
Morelos	128	133
Coahuila	122	131

Registro Nacional de Empresas, Personal y Equipo de Seguridad Privada. Compendio de Datos 2018, elaborado por la Dirección General de Seguridad Privada.

Y en todo ese universo, es vital conocer cuáles son los factores que se deben tomar en cuenta para contratar a una empresa de seguridad, porque es evidente el crecimiento en el número de compañías y de personal, pero no todas han evolucionado en sistemas, procesos, tecnología y otros elementos, que solamente los más profesionales pueden ofrecer. ■

Foto: Creativeart - Freepik

Angel Kociankowski,
director comercial de Corporativo Ultra.

Más sobre el autor:

LA IMPORTANCIA DE LA CAPACITACIÓN EN SEGURIDAD PRIVADA

En esta ocasión, nuestro colaborador invitado explica todo sobre el tema y lo importante que es para el desempeño del guardia

MÉXICO | Hermelindo Rodríguez Sánchez

El conocimiento básico en vigilancia y seguridad privada es el fundamento que debe tener el personal que inicia en el gremio de la vigilancia para desempeñarse adecuadamente, siendo la formación uno de los aspectos de vital importancia para desenvolverse en el desarrollo de sus funciones, de tal forma que pueda cumplir con la finalidad de los servicios.

El personal de seguridad privada requiere, conforme lo establece la ley, tener una formación básica. A continuación, algunos temas como objetivo del plan de capacitación:

OBJETIVOS

Objetivo general: formación del personal de Protección y Seguridad Privada de nuestras organizaciones, a través de la capacitación para proteger a las personas, propiedades, entornos, información y otros, con criterios de: calidad, seguridad, salud, respetando la normativa vigente.

Objetivos específicos:

- Proporcionar al personal de Seguridad Privada las herramientas que le permita identificar, detectar, prevenir y actuar para minimizar riesgos de inseguridad en las instalaciones.
- Promover cambio de ideas y preceptos del guardia de Seguridad Privada, para mejorar el servicio y la imagen que proyecta hacia el cliente y sus compañeros.
- Mejorar la calidad de servicio con base en la capacitación continua del personal de seguridad, para el beneficio de la seguridad del cliente.
- Transmitir los conocimientos, los procedimientos, las normas, ética y valores de todo el personal de seguridad privada.

El personal que ingresa a las filas de la seguridad privada, lo hace muchas veces por necesidad, por ser la única opción laboral que encontró, cuando es puesto en servicio, recibe la inducción muchas veces del propio personal de vigilancia, ni el supervisor en ocasiones sabe cuál es el verdadero trabajo, sólo se concreta a decirle algunas instrucciones o consignas, peor no lo capacita adecuadamente, esto se lo deja al guardia que está en servicio en el lugar, o incluso al cliente que es quien le informa qué hacer al elemento.

Esto genera no sólo mala imagen y desempeño del servicio, afecta la imagen de la empresa y del servicio mismo, por ello es importante que el personal reciba una capacitación adecuada y ante todo lo involucre en la profesión a la que ha llegado. Capacitar es dar herramientas útiles y generar un buen servicio, brindando la garantía que se dará un buen servicio de protección.

En la actualidad vemos que la inseguridad ha rebasado el servicio que nos brinda la seguridad pública, por lo que es necesario contar con personal que proteja las personas, la información y las propiedades, ésta es una labor delicada y debe estar en manos de personal calificado, primero entendamos que no son policías, pero su labor es importante para salvaguardar el sitio donde laboran.

La preocupación por la seguridad es una de las características más notables de nuestra civilización. No podemos prevenir buena parte de amenazas existentes, por el alto grado de incertidumbre de muchos fenómenos naturales y sociales. La buena noticia es que en el ámbito seguridad privada se puede aplicar una metodología que reduce de forma drástica el riesgo y así contar con herramientas para la prevención. El funcionamiento de este sector está asociado a una explotación sistemática de fuerzas y fenómenos del mundo físico, cuyas leyes son bien conocidas y cuyos efectos se pueden predecir con precisión.

La vigilancia y Seguridad Privada expresa que la prestación de estos servicios se orienta a disminuir las amenazas que puedan afectar la vida, la integridad personal y el pleno ejercicio de los legítimos derechos sobre la propiedad y los bienes de las personas que reciban tales servicios, sin invadirlos ámbitos de competencia del Estado asignadas a la seguridad pública.

El guardia de vigilancia y seguridad privada es la persona encargada de precautelar la protección a las personas, propiedades (entorno) de la organización donde labora, teniendo a su disposición recursos físicos, organizativos y tecnológicos.

En este contexto se propone corregir la debilidad existente en los ámbitos de la formación, capacitación, especialización, gestión, control y evaluación de los guardias, orientando sus esfuerzos a la institucionalización y cumplimiento efectivo de su misión y la certificación como entes competentes para el ejercicio de su labor.

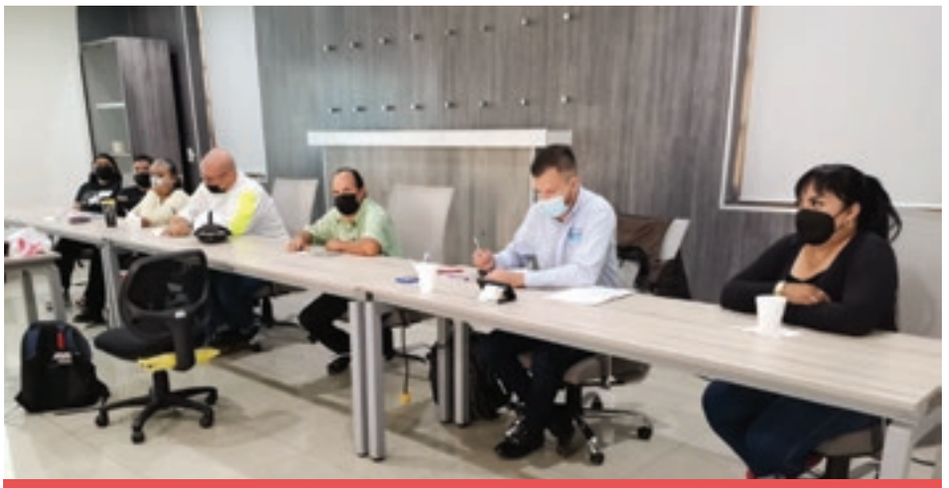
¿EN QUÉ TEMAS DEBEN CAPACITARSE?

Los requerimientos mínimos de los participantes en los procesos de capacitación son:

- Manejo de las operaciones fundamentales.
- Requisitos que demande la ley de seguridad y vigilancia.
- Lectura, escritura y comprensión de textos a un nivel básico.
- Realizar cálculos básicos de suma, resta, multiplicación, división.
- Comprometido con asumir la totalidad de la capacitación.
- Actitud para capacitarse.
- Buena predisposición para compartir los conocimientos con su entorno.

Una de las modalidades contempladas en la Ley Federal de Seguridad Privada es la seguridad intramuros, que es la que desempeñan los guardias, ya sea de empresas de seguridad o internos, y que son la primer imagen de atención al cliente, su desempeño y labor está encaminada a dar atención, prevenir pérdidas y disuadir cualquier acto de riesgo en perjuicio del cliente, son responsables de la protección a personas, información y propiedades, parte del desarrollo de los cursos, que a continuación se exponen:

- Cultura de legalidad, valores y ética.
- Derechos humanos de la Seguridad Privada.
- Conceptos básicos de la seguridad.
- Protocolos de operaciones en seguridad.
- Curso de seguridad integral.
- Primeros auxilios.
- Marco legal.
- Notas y reportes escritos.
- Técnicas de revisión corporal.
- Manual de emergencias.
- Amenaza de bomba.
- Límites de actuación.
- Manual de fundamentos operativos.



El desempeño y resultado de las funciones del guardia están ligadas a su formación y aprendizaje, el cual adquiere por medio de la enseñanza, capacitación, y actualización de conocimientos

El desempeño y resultado de las funciones del personal que desarrolla las labores de vigilancia y seguridad privada están ligadas a su formación y aprendizaje, el cual adquieren por medio de la enseñanza, capacitación, y actualización de conocimientos relacionados con la vigilancia y seguridad privada, que reciben en las escuelas de capacitación y entrenamiento.

En la labor de liderazgo (directores, jefes de seguridad) en compañías de Seguridad Privada, se realiza la medición del conocimiento de los vigilantes, desde el proceso de selección en entrevistas de conocimiento y en el ejercicio diario de la labor de los guardias; en estos escenarios se encuentra notoriamente vacíos académicos que posiblemente se deriven de la falta de asistencia a los cursos de conocimientos.

BENEFICIOS DE LA CAPACITACIÓN

La capacitación de los guardias es responsabilidad de la compañía de seguridad privada y debe realizarse para maximizar el desempeño general del guardia de seguridad. La formación de guardias de seguridad privados es una inversión que vale la pena pagar, porque traerá buenos beneficios para todos en un futuro.

La vida cotidiana de un guardia de seguridad puede ser impredecible y existe una gran diversidad de personas con las que interactúa todos los días.

Las responsabilidades de comunicación serán diferentes en cada turno. Algunos turnos requerirán una estrecha coordinación con el supervisor del guardia de seguridad de turno y otros días requerirán la cooperación de varias personas que pueden estar invadiendo o merodeando en la propiedad de un cliente.

El programa de capacitación de los guardias de seguridad se garantiza para que el personal comprenda la importancia de las habilidades sociales diseñadas para reducir las situaciones que pueden ser tensas y desagradables.

Para que un guardia de seguridad privada pueda desempeñar su función, debe haber recibido un curso de capacitación. En esta capacitación, es preparado en aspectos relacionados con funciones laborales, el manejo adecuado del público (relaciones humanas), reserva y ética profesional y valores, entre otros.

La capacitación de los mismos, crea en nuestros colaboradores, tácticas para prevenir acciones que sean de riesgo para el patrimonio de nuestros clientes. Estando siempre atentos a los detalles y alertas mientras trabajan, de esta manera, los oficiales de seguridad podrán reconocer y reportar cualquier incidente con inmediatez.

El personal de seguridad debidamente capacitado será más consciente de las situaciones potencialmente peligrosas que pueden enfrentar mientras se encuentran en el sitio del cliente. Tener esta habilidad permitirá al guardia de seguridad estar listo para tomar decisiones inteligentes rápidamente mientras está bajo presión.

Según las estadísticas, los guardias de seguridad capacitados tienen mayores tasas de productividad y efectividad. La capacitación hace que se vuelvan más atentos a los detalles y estén alertas mientras trabajan.

Con un mayor estado de alerta, los oficiales de seguridad podrán reconocer y reportar cualquier incidente, esto hará que también aumente la eficiencia de la comunicación. El entrenamiento del guardia de seguridad enseñará la importancia de una comunicación clara, concisa y fácil de entender, y su papel en operaciones de seguridad efectivas.

La capacitación adecuada de los oficiales de seguridad mejora, no sólo la inteligencia de nuestros miembros, sino, a su vez sus sentidos, permitiéndoles manejar más fácilmente las circunstancias de manera responsable y apropiada mientras están bajo coacción.

Tener la capacitación para tomar decisiones difíciles durante circunstancias estresantes no sólo aumentará la eficiencia del desempeño del guardia de seguridad, sino que también optimizará la seguridad de las empresas en las que brinda sus servicios.

El hecho de que la ley no tenga un requisito específico para la capacitación del guardia de seguridad, no significa que no deba completarse. ■

Fotos: Cortesía Hermelindo Rodríguez

Hermelindo Rodríguez Sánchez, CPO, CSSM, DSI, DES,
CEO / fundador de la Consultoría en Seguridad y Protección Integral (COSEPRI).

Más sobre el autor:

Tu seguridad, nuestra prioridad *con excelencia*

OSAO

Seguridad Electrónica

SERVICIOS OSAO

RASTREO SATELITAL | TECNOLOGÍAS GPS | CANDADOS
DRONES | VIDEOVIGILANCIA | CONTROL DE ACCESO

55 679 834 90

55 2430 8253

Info@osao.com.mx

Calle Pirules no. 7, Colonia Valle de San Mateo,
C.P. 53240 Naucalpan de Juárez

PROTOCOLOS EMPRESARIALES PARA SERVICIOS DE CALIDAD EN SEGURIDAD PRIVADA

Foto: Creativeart - Freepik

El protocolo en la actualidad tiene hoy un componente de organización imprescindible para la empresa que no quiera ser un ente aislado sin relación de ningún tipo. Es la herramienta que permite ordenar las relaciones sociales de la empresa, empleados y directivos

MÉXICO

Pablo Romero Navor / *Staff* Seguridad en América

Los protocolos de seguridad privada para empresas son más que un simple requisito legal dentro de la industria. Son, en cambio, medidas de seguridad interna, cuya aplicación permite resguardar al personal de una compañía mientras realiza su actividad económica, proteger la materia prima y los productos terminados, y defender las instalaciones privadas.

Se trata de un documento interno, que consigna los procesos —paso por paso— que deben seguirse dentro de determinada área industrial, para prevenir accidentes de seguridad y qué hacer en caso de que estos llegasen a presentarse.

Este documento debe, necesariamente, contener las acciones a seguir, pasos, procesos y normativas a ejecutar como acciones seguras, en cada una de las áreas de la compañía. Los protocolos de seguridad privada para el resguardo de personal, bienes o capital, se levantan a partir de las necesidades de seguridad específicas de cada empresa.

Normalmente, los protocolos de seguridad privada para empresas, parten desde la misma organización. No obstante, durante los últimos años, estos documentos han logrado nutrirse a partir de las leyes de seguridad industrial, vigentes en cada país.

Su planeamiento y ejecución es tan delicado, como los procedimientos que deben consignarse en él. Al elaborar este documento, la compañía garantiza que ante una situación de riesgo, se seguirán cuidadosamente los procesos ya establecidos, para atender cada tipo de irregularidad, proteger al personal y minimizar las pérdidas.

¿QUIÉN DEBE ELABORAR LOS PROTOCOLOS?

Todas las empresas debidamente constituidas, incluso aquellas con un número de personal bajo o niveles de producción reducidos, estén en el nivel de crear protocolos de seguridad para empresas.

En consecuencia, pese a que muchos protocolos de seguridad para empresas se elaboran dentro de la misma compañía, la verdad es que éstos deberían ser ejecutados bajo la asesoría de expertos, específicamente de una empresa de seguridad.

Muchos expertos han considerado que el protocolo de seguridad para empresas es fundamental para salvar vidas dentro de la compañía, proteger la materia prima y minimizar el riesgo de perder productos terminados o maquinaria. De manera que, si te preguntas cómo hacer un protocolo de seguridad, siempre debes considerar cuáles son tus riesgos potenciales.

Un protocolo de seguridad dentro del área privada es, en consecuencia, una manera práctica de garantizar el orden interno y externo de la empresa, dejando plasmados los procedimientos a seguir en el protocolo de seguridad. Dentro del protocolo de seguridad, necesariamente deben tenerse en cuenta todas las posibles condiciones de riesgos que comprenden cada área específica de la compañía, y cada

proceso productivo que en ella se desarrolla, incluyendo los procesos de mantenimiento.

En el área externa a la empresa, también deben considerarse protocolos de seguridad y vigilancia en caso de que circunstancias externas a la compañía afecten los procesos productivos de ésta, o pongan en riesgo la integridad de personas o bienes.

Partiendo de este planteamiento, es común levantar protocolos de seguridad interna, que comprenden los riesgos que se corren durante la ejecución de cada proceso dentro de la compañía, y protocolos de seguridad externa, en los que se consideran los riesgos de hampa, clima, devastación natural, accidentes cercanos, etc.

Los protocolos de seguridad privada para empresas suelen enfocarse mucho en la protección contra robos o hurtos, por lo que se desarrollan a partir de la vigilancia y la instalación de dispositivos electrónicos de seguridad. Sin embargo, muchos de estos robos que se traducen en pérdidas importantes para los propietarios de compañías, se producen desde el área interna de cada empresa, motivo por el cual debe manejarse la vigilancia también desde dentro de la industria.

¿CÓMO SE APLICAN LOS PROTOCOLOS DE SEGURIDAD EMPRESARIAL?

Contar con protocolos de seguridad empresarial es importante, pero con sólo tenerlo no basta. El sistema de alarmas y video, debe ser testeado periódicamente, y estar colocado en los lugares estratégicos, cubriendo toda el área de la empresa.

Los guardias de seguridad deben ser de confianza o contratados en una agencia de seguridad con comprobada experiencia en el tema. No sólo deben vigilar la empresa y a los empleados, sino también saber qué hacer ante una contingencia.

Las claves de seguridad informática, deben ser protegidas y estar en buenas manos, y ser cambiadas periódicamente. Muchas empresas se han visto perjudicadas por ataques cibernéticos de empleados que han sido despedidos, y conocían las claves de acceso.

La inversión en un *software* de seguridad es esencial para prevenir estos ataques y otros que provengan de afuera. Los datos requieren protección, contratos, números de cuentas bancarias y documentación, son la base económica de la empresa, y deben ser protegidos.

Dentro de la seguridad de la empresa, los controles de acceso son una materia de especial cuidado. Contar con un buen sistema de alta tecnología para proteger los ingresos de personal y otras personas es tan importante, como el protocolo en sí mismo.

También las áreas restringidas de la empresa deben ser monitoreadas, y se deben incluir en el protocolo de seguridad. Para estas áreas específicas, la tecnología provee controles de acceso más sofisticados, como los biométricos.

¿CÓMO ELABORAR UN PLAN DE SEGURIDAD CORPORATIVO?

El cuidar de tu empresa o corporativo es de vital importancia, sobre todo por los acontecimientos que se suscitan día a día en nuestro país, en específico en el tema de seguridad.

Ante ello es indispensable que toda organización tenga un plan de seguridad que ayude a identificar, mitigar así como administrar los riesgos y posibles vulnerabilidades que puedan atentar a tus empleados y empresa.

El realizar un plan de seguridad contempla una serie de acciones enfocado a tres puntos:

1. Reducir amenazas.
2. Aminorar vulnerabilidades.
3. Optimizar la protección de tu organización.

Para ello, es necesario la colaboración de cuatro áreas: Recursos Humanos, Financieros, Administrativos y Operativos. Una persona debe ser la responsable para que el plan se ejecute correctamente y no quede en los documentos "archivados".

PASOS A SEGUIR PARA LA PREPARACIÓN DEL PLAN DE SEGURIDAD

Es importante señalar que este proceso debe contar con mediciones para verificar si funciona correctamente y en su caso, implementar mejoras al plan. Para comenzar con la elaboración del plan de seguridad, debes considerar los siguientes puntos:

- Evaluar los riesgos o vulnerabilidades: primero y antes de aterrizar el plan, es importante que analices los riesgos que corren tanto tu empresa como el personal que trabaja para ti. Eso te servirá de guía para comenzar con el plan de seguridad.

- Analiza los protocolos de emergencia: identifica las emergencias que podrán ocurrir en tu organización, como robos, incendios, catástrofes naturales o hasta accidentes laborales. Capacita y orienta a todo el personal para que al momento de cualquier altercado actúen conforme a los protocolos.

Foto: Creativeart - Freepik

- Implementación de auditorías: es importante que en tu plan de seguridad contemples supervisiones constantes para corroborar que tu empresa y trabajadores funcionen y laboren correctamente. Este punto es crucial para identificar cualquier anomalía o procesos que requiera evaluación.

- Seguridad de la información: hoy en día la tecnología juega un papel importante en las corporaciones, y aunque tiene beneficios como eficiencia y rapidez, en algunos casos es contraproducente debido a que existen personas malintencionadas que hackean información. Por ello, no debes dejar de lado implementar la seguridad en tus sistemas informáticos.

- Controla tus accesos: el contemplar sistemas que refuercen las entradas y salidas en vital para impedir algún ingreso que provoque algún momento desafortunado. Contempla en tu plan de seguridad herramientas que controlen tus accesos.

Recuerda, para que tu plan de seguridad funcione al 100% es fundamental la comunicación con tus empleados y sobre todo la capacitación en los protocolos o los sistemas que pretendas poner en marcha.

Foto: Creativeart - Freepik

¿QUÉ ESTÁ CONTEMPLADO EN EL PROTOCOLO DE SEGURIDAD DE UNA EMPRESA?

- Medidas y normas generales para proteger la empresa de cualquier amenaza externa como robos, ataques a la infraestructura, bombardeos, etc. Debe incluir los riesgos más probables según la ubicación de la empresa, eventos anteriores, etc.

- Incluye normas y medidas de protección para la empresa en general, ante la posibilidad de amenazas internas. Es decir, alguien que desde adentro pueda propiciar algún cambio a la compañía, robar, causar incendios, hacer actos violentos, etc.

- Asimismo, en los protocolos de seguridad para empresas, se contemplan normas para la prevención de hechos riesgosos. Todo lo que pueda prevenirse, se traduce en ganancia. De manera que, se establecen las normas de prevención para evitar accidentes, dentro y fuera de las instalaciones.

- El protocolo de seguridad, además, debe contemplar reglas claras para la protección de los empleados dentro de la planta y en el área administrativa. De manera que, en este documento, se contemplan los pasos de seguridad y protección que deben acatarse por los empleados durante su estadía dentro de la compañía.

- Asimismo, se plasman protocolos de acción para el personal de seguridad, en caso de que exista una amenaza potencial, que ponga en riesgo a los empleados, los productos o bienes de la compañía, inclusive ante la posibilidad de desastres naturales.

- Las normas que se dejan plasmadas en los protocolos de seguridad privada de las empresas además, deben contener el número recomendado y ubicación del personal de seguridad, de acuerdo con los requerimientos específicos de la compañía. Adicionalmente, se deben plasmar las consideraciones que involucren refuerzos al sistema de seguridad humana, como dispositivos electrónicos y sistemas inteligentes de protección digital.

> Muchos expertos han considerado que el protocolo de seguridad para empresas es fundamental para salvar vidas dentro de la compañía, proteger la materia prima y minimizar el riesgo de perder productos terminados o maquinaria

¿QUÉ ES UN PROTOCOLO DE SEGURIDAD LABORAL?

Dentro de una empresa pueden producirse accidentes, y cuando éstos incluyen trabajadores, los costos pueden ser importantes, para minimizarlos, se elabora el protocolo de seguridad laboral.

La elaboración de este tipo de protocolo es importante por los siguientes motivos:

- Aumenta la calidad de vida de los empleados y su fidelidad hacia la empresa.

- El trabajador se siente seguro por trabajar en un lugar con normas de seguridad. Se siente más distendido y por eso su rendimiento mejora, lo mismo que su motivación.

- Mejora la imagen de la empresa, desde el punto de vista interno como externo. Con un nivel alto de prevención, trabajadores y proveedores aumentan su confianza.

- La seguridad en los distintos segmentos de la empresa, hace que atraiga personal de valor hacia la empresa.

- Uno de los puntos para tener en cuenta en los protocolos de seguridad empresarial, es la formación de los empleados. Todos los trabajadores deben conocer los riesgos que su puesto implica, y cómo debe actuar para evitarlos.

Evidentemente, la inversión para la prevención a través de los protocolos de seguridad empresarial es convertir a la empresa en una organización competitiva. O sea, que es una buena forma de fortalecer las bases de la compañía y afianzar su crecimiento.

Contech
secure solutions

"Nosotros te protegemos"

Integramos la mejor tecnología para hacer tu vida más segura.

Conoce nuestros servicios de:

Analíticas Inteligentes
- Conexiones entre personas y vehículos
- Análisis forense de imágenes y video
- Estadística de incidencias

Drones (Unidades Áreas)
- Patrullaje autónomo
- Plataforma integrada a la FACC
- Planeación inteligente de operación

Logística inteligente
- Planificación de ruta segura
- Predicción de riesgos durante la ruta
- Torre de control logístico
- Plataforma de rastreo

Una empresa de Grupo CONTROL SEGURIDAD PRIVADA INTEGRAL

www.contech.mx

5 UTILIDADES DEL PROTOCOLO EMPRESARIAL

1.
El protocolo en la actualidad tiene un componente de organización imprescindible para la empresa que no quiera ser un ente aislado sin relación de ningún tipo. Es la herramienta que permite ordenar las relaciones sociales de la empresa, empleados y directivos.

2.
El protocolo ayuda a comprender la necesidad de adaptarse, integrarse y conocer cuáles son las reglas para seguir y para observar el trato correcto tanto con los superiores como con los subalternos.

3.
El protocolo incluye desde las normas de etiqueta y cortesía hasta las visitas de autoridades a la empresa, la celebración de almuerzos de trabajo o la firma de convenios con otras compañías o instituciones.

4.
El objetivo de esta disciplina, en el ámbito empresarial, es convertir a los responsables/asistentes o invitados a cualquier evento, en un correcto anfitrión, basándose en unas simples reglas de cortesía.

5.
El protocolo corporativo o empresarial es un factor clave no sólo a la hora de generar imagen de las empresas, sino también es un punto a tener en cuenta a la hora de ofrecer a trabajadores y consumidores un plus llamado calidad, el cual, se une a la fidelidad a través de los detalles que el protocolo en este sector lleva a cabo.

El protocolo aporta a la empresa una serie de valores fundamentales, entre los que podemos destacar:

- **Imagen:** ayuda a difundir la imagen de la empresa mediante actos y apariciones públicas.
- **Proyección:** favorece la proyección social de la empresa.
- **Comunicación:** comunica los mensajes de la empresa de modo eficaz.
- **Procedimiento:** establece unas normas y unas técnicas de organización.
- **Rentabilidad:** consigue incrementar los beneficios optimizando el resultado de cada acto.
- **Prestigio:** ayuda a construir una imagen favorable de la empresa.

LOS RETOS DE LA SEGURIDAD EN LA ACTUALIDAD

La seguridad se ha convertido en una de las mayores preocupaciones de nuestra sociedad. Una sociedad bautizada como "sociedad del riesgo" en la cual la tecnología y la ciencia han amplificado el espectro de lo que hasta su proliferación conocíamos como riesgo. La fragilidad de los escenarios que se plantean, lo que conocemos como seguridad líquida, enarbola el dilema de cómo reaccionar a situaciones futuras, en muchos casos impredecibles, dificultando las medidas de prevención.

Los nuevos riesgos nos conducen a nuevas formas de afrontarlos, así como de prevenirlos. La monitorización y vigilancia de la marca, así como la elaboración de inteligencia para la toma de decisiones ya no tiene exclusividad del sector público. Cualquier gran organización cuenta con estas estrategias para proteger su seguridad física, lógica y sus intangibles.

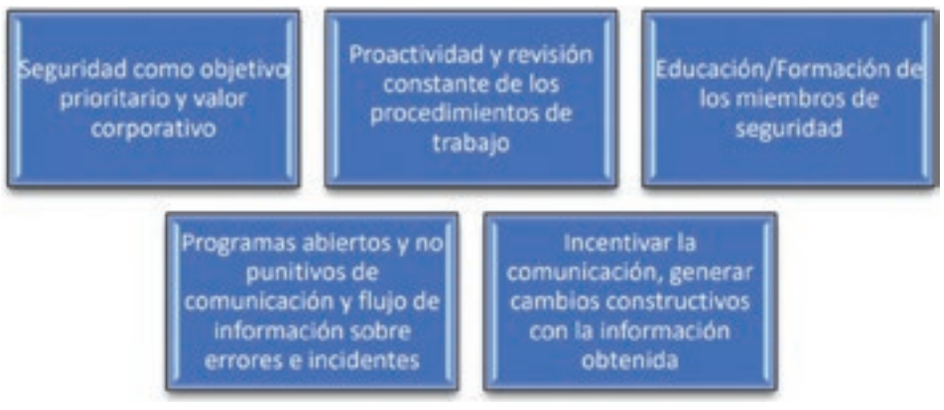
La seguridad se desarrolla en el seno la sociedad y, por lo tanto, evolucionará bajo sus demandas. Esto explica el cambio de paradigma por lo que respecta a la seguridad en el transcurso de los últimos años. Tradicionalmente las funciones del personal de seguridad privada se han asociado a un concepto de seguridad física basado en guardias de seguridad y en ciertas medidas de seguridad como alarmas y videocámaras. Tales medidas fueron para atender a una serie de amenazas determinadas.

El uso de la tecnología acapara cada vez más ámbitos y más sectores de la sociedad y se extiende a gran velocidad como si de una metástasis se tratara. Sin embargo, su grado de penetración en la sociedad no es directamente proporcional al conocimiento de la seguridad ni a los riesgos a los que nos expone. Dicha circunstancia no escapa del ojo del delincuente y encuentra en esta vulnerabilidad para perpetrar sus fechorías.

Este hecho explica en gran parte que actualmente las preocupaciones del sector privado en materia de seguridad se centren en hacer frente a esta lacra. Una lacra que aumenta en número y en magnitud a marchas forzadas tal y como revelan las investigaciones.

La ignorancia de los riesgos asociados al uso de la tecnología se extiende a los departamentos de seguridad y por ende a la figura de los directores de seguridad de tal manera que ven en la ciberseguridad una patata caliente de la que prefieren no hacerse cargo.

En una sociedad bautizada como la sociedad de la información, en la que los datos son el petróleo del siglo XXI, quien tiene la información tiene el poder. La información hay que protegerla —de ahí la importancia de la ciberseguridad—, pero también se tiene que tratar. Se ha pasado de vigilar los mensajes escritos en las pancartas de las manifestaciones a monitorizar la red, Internet 2.0, etc. Esta nueva forma de hacer inteligencia ha abierto una ventana de oportunidad para los responsables de la seguridad corporativa en aras de mejorar la prevención de las amenazas fruto de sus análisis de riegos. ■



ISIS
SEGURIDAD INTEGRAL

Creamos entornos **seguros**

Servicios:

- Guardias Intramuros
- GPS y Monitoreo
- Custodias al Transporte
- Seguridad Electrónica
- Control de Confianza

55 1089 1089

55 7652 6630

ventas@isis-seguridad.com.mx

www.isis-seguridad.com.mx

Canela #352, Granjas México, C.P. 08400 CDMX

SEGURIDAD PRIVADA EN LA INDUSTRIA AUTOMOTRIZ

En el primer semestre del año hubo un incremento en el robo a vehículos nuevos que son transportados en las famosas madrinas

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

En cinco años el panorama de la industria automotriz en el mundo ha cambiado radicalmente. Mientras que en el año 2018 se alcanzó el máximo histórico en la producción mundial de vehículos (96 millones 869 mil 20 unidades), en 2020 la producción mundial retrocedió 15.8% como consecuencia de la pandemia por COVID-19, y en el año 2021 sólo pudo recuperarse en un 3.1% debido a la falta de suministros, principalmente de semiconductores[1].

Estas cifras fueron recopiladas por la Asociación Mexicana de la Industria Automotriz (AMIA) —junto con otras fuentes— que arrojan que el mayor productor de unidades (vehículos) en 2021 fue China, seguido de Estados Unidos, Japón, India, y teniendo en el séptimo lugar a México, siendo los vehículos ligeros los que más se producen en el país (más del 95%).

En México existen 22 plantas de vehículos de 14 empresas, las cuales están en 14 diferentes estados del país; también hay 10 plantas de motores de siete empresas diferentes en seis estados, y siete plantas de transmisiones de seis empresas en cinco estados.

La AMIA agrupa a 22 empresas dedicadas a la fabricación, importación y comercialización de vehículos ligeros, entre ellas: Volkswagen de México, Nissan Mexicana, Toyota Motor de México, Ford Motor Company, BMW de México, Mercedes-Benz México y Stellantis México.

La industria automotriz en México contribuye con el 18.3% del Producto Interno Bruto (PIB) de la industria manufacturera, y con el 3.5% al PIB nacional. Con base en el Instituto Nacional de Estadística y Geografía (INEGI 2021), esta industria emplea a cerca de 930 mil 758 personas beneficiando directamente a 3.5 millones de personas.

En lo que va del año, tanto la AMIA en voz de su director Fausto Cuevas, como Guillermo Rosales, presidente de la Asociación Mexicana de Distribuidores de Automotores (AMDA), informaron a un periódico mexicano, que ha incrementado el "robo de vehículos nuevos que son trasladados de las plantas de manufactura a las distribuidoras, así como en la entrega de los autos a los consumidores, mientras que va en ascenso la presencia del vandalismo en las carreteras, en especial en la zona del Bajío (principalmente Guanajuato y en los límites con Michoacán y Jalisco)"[2]. Guillermo Rosales también indicó que se ha presentado el asalto y robo en los vehículos a traslado rodado, "es decir, los que venden un distribuidor y se entregan a clientes o entre intercambio de distribuidores", o sea a las llamadas madrinas transportadoras.

> "El robo de vehículos terminados y las autopartes nuevas que se registran y denuncian en algunos territorios de nuestro país, así como la corrupción e impunidad están afectando a la industria, el mercado gris y crimen organizado que se alimenta de encargos específicos de autos", **Enrique Arellano Balcázar**

Es por ello que en esta ocasión nuestros tres colaboradores entrevistados y que son expertos en la seguridad de la industria automovilística, nos comparten su análisis sobre el tema.

LA CARRETERA: EL FOCO ROJO DE LA INDUSTRIA AUTOMOVILÍSTICA

Cada industria tiene un foco rojo en donde se concentran la mayor cantidad de delitos, robos o intentos de éstos, en la industria automovilística es en el traslado, es decir en las carreteras.

"La inseguridad en la cadena logística, especialmente el robo en carreteras, es uno de los principales problemas de esta industria; asimismo es preocupante el empoderamiento de la delincuencia organizada en contra posición del debilitamiento de las instituciones de seguridad del Estado, también preocupa el funcionamiento de las fiscalías estatales, ya que existe una gran impunidad en delitos denunciados", comentó Erik Eliut Navarro García, director de Seguridad y Prevención de Incendios de Stellantis México.

Foto: Creativeart - Freepik

De igual manera, Enrique Arellano Balcázar, *Corporate Security Manager* de Mercedes-Benz México, coincidió en que la inseguridad en las carreteras está afectando a la industria de forma considerable, así como la falta de mantenimiento en estas. "El robo de vehículos terminados y las autopartes nuevas que se registran y denuncian en algunos territorios de nuestro país, así como la corrupción e impunidad están afectando a la industria, el mercado gris y crimen organizado que se alimenta de encargos específicos de autos y piezas que finalmente afectan a la cadena logística y clientes por todas estas situaciones", enfatizó.

La delincuencia va adaptándose de forma casi inmediata a la situación social y la demanda del mercado negro, pero los expertos en seguridad, están un paso adelante, ya que logran identificar sus mecanismos de asalto, el territorio e implementan estrategias y tecnología para contrarrestar esos problemas.

Erik Navarro nos compartió algunas de ellas: reforzamiento en la seguridad de los procesos logísticos, incremento en la utilización de tecnología de rastreo satelital, capacitación constante a operadores y empresas de transporte, implementación de tolerancia cero, todos los delitos son denunciados y perseguidos, participación en mesas de seguridad.

Es muy importante la relación y colaboración con las autoridades, así como el apoyo de las diferentes asociaciones de seguridad. "Parte de la estrategia de la marca es implementar procesos robustos y muy bien estructurados que ayuden a mitigar estos riesgos, mismos que compartimos con toda la red de distribuidores para que puedan ser implementados con nuestros clientes.

Adicionalmente, buscamos siempre aprovechar las tecnologías desarrolladas y recursos públicos en materia de seguridad estatal y federal, así como una estrecha comunicación con las autoridades que nos permitan utilizar los recursos de seguridad, aplicación de auditorías y reuniones estrechas con los proveedores de logística y en conjunto detallar al mínimo los procesos de monitoreo, buscar el desarrollo de ingeniería que dificulte el hurto pero otorgue ventajas para las autoridades y finalmente compartir las mejores prácticas que beneficien a la industria automotriz", señaló Enrique Arellano.

Por su parte, José Luis Valderrábano, gerente de Seguridad para México y apoyo a Latinoamérica de Nissan Mexicana, nos compartió que en su experiencia en la industria, para mejorar las estrategias de seguridad es importante trabajar en conjunto con los transportistas, realizar reuniones con las autoridades de seguridad y plantear las problemáticas ante los secretarios de estado.

SEGURIDAD PRIVADA ¿SÍ O SÍ?

La industria de la seguridad privada abarca todos los rubros que se pueda imaginar, desde *retail* hasta entretenimiento, cada uno con sus características específicas y con sus lineamientos, capacitación y requerimientos, la industria automotriz cuenta con este servicio en su mayoría.

"En Stellantis México sí contamos con seguridad privada, ya que es un gran aliado de la empresa para proteger al recurso humano, así como los bienes tangibles e intangibles; como todo, tiene grandes áreas de oportunidad pero siempre se tiene la disposición de mejorar el servicio", comentó Erik Navarro.

Stellantis es una compañía global que diseña, fabrica, distribuye y vende vehículos, y surgió de la unión de dos compañías: Grupo FCA y Grupo PSA (2021). Esta firma se conforma por 14 marcas, entre ellas las ya conocidas en México: Jeep, Dodge, Chrysler, Mopar, RAM, FIAT, Alfa Romeo y Peugeot, además de las que no se comercializan en México, como Citroen, DS y Opel, por mencionar algunas.

"Es preocupante el empoderamiento de la delincuencia organizada en contra posición del debilitamiento de las instituciones de seguridad del Estado, también preocupa el funcionamiento de las fiscalías estatales, ya que existe una gran impunidad en delitos denunciados", **Erik Eliut Navarro García**

José Luis Valderrábano comentó que también cuentan con seguridad privada y aunque es funcional para esta industria, comentó que hay ciertos aspectos que pueden mejorarse. "Considero que falta el compromiso al factor humano y no pensar sólo en la utilidad, así mismo creo que no puedes dar todo el poder por la falta de confianza".

En el caso de Mercedes-Benz México, la seguridad privada también está presente y funciona bien debido a que siguen diversos protocolos con los que se cuenta a nivel mundial para mantener un estándar en todas sus ubicaciones.

"Mi opinión es, que es un recurso que debe constantemente mantenerse actualizado con una visión preventiva y clara en los procesos y canales de comunicación entre las áreas operativas y las administrativas, aportando valor en las distintas operaciones que nos dan soporte y protección logrando transparencia en el servicio", expresó Enrique Arellano.

Y retomando el comentario de Arellano Balcázar, hay aspectos que se pueden mejorar y son necesarios para un mejor funcionamiento de la seguridad privada en esta industria. "Se viene haciendo mucho por mejorar la imagen, desempeño y servicios de seguridad privada, al día de hoy lo más importante en las empresas de seguridad privada es seleccionar adecuadamente al personal y llevarlo a la profesionalización con el apoyo y desarrollo académico y si esto no es posible, una compensación económica justa permitiría reducir actos desleales, siendo clara la comunicación entre la operación y la administración alineada hacia los valores y normas del cliente", puntualizó.

TIPS DE SEGURIDAD EN LA INDUSTRIA AUTOMOTRIZ

A continuación, José Luis Valderrábano nos compartió los cinco tips de seguridad en la industria automotriz al adquirir el material:

1. Cumplir con protocolos de seguridad en la cadena de suministro.
2. Hacer sentir al personal externo como parte importante del equipo y que su trabajo es esencial para la seguridad.
3. Efectuar inspección y verificación del transporte que ingresa y sale de las instalaciones.
4. Considerar tecnología para tener mejor evidencia o eficientar el proceso.
5. Capacitación en los procesos y protocolos al personal efectuando verificación de cumplimiento.

Por su parte, Erik Eliut nos compartió los cinco tips de seguridad en la industria automotriz en la fabricación:

1. Ser aliados de negocio de las áreas de producción.
2. Involucrarse en las operaciones de la compañía (manufactura, logística, etc.).
3. Estar al día con los riesgos presentes en las operaciones.
4. Buscar el acercamiento y apoyo de las autoridades.
5. Capacitación constante del personal de seguridad.

En conclusión, la inseguridad en las carreteras está afectando de forma directa a la industria automotriz, el trabajo en conjunto con las autoridades y la aplicación de estrategias de seguridad y tecnología, ayuda a mitigar los riesgos a los que se enfrenta día con día para llegar a su destino, la seguridad privada es efectiva en esta industria siempre y cuando los elementos tengan una capacitación constante y actualizada en la empresa de donde provienen. ■

REFERENCIAS

[1] *https://www.amia.com.mx/publicaciones/industria_automotriz/*

[2] *"AMDA y AMIA alertan sobre aumento de robos a transportistas de autos nuevos en carreteras del Bajío", Lilia González, El Economista. 06/06/2022. https://www.eleconomista.com.mx/empresas/AMDA-y-AMIA-alertan-sobre-aumento-de-robos-a-transportistas-de-autos-nuevos-en-carreteras-del-Bajio-20220606-0068.html*

"Considero que falta el compromiso al factor humano y no pensar sólo en la utilidad, así mismo creo que no puedes dar todo el poder por la falta de confianza", **José Luis Valderrábano**

DOORMAN

ALGUIEN EN QUIEN CONFIAR

Combate de incendios

Primeros Auxilios

SEGURIDAD PRIVADA

PARTE MUY IMPORTANTE DENTRO DE NUESTRA ORGANIZACIÓN ES LA CAPACITACIÓN, QUE SON 30 HORAS DIVIDIDAS EN 5 SECCIONES:

Defensa Personal

Atención al cliente

Protección Civil

25 AÑOS

PERMISO CNS SEGOB: DGSP/103-13/2306
SSP CDMX: Permiso: 0718-15 Expediente: 3104-10
CESC EDOMEX: Autorización: CESC/001/16-01/SP

CONTÁCTANOS

T. 5555468229 | 5555367725 | 5572589139 | 5556519580

Cóndor No. 100, Col. Los Alpes, Álvaro Obregón, CP 01010, CDMX

www.doorman.com.mx

¿POR QUÉ CERTIFICAR NUESTRA EMPRESA DE SEGURIDAD PRIVADA BAJO LA NORMA ISO 18788? (PARTE 2)

La ISO 18788 es un estándar diseñado para la ejecución de funciones y tareas de seguridad alineadas con buenas prácticas de negocio y manejo de riesgos

Foto: Creativeart - Freepik

VENEZUELA | Adolfo M. Gelder

Continuando con el artículo anterior es muy conveniente que todo profesional de seguridad conozca no sólo la norma ISO 18788, sino todas las normas que existen relacionadas a la seguridad y que se pueden aplicar de manera acertada en nuestro quehacer diario, las nombro a continuación:

1. ISO 22341 CPTED, Diseño del Entorno para la Prevención del Crimen.
2. ISO 23234 Criterios de Seguridad para Planificar la Seguridad de Edificios.
3. ISO 27001 Gestión de la Seguridad Física y del Entorno.
4. ISO 28000 Seguridad de la Cadena de Suministro.
5. ISO 31000 Gestión del Riesgo.
6. ISO 33010 Gestión de Riesgos de Viajeros.
7. ISO 37001 Gestión Anti soborno.
8. ISO 39001 Seguridad Vial.
9. ISO 45001 Seguridad y Salud en el Trabajo.

ISO 22341 CPTED, DISEÑO DEL ENTORNO PARA LA PREVENCIÓN DEL CRIMEN

Esta norma busca disuadir al delincuente actuando sobre el entorno en el que se cometerían los delitos disminuyendo así probabilidad del delito, una metodología de prevención del delito que se basa en el hecho demostrado de que un diseño y uso adecuado de los edificios y del urbanismo, y por supuesto el comportamiento de los ciudadanos, reducen el riesgo y el miedo al delito, mejorando con ello la calidad de vida y la habitabilidad de nuestros espacios públicos y privados.

Dentro de sus beneficios tenemos que la seguridad se convertiría en un valor general, y no individual. En lugar de simplemente implementar medidas de seguridad en pisos aislados, la norma busca proteger y hacer seguras zonas enteras (por ejemplo, una urbanización).

ISO 23234 CRITERIOS DE SEGURIDAD PARA PLANIFICAR LA SEGURIDAD DE EDIFICIOS

ISO 23234:2021. *Buildings and civil engineering works –Security– Planning of security measures in the built environment.* Es la norma que sirve de ayuda a aquellas áreas de seguridad involucradas en la implantación de medidas de protección en nuevos edificios. La norma define el proceso de diseño e implantación a seguir, los entregables a considerar y qué profesionales deben involucrarse.

Detalla los requisitos y recomendaciones para ayudar a las organizaciones a poner en marcha planes de protección contra acciones intencionadas no deseadas. Proporcionando una plantilla bien estructurada para identificar sus requisitos y desarrollar las medidas de seguridad adecuadas.

El objetivo es conseguir edificios que sean seguros desde el punto de vista funcional y también a la hora de evitar el acceso de personas no autorizadas. Se reduce de este modo el riesgo de intromisiones en espacios en los que puede haber almacenada información, a la vez que se mejora la seguridad personal de quienes viven o trabajan en ese tipo de edificios.

ISO 27001 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Es la norma que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así

GSI
SEGURIDAD PRIVADA

GSI Seguridad Privada S.A. de C.V.

Profesionales en Seguridad Privada

Oficiales de Seguridad Armados

- *Oficiales de seguridad*
- *Oficiales de seguridad armados*
- *Protección ejecutiva*
- *Rastreo y monitoreo*
- *Servicios de contratación segura*
- *Seguridad móvil al comercio y zona residencial*
- *Capacitación y formación de equipos de seguridad*

SOMOS GRUPO GSI, orgullosamente una empresa Mexicana

www.gsiseguridad.com.mx

atencionaclientes@gsiseguridad.com.mx

Tel. 800 830 5990

ESR Empresa Socialmente Responsable

redconocer

DNV

AMESP

EMPRESAS DE GSI GRUPO SEGURIDAD INTEGRAL

como de los sistemas que la procesan. Permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

La norma incluye los requisitos para la apreciación y el tratamiento de los riesgos de seguridad de información a la medida de las necesidades de la organización. Los requisitos establecidos en esta norma internacional son genéricos y aplicables a todas las organizaciones, cualquiera que sea su tipo, tamaño o naturaleza.

Define de manera genérica, independientemente de los factores ambientales de organización (entorno, contexto, activos de las TIC, información, cultura organizacional, etc.) —tanto internos como externos a la misma— y de los activos de los procesos de la organización (políticas, procedimientos, procesos, etc.), cómo se planifica, implanta, verifica y controla un Sistema de Gestión de Seguridad de la Información, a partir de la realización de un análisis de riesgos y de la planificación e implantación de la respuesta a los mismos para su mitigación. Es decir, cualquier empresa u organización puede desplegar un SGSI siguiendo esta norma.

ISO 28000 SEGURIDAD DE LA CADENA DE SUMINISTRO

Los sistemas de gestión de seguridad de la cadena de suministro basados en la norma de certificación ISO 28000 identifican los niveles de riesgo en sus operaciones de cadena de suministro. Esta información permite a la organización llevar a cabo evaluaciones de riesgo y aplicar los controles necesarios con el apoyo de herramientas de gestión (es decir, controles de documentos, indicadores clave de rendimiento, auditorías internas y formación).

La norma es aplicable a organizaciones de todos los tamaños que se dediquen a la fabricación, el servicio, el almacenamiento o el transporte en cualquier fase de la cadena de producción o suministro.

Un sistema de gestión conforme a la norma ISO 28000 le ayuda a conseguir:

- Resiliencia empresarial integrada.
- Prácticas de gestión sistematizadas.
- Mayor credibilidad y reconocimiento de la marca.
- Terminología y uso conceptual alineados.
- Mejora del desempeño de la cadena de suministro.
- Evaluación comparativa con criterios reconocidos internacionalmente.
- Mayores procesos de cumplimiento.

ISO 31000 GESTIÓN DEL RIESGO

Esta norma ayuda a las organizaciones en sus análisis y evaluaciones de riesgos. Tanto si trabaja en una empresa pública, privada o comunitaria, puede beneficiarse de la norma ISO 31000, puesto que se aplica a la mayoría de las actividades empresariales, incluyendo la planificación, operaciones de gestión y procesos de comunicación.

Mediante la implantación de los principios y guía de la norma ISO 31000 se podrá mejorar su eficacia operativa, su gobernanza y la confianza de las partes interesadas, al mismo tiempo que minimiza cualquier posible pérdida. Esta norma también le ayuda a fomentar el desempeño de Seguridad y Salud, establecer una base sólida para la toma de decisiones y fomentar una gestión proactiva en todas las áreas.

Una certificación ISO 31000 demuestra que usted tiene las competencias necesarias para apoyar a una organización en la creación y protección de valor. Además, demuestra que es capaz de ayudar a las organizaciones a establecer una estrategia de riesgo, alcanzar objetivos estratégicos y tomar decisiones informadas.

La norma ISO 31000 está dirigida a las personas que gestionan el riesgo en las organizaciones: tomando decisiones, estableciendo y logrando objetivos y mejorando el desempeño.

La norma ISO 31000 está diseñada para poderse aplicar en cualquier tipo de organización, sea cual sea su sector y tamaño. En concreto, la norma "proporciona directrices para gestionar el riesgo al que se enfrentan las organizaciones" y que la aplicación de sus directrices "puede adaptarse a cualquier organización y a su contexto".

ISO 33010 GESTIÓN DE RIESGOS DE VIAJEROS

La norma ISO 33010 se enfoca en servir de apoyo a los encargados de gestionar los riesgos asociados a las personas de una empresa que deben desplazarse. Propone, para ello, un proceso exhaustivo que se asemeja en su propuesta de gestión de riesgos al proceso de la ISO 31000, pero centrándolo en los riesgos asociados al personal desplazado.

En general, esta norma permite generar un programa de protección de desplazados a aquellas áreas de seguridad que no dispongan del mismo, o bien actualizar programas actuales. El enfoque práctico y exhaustivo de la norma sirve de guía para realizar estas labores, y su enfoque puramente relacionado con la gestión de riesgos seguramente sea útil para aquellas áreas de seguridad que hayan tenido dificultad para justificar que la responsabilidad de gestionar estos riesgos esté recogida dentro de su alcance.

La aplicación de esta norma es un avance destacado en la uniformidad de criterios, pero también en la mejora de los niveles de calidad, seguridad, fiabilidad, interoperabilidad y eficiencia del sector. Todo ello conlleva un trabajo importante en el corto plazo: revisar nues-

Foto: Creativeart - Freepik

ISO 37001 es el estándar internacional que especifica los requisitos y proporciona una guía para establecer, implementar, mantener, revisar y mejorar un sistema de gestión anti soborno

tros propios estándares y *frameworks* para adaptarlos a esta nueva referencia, que seguro contribuirá al avance de la seguridad física de los viajeros.

La norma ISO 33010 se creó con la finalidad de ofrecer orientación, coordinación, simplificación y unificación de criterios a las empresas y organizaciones con el objeto de aumentar la efectividad en la gestión de riegos en los viajeros, así como estandarizar los servicios para las organizaciones dedicadas al traslado de personas y mercancías.

¿QUÉ LOGRA UNA EMPRESA AL IMPLEMENTAR LA NORMA ISO 33010?

Beneficios ante el mercado:

- Mejorar la imagen de los productos y/o servicios ofrecidos.
- Favorecer su desarrollo y afianzar su posición.
- Ganar cuota de mercado y acceder a mercados exteriores gracias a la confianza que genera entre los clientes y consumidores.

Beneficios ante los clientes:

- Aumento de la satisfacción de los clientes.
- Eliminar múltiples auditorías.
- Acceder a acuerdos de calidad concertada con los clientes.

Beneficios para la gestión de la empresa:

- Servir como medio para mantener y mejorar la eficacia y adecuación del sistema de gestión de la calidad, al poner de manifiesto los puntos de mejora.
- Cimentar las bases de la gestión de la calidad y estimular a la empresa para entrar en un proceso de mejora continua.
- Aumentar la motivación y participación de personal, así como mejorar la gestión de los recursos.

ISO 37001 GESTIÓN ANTI SOBORNO

ISO 37001 es el estándar internacional que especifica los requisitos y proporciona una guía para establecer, implementar, mantener, revisar y mejorar un sistema de gestión anti soborno. El soborno es una de las formas de corrupción más habituales en el mundo de los negocios.

La implantación de un Sistema de Gestión Anti-soborno según la norma ISO-37001 proporcionará una serie de beneficios a la compañía:

- Establece una serie de mecanismos para prevenir, combatir o minimizar el riesgo antes situaciones de soborno.
- Prevenir a la organización ante posibles sanciones legales derivadas de situaciones de soborno.
- Establecer una política ética empresarial.
- Incrementar la concienciación en cuanto al soborno en la organización.
- Proporciona un valor añadido a la empresa, diferenciándola respecto a la competencia.
- Contribuye a mejorar la imagen de la empresa, garantizando a sus clientes que opera de manera ética.
- Permite tener un mayor control y mostrar una mayor confianza en las transacciones comerciales.

Foto: Creat'rear - Freepik

El objetivo es conseguir edificios que sean seguros desde el punto de vista funcional y también a la hora de evitar el acceso de personas no autorizadas

¿CÓMO SE BENEFICIA UNA EMPRESA AL IMPLEMENTAR UN SISTEMA DE GESTIÓN ANTI SOBORNO?

Los beneficios de implementar esta medida se resumen en cinco puntos básicos:

1. **Reducción del riesgo de sobornos:** el beneficio más evidente de la lista y, claro, uno de los más importantes, es el de ayudar a llevar a cero los posibles casos de soborno en la organización.

2. **Demostrar transparencia:** con el uso de un Sistema de Gestión Anti soborno la organización le estará diciendo a sus trabajadores, propietarios, socios y al resto del mundo que tiene una política de tolerancia cero hacia la corrupción.

3. **Incremento de la competitividad:** al demostrar un fuerte compromiso ético, el éxito de la organización se verá en aumento pues la inversión externa y los clientes potenciales la contemplarán como una referencia o modelo a seguir.

4. **Detección oportuna de suspicacias:** implementar el Sistema de Gestión Anti soborno permitirá detectar cualquier irregularidad alrededor de los asuntos financieros o comerciales, contribuyendo a disminuir la corrupción.

5. **Proveer evidencia:** el último de los beneficios es también uno que ninguna organización quisiera tener que enfrentar. La correcta implementación del ISO 37001 permite presentar evidencia favorable en casos en los que exista una investigación criminal, demostrando que la empresa procuró evitar este tipo de sucesos de manera correcta.

ISO 39001 SEGURIDAD VIAL

La norma ISO 39001 establece los requisitos mínimos para un sistema de gestión de la seguridad del tráfico en carretera. Los gobiernos, autoridades de tráfico, asociaciones de seguridad y empresas privadas exigían desarrollar una norma como esta, debido al creciente número de personas fallecidas o heridas en la carretera cada año.

¿Para quién es la norma ISO 39001?

- Empresas de Transporte de pasajeros o mercancías.
- Empresas con flotas de vehículos.
- Empresas con personal de ventas, instalaciones, mantenimiento, repartidores, mensajería, etc.

¿Cuál es el objetivo de la norma ISO 39001?

- Diferenciarse de la competencia.
- Mejorar la eficiencia a través de una mejor gestión.
- Acreditar su compromiso con la seguridad vial.
- Mejorar y reducir costos.

¿Qué logra una empresa al implementar la ISO 39001?

- Reducción de costes relacionados con la siniestralidad vial.
- Mayor eficiencia en los costes relacionado con los tránsitos por carretera en la organización.
- Evidenciar a las partes interesadas el compromiso real de la organización con la seguridad vial.
- Disminución de incidentes y accidentes en carretera.
- Reducción en primas de seguros relacionados con la seguridad vial (responsabilidad vial, seguros de autos, etc.).
- Incremento en la eficiencia de los servicios prestados que estén relacionados con la seguridad vial (transporte de personas, mercancías, etc.).
- Disminución de incidentes en carretera.
- Evidencia objetiva de cumplimiento de requisitos legales de seguridad vial.
- Elemento de diferenciación competitiva.
- Ventaja en licitaciones públicas y similares.
- Mayor eficiencia en la prestación de servicios relacionados.

Foto: Creativeart - Freepik

Una certificación ISO 31000 demuestra que usted tiene las competencias necesarias para apoyar a una organización en la creación y protección de valor

ISO 45001 SEGURIDAD Y SALUD EN EL TRABAJO

Se trata de la primera norma internacional que aborda la seguridad y salud en el trabajo, ofrece un marco claro y único a todas las organizaciones que deseen mejorar su desempeño en materia de SST. Se dirige a los máximos responsables de las organizaciones y pretende crear un lugar de trabajo seguro y saludable para los empleados y para cualquier persona que acceda a las organizaciones. Para lograrlo, es crucial controlar todos los factores que puedan dar lugar a enfermedades, lesiones y, en casos extremos, la muerte, mitigando para ello los efectos adversos en el estado físico, mental y cognitivo de las personas. Aunque la ISO 45001 se basa en el Estándar OHSAS 18001 —la anterior referencia en materia de SST— se trata de una norma nueva y diferente.

La norma ISO 45001, ofrece una serie de beneficios a las organizaciones que deseen implementar un Sistema de Gestión de Seguridad y Salud en el Trabajo, que pueden ser:

- Desarrollar e implementar las políticas y los objetivos del Sistema de Gestión de SST.
- Establecer los procesos sistemáticos que consideran su contexto y que tengan en cuenta sus riegos y las consecuencias jurídicas que pueden tener.
- Determinar los riesgos que están asociados a sus actividades, trata de eliminar o poner controles para reducir al mínimo los efectos potenciales.
- Establecer todos los controles operacionales para gestionar los riesgos con su Sistema de Gestión de Seguridad y Salud en el Trabajo.
- Incrementar la conciencia en cuento a los riesgos.
- Evaluar el rendimiento y tratar de mejorarlo mediante la toma apropiada de comportamiento.
- Los trabajadores se aseguran de tener un papel activo en el Sistema de Gestión de Seguridad y Salud en el Trabajo.

¿CUÁL ES LA DIFERENCIA ENTRE ISO 45001 Y OHSAS 18001?

La principal diferencia entre ambas normas es que la ISO 45001 adopta un enfoque proactivo que requiere que los riesgos de peligro se evalúen y corrijan antes de que causen accidentes y lesiones, mientras que la OHSAS 18001 adopta un enfoque reactivo que se centra únicamente en los riesgos y no en las soluciones.

En una próxima entrega hablaremos sobre las normas europeas relacionadas a la seguridad y cómo poder implementarlas en América, los espero. ■

Adolfo M. Gelder,
director del Proyecto Mente Táctica.

Más sobre el autor:

GRUPO CORPORATIVO DE PREVENCION

NUESTRA EXPERIENCIA DA RESULTADOS

BASC
BUSINESS ALLIANCE FOR SECURE COMMERCE
CERTIFICADO BASC
MEX-GDL-00045-1-14

GRUPO CORPORATIVO DE PREVENCIÓN ES UNA EMPRESA LEGALMENTE CONSTITUIDA Y CERTIFICADA

NUESTROS SERVICIOS:

- SUPERVISIÓN A TRANSPORTE DE CARGA (CUSTODIA CIVIL)
- SEGURIDAD INTERNA (GUARDIAS INTRAMUROS)
- Y MÁS...

SÍGUENOS EN NUESTRAS REDES SOCIALES:

@grupocorporativodeprevencion
@grupocorporativodeprevencion
@GCP_seguridad

CONTÁCTANOS

Leona Vicario No. 6 Cuautitlán Izcalli
ventas@grupogcp.mx
55 7931 6739

PROFESIONALIZACIÓN DE LA SEGURIDAD PRIVADA EN MÉXICO

Un guardia de seguridad debe saber cómo actuar y resolver novedades, es necesario que entienda que está trabajando para una empresa a la que le debe lealtad por ser su empleador y que éste a su vez se comprometió a prestar un servicio, por lo que debe estar comprometido con el cliente y dar resultados efectivos

MÉXICO

Pablo Romero Navor / *Staff* Seguridad en América

SURGIMIENTO DE LA SEGURIDAD PRIVADA

La Seguridad Pública es una función del Estado y una obligación de éste para con su población. Sin embargo, el aumento de los índices delictivos y la percepción de inseguridad constante ha propiciado —entre otros factores— que la ciudadanía, en sus distintas formas de organización, busque alternativas para la protección de su persona y sus bienes; siendo una de estas la seguridad privada.

La seguridad privada se puede definir como "el conjunto de bienes y servicios brindados por entes privados, para proteger a sus clientes de delitos, daños y riesgos". En una definición más amplia; es "el conjunto de bienes y servicios ofrecidos por personas físicas y jurídicas privadas, destinados a proteger a sus clientes —y a sus bienes y patrimonio— de daños y riesgos, a auxiliarlos en caso de delitos, siniestros o desastres, y a colaborar en la investigación de delitos que los involucren. Los clientes pueden ser personas físicas o jurídicas, públicas o privadas".

En ese mismo sentido, la Ley Federal de Seguridad Privada define a esta. actividad en la fracción 1 de su Artículo 2 como: "Actividad a cargo de los particulares, autorizada por el órgano competente, con el objeto de desempeñar acciones relacionadas con la seguridad en materia de protección, vigilancia, custodia de personas, información, bienes inmuebles, muebles o valores, incluidos su traslado; instalación,

Foto: Creativeart - Freepik

Foto: Pixabay

> Debemos terminar con la imagen de ignorancia y mediocridad que tienen los guardias de seguridad en nuestro país

operación de sistemas y equipos de seguridad; aportar datos para la investigación de delitos y apoyar en caso de siniestros o desastre en su carácter de auxiliares a la función de Seguridad Pública".

La seguridad privada como la conocemos actualmente cobró fuerza en el mundo a partir de la década de los 80, debido a un entorno cada vez más complejo y ante amenazas crecientes por la inseguridad provocada por factores como el terrorismo, la pobreza extrema y las crisis que han afectado a toda la población.

LA PRIVATIZACIÓN DE LA SEGURIDAD PÚBLICA Y EL MERCADO EMERGENTE

Mientras los actores privados toman mayor control en los servicios de seguridad, el Estado mantiene la responsabilidad de regular, gestionar y operar aspectos intrínsecos a la seguridad privada, con el fin de que se apegue a las leyes y respete los derechos humanos de sus trabajadores y de la población.

Delimitar las fronteras entre seguridad pública y privada es un trabajo complejo por la porosidad y traslape de funciones entre ambas. Empero, se pueden señalar puntos de análisis. Por ejemplo, el ámbito de acción, público o privado donde las funciones para la seguridad pública son amplias, principalmente de acción reactiva; mientras que para la seguridad privada son limitadas, y de acción preventiva; los sujetos son funcionarios, para el caso público y ciudadanos, para el caso privado.

De igual forma, la seguridad pública responde al Poder Ejecutivo y Legislativo; la policía privada a su empresa. La financiación de la policía pública es realizada por los ciudadanos a través del gobierno, y la privada por los clientes. De igual forma, ambas tienen redes y estructuras organizativas distintas donde emergen nuevos actores con intereses, incluso contrarios a la seguridad. Por ejemplo, los intereses del sector privado convierten a la seguridad en un negocio altamente rentable.

El origen de la seguridad privada se argumenta como resultado de la carencia de protección empresarial, frente a la desactualización de la seguridad pública para enfrentar las nuevas modalidades de ataque. Aunque histórica y empíricamente se muestra que el aumento de seguridad privada responde a factores como el crecimiento económico, las nuevas responsabilidades civiles y penales para las empresas, mayores estándares de referencia en seguridad, la competitividad de la industria, entre otros.

LOS SERVICIOS DE SEGURIDAD PRIVADA EN MÉXICO

Los inicios de la seguridad privada en México datan de la década de 1970, con apenas 40 empresas. Después de la crisis económica de 1994 el número de empresas comenzó a crecer, pues se especulaba el aumento delictivo. Así, en los años siguientes se registraron anualmente alrededor de 151 empresas con dimensiones y calificaciones desiguales. Para el año 2000 ya eran mil 400 empresas.

La seguridad privada en México registra un crecimiento de entre 18 y 24 por ciento en los últimos años y actualmente alcanza un valor de 485 mil millones de pesos, equivalente a dos por ciento del Producto Interno Bruto (PIB).

En la década de 1990, la Ciudad de México aprobó un reglamento que responsabilizaba a la Procuraduría General de Justicia del Distrito Federal del registro de los servicios de seguridad privada. Con esta legislación especial se inauguran las regulaciones al sector. En 2006 se publicó la Ley Federal de Seguridad Privada. Las entidades federativas cuentan con sus propias regulaciones de las empresas de seguridad privada, muchas de ellas basadas en la legislación federal.

La seguridad pública se fundamenta en el artículo 21 de la Constitución Política de Estados Unidos Mexicanos, que establece las bases de las instituciones de seguridad pública. En primer lugar, tiene competencia concurrente, es decir que su regulación, gestión y administración son responsabilidad federal, estatal y municipal.

En segundo lugar, su función es prevenir, indagar, perseguir y sancionar los delitos o infracciones administrativas. La rigen los principios de legalidad, objetividad, eficiencia, profesionalismo, honradez y respeto a los derechos humanos. Su carácter es civil, disciplinario y profesional. Las instituciones encargadas de la seguridad pública (de los tres niveles de gobierno y el ministerio público), se concentran en el Sistema Nacional de Seguridad Pública.

La constitución establece las normativas básicas para homologar las funciones de seguridad pública. El carácter auxiliar de la seguridad privada las enmarca dentro del Sistema Nacional de Seguridad Pública, de acuerdo con el artículo 151 de la Ley General del Sistema Nacional de Seguridad Pública.

BASES DE COORDINACIÓN DEL SISTEMA NACIONAL DE SEGURIDAD PÚBLICA

La Ley General del Sistema Nacional de Seguridad Pública establece las bases de coordinación y regulación nacional de los servicios de seguridad privada en el país. El artículo 150 dicta las modalidades para prestar el servicio mismas que refieren al monitoreo electrónico, a la seguridad, protección, vigilancia, custodia o traslado de personas, bienes o valores. También se consigna vagamente la distribución de competencias. La federación regula las empresas que prestan servicios en dos o más entidades federativas. Las entidades federativas regulan empresas que funcionan solo en su entidad. Los municipios no tienen facultades regulatorias.

Foto: 200 Degrees en Pixabay

La seguridad privada como la conocemos actualmente cobró fuerza en el mundo a partir de la década de los 80, debido a un entorno cada vez más complejo y ante amenazas crecientes por la inseguridad provocada por factores como el terrorismo, la pobreza extrema y las crisis que han afectado a toda la población

El artículo 150 señala al final que las empresas después de cumplir con la autorización de la Secretaría de Gobernación, deben cumplir con la regulación local. Esto contraviene la distribución de competencias y enreda la regulación, pues hace de competencia local a las empresas de competencia federal. Para resolver el enredo, la Suprema Corte de Justicia ordenó que la regulación local no sobrepasara los requisitos de la Ley Federal de Seguridad Privada. En la práctica se encuentra que la mayoría de las regulaciones estatales exceden los requisitos de la ley federal y regulan modalidades distintas a las establecidas en el artículo 150.

El carácter de auxiliar define a los servicios de seguridad pública como apoyo de las autoridades e instituciones de seguridad pública. El apoyo otorgable está sujeto por las siguientes condiciones: asistir en situaciones de urgencia, desastre o en caso de ser solicitadas por las autoridades de seguridad pública; el auxilio será en la modalidad autorizada; la autorización debe establecer condiciones y requisitos de colaboración con las autoridades de seguridad pública.

El artículo 152 de la Ley General del Sistema Nacional de Seguridad Pública dicta que las empresas de este sector se regirán por las normas y principios de esta ley, mismos que comparten con el cuerpo de seguridad pública; sin embargo, sus elementos operativos no tienen el carácter de autoridad. En consecuencia, el único principio aplicable es el respeto a los derechos fundamentales y las garantías constitucionales que tiene cualquier particular.

El artículo también obliga a los prestadores del servicio a aportar datos necesarios para el registro de su personal y equipo, proporcionar información estadística y sobre delincuencia al Centro Nacional de Información. Es necesario que se establezca una base de datos especializada para los servicios de seguridad privada en concordancia con la Ley Federal de seguridad privada.

Las empresas están obligadas a evaluar y aplicar controles de confianza a su personal operativo. Estos controles no pueden ser iguales a los presentados por la seguridad pública, y deben respetar los derechos a la intimidad, el honor, la propia.

LEGISLACIÓN COMPARADA: EL CASO DE ESPAÑA

España cuenta con tres modelos de regulación de la seguridad privada: el primero es "una regulación mínima, como de libre mercado; el segundo una regulación máxima, una legislación estricta y restrictiva; y el tercero combina definiciones amplias de seguridad y controles estrictos con una gran implantación social de los servicios privados".

La regulación en España inicia con reglamentos y decretos para la seguridad especializada, concorde al tipo de servicio y bienes protegidos, en los años 40. Para la década de 1970 se legisla en función de regular la seguridad de instituciones de crédito y en 1981 aparece el término seguridad privada y con la reglamentación para la prestación del servicio, unificando las normas preexistentes.

En España, en junio de 2014, entró en vigor la Ley 5/2014. Aunque la actual legislación mexicana retoma la experiencia española, la realidad de ambos países diverge bastante en la prestación de servicios sobre todo en la profesionalización de los servicios de seguridad privada, de la que carece la legislación mexicana.

LA ERA DE LA PROFESIONALIZACIÓN PARA LA SEGURIDAD PRIVADA EN MÉXICO

La profesionalización para la seguridad privada en México, aún en el más básico e indispensable ámbito de los requisitos de ley, presenta lo que se podría describir como condiciones de confusión y dificultad para su cumplimiento, derivado de la diversidad y discrepancia entre estas regulaciones institucionales, cuya principal repercusión son mayores costos para la operación, tanto directos como indirectos, resultado estos últimos de fenómenos como las prácticas de corrupción que encuentran sus espacios de oportunidad en la aplicación de atributos de discrecionalidad ante las imprecisiones, deficiencias y contradicciones en dichas regulaciones.

Esta situación estimula la creatividad empresarial para reducir el costo de cumplimiento con estas regulaciones, con recursos que van desde la aplicación esquemas mínimos a costa de sacrificar efectividad y calidad en los procesos de capacitación y adiestramiento, hasta la simulación de los mismos mediante la elaboración interna o la compra externa de los comprobantes correspondientes. Situación que permea en todos los segmentos de empresas, desde las micro, pequeñas y medianas, que integran el 60% de las fuentes de empleo, hasta las de mayor dimensión y prestigio.

Por su parte, los programas y certificaciones de entidades privadas, tanto nacionales como internacionales, que ofrecen capacidades de valor agregado respecto a los requisitos obligatorios establecidos por las instancias institucionales, aunque detentan una posición de prestigio en particular entre asociaciones y empresas con encomiables intereses y propósitos de mejora y de calidad en los servicios, así como cierto

Foto: Pixabay en Pexels

nivel de solvencia económica que les permite financiar su costo, no tienen una gran penetración en el ámbito de estos servicios, precisamente por los aspectos de costo y desvinculación con los requisitos obligatorios.

En consecuencia, se puede considerar que, en las condiciones actuales, se proyecta un escenario poco favorable para desarrollar los niveles de profesionalización idóneos que permitan sustentar la prestación de servicios de seguridad privada efectivos y de calidad. Un escenario en el que los buenos son la excepción cuando deberían ser la regla.

Por ello se estima conveniente considerar la imposición, desde las instancias institucionales y en ejercicio de sus atributos jurisdiccionales, de un ordenamiento claro de lineamientos para la profesionalización de la seguridad privada, que contemple facilidades para promover y propiciar su cumplimiento, así como mecanismos de control para verificar dicho cumplimiento, y sin olvidar un régimen de sanciones efectivas en caso de incumplimiento.

FACTIBILIDAD Y BENEFICIOS DE PROFESIONALIZAR EL PERSONAL DE SEGURIDAD PRIVADA

Los guardias de seguridad en una empresa de vigilancia prestadora de servicios son el recurso de mayor importancia porque son las personas que realizan la labor, por la cual los contratan.

Cuando contamos con profesionales que van a desempeñar una labor de calidad, las empresas de vigilancia podremos ofrecer un servicio con el que podrán estar tranquilos nuestros clientes de que, en cualquier eventualidad o novedad presentada de cualquier tipo, nuestro personal sabrá reaccionar y actuar de forma eficaz y eficiente, sin incurrir en errores que normalmente se justifican por el nivel de educación de los guardias de seguridad.

Foto: BodyWorn by Utility en Pixabay

Ofrecer soluciones y no más problemas a los clientes nos convierte en un sector de servicios que además de ser necesario se puede convertir en una solución, un apoyo y una ayuda para las personas que administran los diferentes entes que vigilamos. De igual forma con personal profesional en su labor podemos exigir informes detallados de su labor, tanto preventivos como de desempeño y así hacer medibles nuestros resultados y llegar a tener y mantener las certificaciones de calidad, que le dan un valor agregado muy importante a la prestación de nuestros servicios.

Hoy en día cuando se firman contratos de prestación de servicio de vigilancia deben estar sujetos a que las personas que se contratan para prestar el servicio desempeñen adecuadamente su labor y sean personas comprometidas y con la conciencia plena de la gran responsabilidad que tienen al ejercer esta actividad; sin embargo la falta de conocimiento de estas personas muchas veces no se ve reflejado sino hasta el momento en el que tienen que enfrentarse a los riesgos que conlleva esta labor y deben tomar decisiones, en la mayoría de casos equivocadas.

Debemos terminar con la imagen de ignorancia y mediocridad que tienen los guardias de seguridad en nuestro país, los salarios que en este momento está recibiendo este gremio son salarios que se igualan a los que en muchas empresas les pagan a empleados profesionales de diferentes áreas.

La importancia de un guardia de seguridad sepa cómo actuar y resolver novedades, es necesario que entienda que está trabajando para una empresa a la que le debe lealtad por ser su empleador y que este empleador a su vez se comprometió a prestar un servicio que representado por el guardia de seguridad debe estar comprometido con el cliente y debe dar resultados efectivos en la prestación de su servicio.

Siendo así estos empleados deben saber que aunque en el contrato de trabajo sólo existe un empleador, debe responderle a dos autoridades de forma eficaz y comprometida, el guardia de seguridad es contratado por una empresa de vigilancia que es su empleador con la cual sostiene un contrato de trabajo, en el cual se compromete a cumplir con unas consignas o funciones generales y propias del servicio de la vigilancia y seguridad privada, y adicional a esto con un reglamento de trabajo generado por la empresa y con todas las normas como empleado.

La principal problemática de una empresa de seguridad es el manejo del personal que se contrata para prestar los servicios de vigilancia, ya que los guardias de seguridad no son conscientes de la gran responsabilidad que tienen al ejercer esta labor y tampoco tienen los conocimientos necesarios para prestar un servicio efectivo.

Otro gran problema son las academias de seguridad no ofrecen cursos completos de teoría ni de entrenamiento, los cursos que ofrecen actualmente, son cursos con una intensidad horaria mínima en la que ven todos los temas de forma muy superficial, existen aspectos legales importantes que se deben conocer a fondo, como también formas de proceder en cada novedad que se pueda presentar en su labor.

Es necesario que las empresas de seguridad privada de nuestro país estén comprometidas con la colaboración para la educación de las personas que trabajan para ellas. Formar una mentalidad diferente a los guardias de seguridad, para que sean personas con ética profesional, comprometidas y responsables en su labor.

Es de gran importancia profesionalizar este gremio, es necesario que tengan la conciencia de la gran responsabilidad que tienen al ejercer esta labor y por consiguiente tener profesionales que tengan el conocimiento pleno de cómo proceder y actuar de manera adecuada y proactiva, para así mismo ofrecer un servicio de calidad a los clientes y tener un empleado satisfecho con su labor y la remuneración de la misma. ■

El artículo 152 de la Ley General del Sistema Nacional de Seguridad Pública dicta que las empresas de este sector se regirán por las normas y principios de esta ley, mismos que comparten con el cuerpo de seguridad pública; sin embargo, sus elementos operativos no tienen el carácter de autoridad

SEGURIDAD EN AMÉRICA

Suscripción Anual (6 ejemplares)

México: **$650 pesos**

Extranjero: **$270 dls.**

(incluye gastos de envío)

¡SUSCRÍBETE YA!

Cel. 55 5965 4582 (55) 5572 6005

telemarketing@seguridadenamerica.com.mx

www.seguridadenamerica.com.mx

Foto: Archivo

HÉCTOR ROBLES CONDE,

presidente de International Foundation For Protection Officers (IFPO) Capítulo México

1. ¿Cuáles son los objetivos de International Foundation For Protection Officers (IFPO)?

La Fundación Internacional para Oficiales de Protección está comprometida con el desarrollo profesional de oficiales de protección y supervisores, a quienes apoya y representa. Al promover estándares de formación y suministrar capacitación, educación y oportunidades de certificación accesibles, buscamos mejorar su posición profesional e incrementar y diversificar el valor de los servicios vitales que estos proveen.

2. En específico, ¿cuáles son los objetivos de IFPO México?

En México no existía un capítulo hasta octubre de 2021. Existían personas certificadas en las modalidades de IFPO: Certificados en CPO (Certified Protection Officer – Oficial Certificado en Protección), y CSSM (Certified in Security Supervision and Management – Certificación en Supervisión y Gerencia de Protección). Los objetivos de IFPO México son dar mayor promoción y presencia de IFPO en el país para que, de nuevo, IFPO sea considerado como una alternativa seria, profesional y respetable; una alternativa muy atractiva de capacitación operativa, táctica y estratégica. México es un mercado muy importante en America Latina. No se podía pensar en no tener mayor fuerza en México si el HAB de IFPO quería crecer y consolidarse a nivel global.

3. ¿Cuáles son los beneficios de pertenecer a la IFPO?

IFPO es una organización internacional creada en 1988, con su Oficina Central en Florida (USA), con representación académica e instructores en 56 países, presente en más de 140 países con miembros, alumnos y profesionales certificados por IFPO, y con más 96 mil certificados por IFPO en todo el mundo. En Latinoamérica tiene presencia en: Honduras, Argentina, Ecuador, Perú, Venezuela, República Dominicana, Guatemala, Brasil, Nicaragua, Paraguay, Uruguay, Colombia, Costa Rica, Cuba, El Salvador, Bolivia, Chile y México.

4. ¿Cómo llegó a liderar la IFPO México?

Al no existir un capítulo en México, el HAB de IFPO liderado por Kevin Palacios (Ecuador) y Alfredo Yuncoza (Venezuela) se ponen en contacto con Ivan Ivanovich para invitarlo a ser parte de la junta del HAB IFPO. A su vez por la necesidad de arrancar de manera urgente e inmediata, Ivan Ivanovich me invita a liderar el capítulo en México y formar la junta directiva local.

5. ¿Cuál es la importancia de capacitar y certificar a un Oficial de Protección?

Siempre es importante y una obligación legal, al menos en México, el capacitar a la gente para que desempeñe mejor su trabajo y tenga mejores oportunidades de crecimiento laboral en el futuro. La profesionalización de los que participamos en el sector de seguridad privada es indispensable para dar un mejor servicio, crear confianza y credibilidad, así como para la dignificación de todos en el sector.

Certificar a un Oficial de Protección bajo el sello organizaciones internacionales, contribuye a la estandarización de las funciones operativas, tácticas y estratégicas. La Certificación CPO da la oportunidad de obtener los conocimientos generalistas básicos y hasta un nivel de supervisión de diferentes ramas de la seguridad privada.

En México estamos buscando alinear el CPO y CSSM con CONOCER. Es una labor que llevará un poco de tiempo, al menos un año en el mejor de los casos. Sin embargo, las certificaciones de IFPO son sumamente relevantes en los niveles operativos y tácticos, es decir de un nivel principiante a nivel medio. ■

PROTECCIÓN A TRAVÉS
IFPO
DEL CONOCIMIENTO

Únete
a la red de empresas
y profesionales IFPO en
Hispanoamérica

IFPO
MIEMBRO

La membresía CORPORATIVA en IFPO otorga beneficios a todos los trabajadores y a tu empresa:

- ***Reconocimiento internacional***
- ***Beca garantizada***
- ***Acceso a eventos exclusivos***
- ***Descuentos especiales***

+593 95 899 6683 ***https://ifpo.es/membresia-corporativa***

LA PROTECCIÓN EJECUTIVA EN EL ÁMBITO PRIVADO Y SU REALIDAD EN AMÉRICA LATINA

Foto: pixel-shot.com - Freepik

El reto de proteger a personas que viajan en un mundo inseguro

ECUADOR | Francisco Hernández

La inseguridad que viven nuestros países en Latinoamérica es cada vez mayor, la delincuencia, el narcotráfico con todas sus aristas no dan tregua y esto ha significado un gran reto para las personas que trabajamos en el área de protección, y es justamente éste último punto que, orientado hacia la seguridad de personas, crea un verdadero desafío para quienes tienen bajo su responsabilidad vidas de seres humanos.

Existe una brecha bastante extensa entre la protección a personas en medio público como parte de un estado y la protección a personas en el ámbito privado, el primero tiene la capacidad económica, recurso humano, medios técnicos e infraestructura casi ilimitados para cumplir con su misión, de hecho, armamento, vehículos, personal militar, policial, inteligencia, equipos con alta tecnología, y en algunos casos aeronaves, hacen de éste un esquema de seguridad muy complejo y a la vez muy costoso, en donde solamente un estado podría sostenerlo.

Por el otro lado, tenemos al mismo objetivo de protección a personas, pero desde el ámbito privado, en el cual muy pocas empresas o personas podrán darse el "lujo" de gastar millones de dólares en esquemas complejos de protección. Me refiero a esquemas que conformen caravanas de tres o más vehículos, equipos de avanzada, motorizados de apoyo, equipos de reacción, centro de operaciones, inteligencia y demás elementos que intervienen en un óptimo esquema de protección.

A lo mejor empresas multinacionales o transnacionales reconocidas pueden sostener esquemas similares, pero generalmente la mayoría de empresas locales, grupos económicos importantes e inclusive las antes mencionadas no tienen la capacidad económica para afrontar esquemas complejos, o, si la tienen, la protección de personas no es su prioridad y es ahí en donde la realidad para la protección a personas en América Latina es poco comprendida por las empresas o sus directivos.

Foto: edophoto - Freepik

ENTRENAMIENTO

Uno de los errores más comunes que se presenta en la industria de la protección a personas en el ámbito privado, es el entrenamiento, que difiere en algunos aspectos de la realidad que vivimos, entrenamientos dirigidos para formarse como guardaespaldas, escoltas, protectores o como se denomine en cada país, en los cuales algunas organizaciones dedicadas a la capacitación venden programas de entrenamientos para convertirse en guardaespaldas muchas veces sin tomar en cuenta el perfil requerido y dando falsas expectativas a ingenuos participantes.

En Latinoamérica es evidente la diferencia salarial comparando con países más desarrollados, donde un trabajo de este tipo no llega a costar menos de 5 mil dólares mensuales, y por ende existe un estancamiento de la profesionalización

En el entrenamiento aprenden y repasan, formaciones de tres o más elementos para proteger a un ejecutivo, avanzadas, reacción, etcétera, cuando en la realidad mantener un solo equipo con dos personas y un vehículo ya es un logro. Por el lado de la conducción es similar, en los entrenamientos se realizan varias maniobras evasivas-defensivas siendo el primer error el utilizar vehículos que, son generalmente rentados, con un centro de gravedad bajo y una fuerza G (capacidad de aguantar fuerzas laterales) muy alta, que prácticamente hacen del entrenamiento una película al estilo 007, pero una vez que terminan y regresan a laborar, la realidad cambia, y continúan utilizando los vehículos en su mayoría SUV con centros de gravedad altos.

En algunos casos blindados nivel NIJ II o III que los hacen muy pesados, y cuyas fuerzas G han variado y que obviamente no podrán ejecutar las maniobras aprendidas en los autos del entrenamiento, conllevando más bien en un peligro constante para su vida y la de sus protegidos, la experiencia nos ha demostrado un sinnúmero de ocasiones en donde el equipo de seguimiento que generalmente utiliza un vehículo de una gama más baja que el principal, termina colisionando con el mismo o peor aún teniendo accidentes graves con otros vehículos debido al "seguimiento" que tratan de hacerlo con un vehículo con menores prestaciones y tecnología.

La instrucción debe adaptarse a la realidad de cada entorno, de cada país, de cada problema o amenaza que exista y que esté plenamente identificado con un correcto análisis de riesgos.

Un entrenamiento generalizado no da la claridad y las herramientas necesarias para que un protector o escolta se desenvuelva eficientemente, ya que no es lo mismo el esquema de protección para una persona que tiene en riesgo su vida, que a una persona que tiene el riesgo de ser secuestrado o un artista o figura mediática, los esquemas son diferentes.

Con esto no quiero decir que un entrenamiento generalizado no sea bueno, siempre hay algo que aprender, pero dependerá mucho del gerente de protección, que complemente las competencias, habilidades y aptitudes que requiere una persona dedicada a esta profesión y en los escenarios que más se adapten a su propia realidad.

SALARIOS JUSTOS

Poco se habla sobre los salarios justos que una persona dedicada a la protección debe percibir, basándonos en lo anteriormente dicho, un adecuado entrenamiento de una persona para proteger la vida a seres humanos demanda un alto valor económico, y que muchas veces lo hacen a costo personal, aspectos importantes como un estado físico óptimo, conducción evasiva-defensiva, conocimiento de sistemas electrónicos de seguridad, manejo de armas, defensa personal, conducción de motocicletas, inteligencia, protocolo, entre otros, equivale a muchas horas de capacitación y un importante recurso económico.

En el entrenamiento aprenden y repasan, formaciones de tres o más elementos para proteger a un ejecutivo, avanzadas, reacción, etc., cuando en la realidad mantener un solo equipo con dos personas y un vehículo ya es un logro

En Latinoamérica es evidente la diferencia salarial comparando con países más desarrollados, donde un trabajo de este tipo no llega a costar menos de 5 mil dólares americanos mensuales, el promedio en nuestro medio es bajísimo y por ende existe un estancamiento de la profesionalización de personas en ésta actividad, las empresas, empezando por las de servicios de seguridad deben replantear su apreciación y valoración de lo que significa un profesional de protección a personas y darle a ésta profesión el puesto que se merece.

Para finalizar, es importante que el gerente de seguridad o de protección de una empresa asigne el presupuesto necesario para mantener un esquema de seguridad de protección a ejecutivos óptimo, eficiente y eficaz y eso dependerá mucho de la habilidad, experiencia, el correcto análisis técnico del proyecto a fin de que sea comprendido y acogido por el CEO de una organización. ■

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

Francisco Hernández, CPP,
gerente general de Ottoseguridad Cia. Ltda.

Más sobre el autor:

CERTIFICACIÓN DE COMPETENCIAS VS. CERTIFICACIÓN ACADÉMICA

Para generar buenos elementos de seguridad no sólo es necesario formarlos, sino analizar las competencias que ellos requieren para realizar bien su función y certificarlas

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

MÉXICO | Ulises Figueroa Hernández

Cuando concluimos un programa de estudios ya sea de preparatoria, licenciatura, maestría, doctorado, etc., incluso en algún otro aspecto del ámbito formativo, se obtiene un documento que certifica que hemos concluido un programa de estudios, hemos presentado y aprobado los exámenes pertinentes y entregado de manera satisfactoria todos los requisitos, trabajos y prácticas que se solicitaron; esto se refleja en un certificado de estudios.

De manera que un certificado de estudios certifica que hemos adquirido un conjunto de conocimientos y habilidades que nos preparan para integrarnos con éxito al campo laboral de la rama de estudios de que se trate, esto en sí representa que estamos preparados para ejecutar un trabajo, mas no significa ni mucho menos garantiza que ese trabajo lo vayamos a desempeñar bien con los estándares de calidad que la función requiere.

Para explicar esto me permito poner un ejemplo: existen muchas personas que saben conducir un vehículo, pero no significa ni garantiza que todas las personas que saben conducir un vehículo sean buenos conductores, saber conducir un vehículo es una habilidad, mientras que ser un buen conductor es una competencia.

Aterrizando la idea al ámbito de la protección a personas, no es lo mismo haber estado en un curso y adquirir un conjunto de habilidades o conocimientos para después salir a la calle a brindar un servicio de seguridad y desempeñarlo con éxito; al haber concluido un curso exhaustivo de Protección a Funcionarios tal vez se obtenga un certificado académico que haga constar

Se debe elaborar un listado de los elementos que necesita una persona para ser no sólo un escolta, sino un buen escolta en términos de resultados para estandarizar sus funciones

que se concluyó con todas las asignaturas del curso y se realizaron las prácticas correspondientes pero eso no garantiza un buen desempeño en el campo laboral.

Por otra parte, una certificación de competencias se realiza cuando una vez adquiridos los conocimientos y habilidades necesarias, estas se ponen en práctica en el puesto laboral real y se demuestra su efectividad a través de desempeños, productos y conocimientos que se recopilan en un portafolio de evidencias por un evaluador experto en la función.

La certificación de competencias no es lo mismo que la certificación formativa, porque una cosa es la formación y otra cosa es la función; para certificar una competencia se requiere un documento que defina en términos de resultados la actividad formativa, pero enfocada al puesto laboral real y no a la formación en sí, ese documento se llama Estándar de Competencia.

Volviendo al ejemplo del conductor si hacemos una lista de lo que necesita una persona para saber conducir y otra lista de lo que necesita una persona para ser un buen conductor y contrastamos ambas, nos daremos cuentas de que no son los mismos elementos los que se necesitan, los elementos que contenga la lista de lo que se necesita para ser un buen conductor son los elementos de los que se compone un Estándar de Competencia.

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

PROTECCIÓN A PERSONAS

Si trasladamos lo anterior al ámbito de la Protección a Personas, es muy importante que las instituciones de seguridad sepan diferenciar entre la formación y la competencia, porque para generar buenos elementos de seguridad no sólo es necesario formarlos y dejarlos a la deriva cuando salen a la calle, sino analizar las competencias que ellos requieren para realizar bien su función y certificarlas a través de un Certificado de Competencias para ir generando un verdadero capital humano reflejado en especialistas en Protección a Personas.

Derivado de lo anterior se debe elaborar un listado de los elementos que necesita una persona para ser no sólo un escolta, sino un buen escolta en términos de resultados para estandarizar sus funciones.

Un ejemplo de esto enfocado a la Protección a Personas es que en los cursos de academia se les enseña distintos tipos de desenfundes como lo son desenfunde a la cadera, desenfunde israelí, desenfunde al pectoral, etc., pero eso sólo es la formación, si enfocamos lo anterior a la función entonces tendremos que definir qué resultados esperamos ver con cualquiera de esos desenfundes y seguramente encontraremos que se lo que se espera para ser competente en la función no es realmente el desenfunde, sino el resultado del mismo.

¿Qué se espera de un buen desenfunde? Lo que se espera es que cualquiera que sea el movimiento que realice el escolta, ese movimiento (desenfunde) sirva para neutralizar de manera efectiva una amenaza y poner a salvo a su principal, por lo tanto la competencia no es el tipo desenfunde, sino el resultado efectivo del mismo, eso es estandarizar una competencia.

> No es lo mismo haber estado en un curso y adquirir un conjunto de habilidades o conocimientos para después salir a la calle a brindar un servicio de seguridad y desempeñarlo con éxito

Por lo tanto una vez más mi invitación a certificar las competencias del personal de seguridad en este caso de los escoltas con la intención de contar con personal capacitado, pero además certificado en las funciones que realizan, no desde la formación sino desde el puesto laboral real.

Vaya lo anterior con cariño y admiración a todas las personas que se dedican a tan loable labor de proteger y servir. Saludos. ■

Ulises Figueroa Hernández,
Licenciado en Seguridad Pública del Servicio de Protección Federal y Metodólogo en la Elaboración de Estándares de Competencia.

Más sobre el autor:

Foto: Erick Martínez / SEA

MAKOTO NANCARROW: ALGUIEN EN QUIEN CONFIAR

Hijo de migrantes, con tres influencias culturales y una pasión por la seguridad que lo motiva a proteger y ser protegido

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Grandes personas y personajes han llegado al sector de la seguridad sin saber que terminarían aquí. La mayoría de ellos, convirtiendo una profesión en una pasión, en una forma de vida y sobre todo, contribuyendo por el bienestar de su país. David Makoto Nancarrow Sugiura es uno de estos personajes de la seguridad que combina la cultura, humildad y empeño de quienes han y siguen siendo sus ejemplos de vida.

"Vengo de una familia de migrantes, de madre japonesa y de padre norteamericano, pero orgullosamente nacido en México. Mi madre es arqueóloga por la UNAM (Universidad Nacional Autónoma de México) y mi padre fue compositor de música contemporánea. Ellos son mi inspiración y ejemplo de vida, son seres humanos que tuvieron la fortuna de encontrar su pasión a una corta edad, siempre humildes, entregados, dedicados y trabajadores", explicó.

David Makoto es Ingeniero Civil por la Universidad Iberoamericana (plantel Ciudad de México), durante gran parte de su vida se dedicó a la construcción, tanto de casas habitación, como de corporativos, pero siempre tuvo la inquietud sobre la seguridad y la mitigación de la violencia enfocada en México. Profesionalmente, colaboró con el gobierno de Puebla a la cabeza de una subsecretaria con el nombre de "Cultura para la No Violencia", en la que trabajó en los polígonos más violentos y en los centros penitenciarios, utilizando la cultura y el arte para prevenir y mitigar la violencia en el Municipio de Puebla. Ahí se abrió la puerta hacia la seguridad.

DOORMAN: CALIDAD, COMPROMISO Y ENTREGA

Hace unos años atrás, Makoto tuvo la oportunidad de participar como socio en Doorman Plus S.A. de C.V., empresa de Seguridad Privada fundada hace 25 años por la visión y compromiso del Coronel Luis Méndez Parra, con la finalidad de proveer servicios de seguridad a la población mexicana.

"Llegué a Doorman como socio y surgió la oportunidad de liderarla. Sin conocimiento del negocio, me adentré en este fascinante mundo de la seguridad, tomando cursos y *webinars*, leyendo libros de todas las ramas de la seguridad y conociendo gente maravillosa del gremio que me ha abierto las puertas a su conocimiento y experiencia. Así es como se volvió la seguridad una pasión para mí. Me generó un sentido de compromiso y de lealtad para tener un México más seguro", comentó.

Foto: Cortesía Makoto Nancarrow

Doorman Plus está presente en: edificios corporativos y oficinas, condominios y residencias, y locales, centros comerciales y hoteles, principalmente. Su personal está capacitado en atención a clientes, protección civil, combate de incendios, defensa personal y control de accesos.

Foto: Cortesía Makoto Nancarrow

Foto: Cortesía Makoto Nancarrow

"Todo ser humano tiene en el fondo la necesidad de proteger y ser protegido, en mi caso encontré mi pasión en la protección y servicio hacia otros"

MÁS ALLÁ DE LA SEGURIDAD

Pasatiempo favorito:
Crossfit.

Grupo de música o cantante favorito:
U2.

Programa o serie de TV favorito:
Seinfeld.

Película favorita:
Ferris Bueller's Day Off / Top Gun.

Libro favorito:
"*Bushido (El libro de los cinco anillos)*" de Miyamoto Musashi.

Destino favorito de vacaciones:
Japón y cualquier lugar de México.

Bebida favorita:
Sake y pulque.

Comida favorita:
Mexicana y japonesa.

Actor favorito:
Anthony Hopkins.

Personaje favorito:
Spiderman.

ASOCIACIÓN DE PALABRAS

México:
Mi casa.

Seguridad:
Doorman.

Presidente:
Decepción.

Gobierno:
Sin compromiso por México.

Policía:
Mucho por trabajar.

Familia:
Motor de vida.

Amigos:
Familia.

Doorman:
Alguien en quien confiar.

Una de las metas profesionales de David es continuar con el legado del Cnel. Luis Méndez Parra, "ser una empresa confiable y comprometida con la seguridad de sus clientes, pero sobre todo, que Doorman sea un referente de calidad, compromiso y entrega trabajando en alianzas por un México Seguro", puntualizó.

COVID-19: APRENDIZAJE DE VIDA

Estamos en ese momento de la vida en que usar cubrebocas ya es parte de nuestra rutina, en el que incrementan los contagios por COVID-19, pero ya sabemos los protocolos de bioseguridad a seguir, no obstante todos llevamos alguna secuela que esta pandemia dejó en nuestras vidas.

"Estamos a poco más de dos años de que inició la pandemia, pasará mucho tiempo y seguiremos acordándonos de los fallecidos, los enfermos y las secuelas que dejó esta enfermedad, no sólo las graves consecuencias económicas, sino también el impacto social y en la salud mental. Creo que una de las cicatrices más grandes y catastróficas se verá reflejada en la educación", externó Makoto y enumeró algunas de las lecciones de vida que le dejó la pandemia:

1. La vida es muy frágil.
2. La salud es nuestro más preciado tesoro.
3. Las cosas más importantes son los pequeños detalles de la vida te ofrece.
4. Hay que cambiar muchos paradigmas en la educación y la salud.
5. Encontrar la armonía y equilibrio en nuestro día a día.
6. El valor de la espiritualidad.

MÉXICO SEGURO

La industria de la seguridad privada representa hoy en día un importante porcentaje en la economía del país, casi el dos por ciento para ser precisos, además de generar más de 700 mil empleos en todo el país. Pero para quienes lo integran, no es sólo economía e ingresos, inversión y negocio, es un proyecto profesional y personal para contribuir con la seguridad del país, reducir los índices de violencia y contribuir en el bienestar de la sociedad, David Makoto es uno de estos personajes que están en constante profesionalizar para cumplir estas metas.

"Creo que todo ser humano tiene en el fondo la necesidad de proteger y ser protegido, en mi caso encontré mi pasión en la protección y servicio hacia otros. También considero que todos nuestros actos, conductas y comportamientos tienen consecuencias en la vida, por lo que los momentos malos y buenos que experimentamos son importantes, son lecciones de vida que nos van a instar a madurar y a crecer, por ello trabajo todos los días, para ser un mejor ser humano, comprometido y entregado a su familia, amigos y a México", finalizó. ■

LA TÉCNICA DE ENTREVISTA SUE

Foto: Creativeart - Freepik

COLOMBIA | Gonzalo Gómez Sanabria

La Strategic Use of Evidence (SUE) es una herramienta de investigación en la detección de mentiras

La ciencia ha demostrado que los entrevistadores o interrogadores que emplean únicamente señales de lenguaje corporal como herramienta para detectar el engaño durante una entrevista, presentan un fuerte sesgo frente a la mentira. Se ha encontrado que son más propensos a diagnosticar estados como si se presentaran mentiras cuando son realmente veraces. Mientras tanto, las personas inocentes están siendo acusadas injustamente y las señales que sí indican engaño pasan desapercibidas. Con el tiempo, los entrevistadores van a reconocer la abrumadora evidencia científica que exige prestar más atención a las señales verbales como un método mucho más productivo de detectar el engaño durante la entrevista.

Vale destacar que la preparación de la entrevista es fundamental para su éxito, y esto implica no sólo conocer previamente los hechos, entender el caso, la personalidad e historia del sujeto, los cuales deben dominarse; sino además el tener bastante claro el plan de abordaje a seguir y los diversos indicadores de mentira o verdad de los que hoy día se tiene evidencia científica. En este mismo sentido el entrevistador debe conocer bien las desventajas de una mala planificación y preparación de la entrevista, a continuación, se presentan algunas:

- Se podría pasar por alto las pruebas o evidencias relevantes.
- No identificar las incoherencias en la versión o las mentiras.
- Podría hacer pausas innecesarias para obtener más información.
- Podría tener que realizar más entrevistas adicionales innecesarias con la misma persona.
- Puede perder el control de la entrevista.
- El entrevistado podría notar la falta de preparación y sacar ventaja.

Por otro lado, la falta de evidencia empírica que apoyará en sus inicios la aproximación no verbal-emocional en detección de mentiras, propició el desarrollo de investigaciones científicas. La psicología cognitiva es una de las áreas que ha desarrollado estas investigaciones. Sostiene esencialmente que mentir es cognitivamente más complejo o desgastante para el cerebro que decir la verdad, y que un aumento artificial de la dificultad cognitiva provocado por el investigador durante una entrevista, hará que el mentiroso muestre señales delatoras de sobrecarga cognitiva.

Es por esto por lo que la ciencia ha impulsado a que los profesionales tengan un conocimiento más claro sobre el funcionamiento de la memoria y del sistema cognitivo para poder comprender el significado de los indicadores de carga cognitiva. Por su parte, los científicos también deben desarrollar modelos cognitivos de la mentira y elaborar las hipótesis a partir de mecanismos y procesos cognitivos específicos.

La teoría sobre la carga cognitiva en la detección de mentiras defiende que las operaciones mentales que debe hacer una persona que miente al construir y contar su historia son muy distintas de las que debe hacer una persona sincera. Algunos investigadores en detección de mentiras han argumentado que inventar una historia falsa requiere algún grado de desgaste mental, lo cual resulta mucho más complejo que contar alguna situación cotidiana.

Vrij y Granhag (2014, citados por Blandón-Gitlin et al., 2017, p. 98) enumeran varias razones por las cuales mentir durante un interrogatorio o una entrevista puede ser cognitivamente más complejo. Se requiere un esfuerzo mental mayor que cuando se dice la verdad, se desarrolla un gran consumo de recursos cognitivos. Quien miente se ve abocado a inventar una historia concreta que no contradiga lo que el oyente conoce o pueda llegar a determinar.

Debe procurar que no se le escape información relevante al igual que debe memorizar la historia falsa que está contando para poder repetirla en el futuro de ser requerido. Además, al ser consciente de que está mintiendo, debe prestar mucha atención a su propia conducta y procurar controlarla con el fin de ocultar deslices corporales o posibles indicios que evidencien su engaño. El que está falseando una historia también debe estar muy atento al comportamiento del receptor para ver si muestra alguna señal de asombro, sospecha o decepción y debe seguir deliberadamente con su actuación.

Cuando al entrevistado se le hace una pregunta, es posible que en su conciencia la verdad se active automáticamente. Si su intención es mentir, deberá inhibirla. El pretender decir algo que no es verdad, el inventar una versión de la realidad es un hecho que no siempre sucede automáticamente. Es un acto deliberado y trabajoso. Esta teoría ha hecho que algunos procedimientos de entrevista pretendan incrementar más aún el esfuerzo cognitivo del entrevistado. Esto resultará más perjudicial para el mentiroso porque puede llegar a mostrar señales de sobrecarga cognitiva derivada de la propia actividad de mentir, además puede llegar a mostrar signos observables de este desgaste a través de la conducta, por lo tanto se deben estudiar aspectos como vacilaciones y errores al hablar, velocidad del habla, movimientos de piernas y pies y cambios en el parpadeo.

Específicamente la técnica de entrevista SUE (Strategic Use of Evidence), de los investigadores Maria Hartwig, Anders Granhag y Leif Strömwall, desarrollada desde el año 2005 en Suecia, como un tipo de entrevista policial o investigativa que pretende generar aumento artificial de la carga cognitiva y dentro de la cual se maneja la evidencia que dispone el entrevistador de modo estratégico, desplegando cuidadosamente la información incriminatoria administrada sobre el sospechoso, puede generar inconsistencias en las declaraciones de mentirosos y también obtener información adicional frente a un evento. El fundamento de esta técnica radica en los diferentes estados mentales con los que sinceros y mentirosos afrontan las entrevistas o los interrogatorios (Granhag et al., 2007).

> La técnica SUE señala que, si se le pone de preaviso al sospechoso de que existe evidencia en contra de él, que pueden existir declaraciones, video, huellas u otras pruebas, el entrevistado inventará una historia que encaje con dichas pruebas

Un estudio empírico realizado por los psicólogos Masip y Herrero en el año 2013 sobre las medidas que personas culpables e inocentes toman durante una entrevista para mostrarse convincentes frente a preguntas específicas, evidenciaron que la tendencia a preparar una estrategia de antemano y tomar medidas frente a preguntas relevantes directas y centrales del caso es mayor en culpables que en inocentes.

Existen varios factores que el mentiroso debe considerar en una entrevista y que tiene un nivel de exigencia cognitivo muy elevado, como primera medida debe monitorear y controlar su propia conducta para parecer honestos, segundo están muy atentos a las reacciones del investigador con el ánimo de evaluar si están saliéndose con la suya, tercero deben recordar lo que han dicho anteriormente y a quien se lo han dicho para mantener la coherencia de la versión; esto genera mucha preocupación aunado a que deben suprimir de sus recuerdos la verdad de lo sucedido.

Además, los entrevistados culpables evitan mencionar la información incriminatoria, y si se les confronta con ella, la niegan. Además, distraen la atención del entrevistador hacia otros temas. La teoría agrega que esta no es sino una forma particular de la tendencia general en los seres humanos para evitar una estimulación aversiva y huir de ella si se presenta. Por el contrario, las personas inocentes no tienden a la evitación y la huida. Se perciben como dispuestos a proporcionar información para ayudar al investigador (Masip y Herrero, 2015).

Algunas técnicas de entrevistas recomiendan que cuando se sospecha de alguien hay que confrontarlo desde el principio de la actividad con la evidencia en su contra con el fin de que el entrevistado dude, se arrepienta y confiese. Por el contrario, la técnica SUE

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

señala que, si se le pone de preaviso al sospechoso de que existe evidencia en contra de él, que pueden existir declaraciones, video, huellas u otras pruebas, el entrevistado inventará una historia que encaje con dichas pruebas, distorsionando la evidencia o justificando su presencia en la escena del crimen, no admitirá nada que pueda incriminarlo.

Por otro lado, si la persona es culpable y cree que no dejó ninguna evidencia o prueba, puede que niegue conocer a la víctima o niegue rotundamente haber estado en la escena del crimen. Al disponer el entrevistador de evidencia incriminatoria se sabrá que está mintiendo, comprobando, hasta entonces la presunta culpabilidad. El entrevistador iniciará la confrontación positiva de una manera en la cual va a ir mostrando la evidencia poco a poco y preguntado al sujeto cual es la razón por la cual se están presentando o se presentaron las inconsistencias en su versión y por qué no coincide con la información con la que se dispone.

Es importante tener en cuenta que es una técnica compatible con modelos éticos probados y ampliamente utilizados en entrevistas de investigación como son: el modelo PEACE la Gestión de la Conversación, entrevista estándar de investigación y La Estrategia General de Entrevistas, entre otros. Es por esto que, la técnica SUE añade tácticas científicamente fundamentadas, para optimizar el valor de la información que dispone el entrevistador, en tanto que se deben conocer los dos objetivos de esta metodología como son la detección de indicadores de engaño que puedan ir guiando al entrevistador para determinar si el sospechoso miente o no y la construcción sólida del caso, estos serían los dos principales objetivos (Granhag y Hartwig, 2014).

PASOS DE LA ENTREVISTA SUE

- **Planificación:** el entrevistador examina la información, documentación o evidencias que dispone del caso y profundiza en la que pueda ser potencialmente incriminatoria, en especial aquella que es probable que el sospechoso ignore o desconozca que exista.

- **Recuerdo libre:** el entrevistador hace preguntas abiertas. Le pide al sujeto que cuente lo que hizo en momentos en los cuales se cometió el delito o el hecho bajo investigación: dónde se encontraba, con quién estaba, quién lo vio o quiénes puede declarar que lo vieron, etc. Durante esta fase los culpables no mencionan información potencialmente incriminatoria, el entrevistador tampoco debe mencionar que tiene evidencia o información incriminatoria.

- **Preguntas:** después de la narración libre de lo que conoce o es testigo, el entrevistador formula preguntas cerradas y concretas. Además, puede hacer preguntas centrales sobre temas potencialmente incriminatorios en los cuales ya se puede saber la respuesta. Durante esta fase de preguntas, los culpables muestran más inconsistencias que los inocentes.

- **Comprobación y compromiso:** el entrevistador hace un recuento de lo manifestado, es decir, repite al sospechoso las respuestas dadas por este con el fin de que le corrija si hay algo erróneo en lo que se le dijo al investigador, que agregue algo más y aclare si algo de lo manifestado no está bien o no se entendió como debía. Con ello también se logra que el sospechoso se comprometa con su declaración.

- **Contraste entre la declaración y la evidencia incriminatoria:** si hay obvias inconsistencias entre las declaraciones del entrevistado y la evidencia de la que disponía el entrevistador, se le pide al sospechoso que las explique una a una. Inicia así el empleo estratégico de la evidencia. Según Granhag, la Técnica SUE propone que la consistencia entre la evidencia disponible y la historia que cuenta el sospechoso es un indicador de veracidad.

Los nuevos enfoques para la realización de las entrevistas especializadas ponen el énfasis en la carga cognitiva y los procesos de memoria, ya que la mentira es un asunto tortuoso y complejo para el cerebro, pues la persona busca que la verdad natural y sencilla para ella sea ocultada, y este esfuerzo termina por manifestarse de modo inconsciente pero claro. Plantear preguntas inesperadas, repetir preguntas, pero formuladas de manera un poco diferente, reiterar preguntas incómodas, o permitir que el sujeto otorgue su versión de los hechos y luego expresamente contrastarla en la entrevista con la evidencia incriminatoria, pueden hacer surgir estas manifestaciones que evidencian el engaño o que permitan conocer lo que es verdad. ■

REFERENCIAS

- *Granhag, P. A, Strömwall, L., y Hartwing, M. (2007). The SUE-technique: The way to interview to detect deception. Forensic Update, 88, pp. 25-29.*
- *Masip, J., y Herrero, C. (2015). Nuevas aproximaciones en detección de mentiras II. Estrategias activas de entrevista e información contextual. Papeles del Psicólogo, 36, pp. 96-108.*
- *Granhag, P. A. and Hartwig, M. (2014) The Strategic Use of Evidence Technique, in Detecting Deception: Current Challenges and Cognitive Approaches (eds P. A. Granhag, A. Vrij and B. Verschuere), John Wiley & Sons, Ltd, Chichester, UK. doi: 10.1002/9781118510001.ch10*
- *Granhag, P. A., Strömwall, L. y Hartwig, M. (2007). The SUE-technique: The way to interview to detect deception. Forensic Update, 88, 25-29.*
- *Vrij, A., Fisher, R., Mann, S. y Leal, S. (2008). A cognitive load approach to lie detection. Journal of Investigative Psychology and Offender Profiling, 5, pp. 39-43. http://dx.doi.org/10.1002/jip.82*
- *Vrij, A., y Granhag, P. A. (2014). Eliciting information and detecting lies in intelligence interviewing: An overview of recent research. Applied Cognitive Psychology, 28(6), pp. 936-944. https://doi.org/10.1002/acp.3071*

Gonzalo Gómez Sanabria,
Psicólogo, Mágister en Seguridad Pública y gerente en CCO Consultores en Credibilidad y Confianza.

Más sobre el autor:

COLEMAN

Jetlife

EL PODER DE VOLAR

RENTA DE AVIONES PRIVADOS Y HELICÓPTEROS

Contamos con: Phenom 100, Phenom 300, Legacy 600 y Bell 407

Powered by:
SEGURIDAD EN AMÉRICA

IS-BAO

OPERATOR

AEROPUERTO INTERNACIONAL DE TOLUCA

Calle 1, Hangar 1,
Toluca, Estado de México. C.P.50209.
krauda@seguridadenamerica.com.mx

Tel. 55.2105.2230

LA ISO 27001, ¿QUITA O DA PROTAGONISMO A LA PROTECCIÓN FÍSICA DE LOS ACTIVOS?

Foto: Creativeart - Freepik

ECUADOR | José Echeverría

La norma ISO 27001 aporta a la cultura de seguridad y al análisis de riesgos para gestionar los procesos en una empresa

En el camino de la transformación digital de las organizaciones, donde la tecnología y la virtualidad son áreas de consumo general para los colaboradores; conscientes de que hace casi una década los riesgos virtuales superaron en número a los riesgos físicos, nos deja la impresión que casi a la fuerza los directivos de la mayoría de estas organizaciones, están enfocando su atención en los activos digitales más que en los físicos. Bajo esta premisa, podría entenderse que la palabra seguridad y todo lo que conlleva se estaría también "digitalizando".

Un indicador que da sentido a esta conjetura es el hecho de que cada vez hay más ofertas laborales para los CISO (*Chief Information Security Officer*) en comparación con los CSO (*Chief Security Officer*), y que los primeros están asumiendo los retos como cabezas o responsables de la protección corporativa a nivel global, porque su perfil está ya enfocado hacia lo digital, hacia esa anhelada transformación.

Es importante considerar que ni los activos físicos ni los riesgos a los que están expuestos, se han reducido en una empresa, al contrario, debido a diferentes factores que se vive en toda Latinoamérica este tipo de riesgos se han incrementado. El narcotráfico, la violencia, la delincuencia organizada y común, la extorsión, el fraude, la corrupción, etc., siguen presentes y pululan cual virus en todas las organizaciones.

La prevención de pérdidas y las contramedidas que se deben aplicar para mitigar esos riesgos necesitan de un presupuesto que, en línea opuesta a su incremento podría hoy estar estancado o inclusive mermado, como pasó en épocas de pandemia, mermado al igual que el protagonismo de la "seguridad física" que estaría también reduciéndose por efectos de esta mentada transformación digital.

La pregunta que sale a flote es: ¿Cómo apoyarse en esta dinámica digital para hacer énfasis en la protección física de los activos? Los sistemas de gestión y los estándares internacionales como las ISO (*International Organization for Standarization*) que son aplicadas en muchas organizaciones, en buena hora prescriben parámetros generales para proteger los activos,

> La única opción que tenemos es asumir este reto y enfrentar de manera adecuada los riesgos virtuales que afectan a las organizaciones, llevando nuestra gestión de protección y nuestro perfil profesional hacia la fusión de la seguridad integral

sean estos digitales o físicos. La norma ISO 27001 en particular se enfoca en protección de los activos de información y dentro de las diferentes consideraciones que contempla esta norma están los controles de seguridad física y otros factores que son de utilidad en la gestión de seguridad.

La norma ISO 27001 en particular se enfoca en protección de los activos de información y dentro de las diferentes consideraciones que contempla esta norma están los controles de seguridad física y otros factores que son de utilidad en la gestión de seguridad

APORTES DE LA ISO 27001 A LA GESTIÓN SEGURIDAD	
Línea base	Considera aspectos clave para impulsar la gestión de seguridad como como el liderazgo y el involucramiento de la alta dirección; siendo parte de un sistema de gestión sigue el proceso PDCA del ciclo de Deming.
Evaluación de riesgos	Teniendo como referencia la ISO 31000, enmarcados en un SGSI, permite gestionar riesgos relacionados con los activos de información (digitales o físicos) y brinda el marco para revisar el resto de riesgos físicos que pueden afectar la organización.
Mejora continua	Un SGSI bajo el ciclo PDCA siempre tiene una mejora continua, los 114 controles aplicados en la norma, son sujetos a evaluación para irlos mejorando y actualizando.
Seguridad física de área	Si el acceso a una instalación está bien protegido también lo estará el acceso a los sistemas de información, revisa por lo tanto temas como la seguridad perimetral, controles de acceso, seguridad de oficinas, bodegas, aplicación de áreas seguras de trabajo, etc.
Seguridad física de los equipos (que contienen información)	Considera aspectos relacionados con la protección contra riesgos naturales, criterios de continuidad en cuanto a energía, protección de cableado, etc.
Cultura de seguridad	Siendo parte de un SGSI, esta norma impulsa en los colaboradores la capacitación y la concienciación, que son elementos vitales para la implementación del SGSI y el involucramiento de cada empleado de la empresa cuando el sistema sea aplicado y aportan de manera objetiva en el incremento de la cultura de seguridad.

OBJETIVOS Y DESAFÍOS

Varios años atrás, el responsable de seguridad corporativa en una empresa era subvalorado porque en algunos casos no hacía "clic" con el resto de profesionales, no tenía un lenguaje corporativo, quizás por haber estado familiarizados más con la vida policial o militar, ahora que esos paradigmas se han superado y tenemos profesionales competitivos en la industria de la seguridad, vienen otros retos como son los riesgos virtuales y el tsunami de tecnología que hace que nuestra gestión de riesgos físicos sea opacada.

La única opción que tenemos es asumir este reto y buscar nuestra propia convergencia, comprendiendo de manera adecuada los riesgos virtuales que afectan a las organizaciones, llevando nuestra gestión de protección y nuestro perfil profesional hacia la fusión de la seguridad integral, sin dejar brechas, sin generar espacios que nos hagan quedar del otro lado de la cerca, fuera del protagonismo en la toma de decisiones corporativas, como pasó décadas atrás.

Tal como la norma ISO 27001 aporta a la cultura de seguridad y al análisis de riesgos para gestionar los procesos en una empresa, hay otras normas ISO que apoyan a la gestión de seguridad corporativa, entre otras son: la ISO 31000 Gestión del Riesgo, ISO 37001 Gestión Antisoborno, ISO 9001 Gestión de Calidad, ISO 28001 Seguridad en la Cadena de Suministro, ISO 22000 Seguridad Alimentaria, ISO 45001 Gestión de la Seguridad y Salud.

Existen sin duda otras más que pueden aportar a nuestra gestión, su aplicación dependerá del giro del negocio de la empresa en la cual estamos gestionando la seguridad. Tampoco podemos dejar de lado los estándares de ASIS Internacional como el de Resiliencia Organizacional, Continuidad del Negocio, ESRM y otras guías más que aplican en cualquier organización, son sin duda alguna un aporte impresionante en esta gestión.

Con la aplicación, dominio y apropiación de la norma ISO 27001 cumpliremos los dos objetivos como gestores de la seguridad: 1) Ingresar al umbral de la transformación digital a través de la seguridad de la información y 2) fortalecer la administración de los riesgos físicos relacionados de manera directa e indirecta con esta norma. Es a toda luz oportuno e importante estudiar esta norma con mayor detalle, comprenderla, aplicarla y explotarla en beneficio de la protección de los activos de la empresa sean estos digitales o físicos, el retorno será de valor para cualquier organización y en especial para el responsable de seguridad que la domina y la gestiona. ■

José Echeverría, CPP, MSc.,
consultor de Seguridad en S2C.

Más sobre el autor:

Este tipo de comunicación nos permite dialogar con calma y respeto, expresando lo que queremos decir, pero sin herir los sentimientos de las otras personas

PERÚ | Herbert Calderón

LA HERRAMIENTA PARA LOGRAR EL CLIMA DE FAMILIA EN LA ORGANIZACIÓN: LA COMUNICACIÓN ASERTIVA

Foto: Creativeart - Freepik

Anteriormente habíamos comentado que las empresas han venido perdiendo la sensibilidad con los colaboradores, debido a que la primera opción de las gerencias es la rentabilidad, los proyectos, los clientes, lo cual evita que se destinen tiempo y recursos para lo que verdaderamente vale la pena, que es el factor humano.

Las personas debidamente motivadas logran mejores respuestas, en un ambiente en el que se sientan como en su casa, buena comunicación, retroalimentación constructiva, por ello a mayor soporte positivo en las mentes de los colaboradores tendremos una mejor respuesta con sinergia y lograremos excelentes resultados y por ende productividad en un 65% a 100%.
Por ello el lograr tener a los empleados felices en un ambiente familiar permitirá hacer frente a las contingencias con creatividad y plena respuesta.

Un requisito importante para lograr esta sinergia es el conocer las necesidades, problemas, preocupaciones, frustraciones, clima laboral en general, para ello debemos utilizar diferentes recursos que nos provean de información adecuada y suficiente, logrando un plan de trabajo, para luego buscar la solución conjunta con todos los colaboradores en forma integral.

El principal recurso es la comunicación con ellos, sin embargo, la palabra comunicación es muy amplia en su contexto. La comunicación debe ser adecuada, abierta, sencilla, amigable, familiar, y esta definición se conoce como comunicación asertiva.

La comunicación asertiva está basada en su honestidad, respetabilidad, sinergia, ser transparente, ser abierto permite ser escuchado, y tener las respuestas del entorno, en forma honesta, así como sustentar nuestra posición, pero con la retroalimentación del equipo. Esto permitirá lograr dos situaciones:

1. Enterarnos de toda la problemática.

2. Obtener el involucramiento de todos para aplicar nuestro plan de trabajo conjunto.

Por lo tanto, para poder comunicarnos de forma asertiva es tan importante lo que queremos decir como el cómo lo decimos y cuándo lo decimos.

BENEFICIOS DE LA COMUNICACIÓN ASERTIVA

a. Acercamiento de los empleados apropiadamente con un lenguaje y actitud inspiradora.
b. Trabajo en equipo, involucrar a los trabajadores en la confección de los planes.
c. Participación de todos en la solución de problemas.
d. Aumento en la producción.
e. Ambiente de familia o pertenencia de los colaboradores.
f. Mejor relación entre empleados y en general miembros de la organización.
g. Generación de empatía, fidelización con la empresa.

PASOS RECOMENDADOS

a. Fijar estrategias de trabajo con las gerencias.
b. Tomar encuestas, consultas, cuestionarios, entrevistas.
c. Revisar los resultados de la problemática existente.
d. Formar equipos de trabajo con representantes de cada área con fin de coordinar y capacitar en el estilo de comunicación a emplear.
e. Fijar políticas de incentivos, reconocimientos, remuneraciones, incentivos.
f. Iniciar programas de reuniones por departamentos, áreas, con directores.
g. Volver a medir resultados. ■

Herbert Calderón, CPP, PCI, PSP, CSMP, CFE,
gerente corporativo de Seguridad Integral de Grupo Gloria.

Más sobre el autor:

EL PODER DEL LIDERAZGO DESCENTRALIZADO
PARA RETENER A LOS EMPLEADOS

Permite a los individuos ampliar sus habilidades y desarrollar una mayor comprensión de diversos elementos del negocio

VENEZUELA | Abraham Desantiago

Recuerdo perfectamente que hace poco más de un año hice mi primer aporte a esta prestigiosa publicación internacional y hablaba sobre el liderazgo asertivo y la ley del castigo. Luego de participar en diferentes dinámicas y actividades de ASIS Internacional como la actualización de la PRE-EMPLOYMENT BACKGROUND SCREENING GUIDELINE (ASIS PBSV – 2022) ha nacido en mí la curiosidad de buscar más conocimientos y datos sobre el liderazgo en las distintas organizaciones.

Recientes investigaciones y estudios han demostrado desde hace tiempo que los directivos desempeñan un papel fundamental en la configuración de las carreras profesionales de sus subalternos directos, bien sea para bien o mal. Mientras que los malos directivos pueden ser la razón por la que los empleados deciden dejar su trabajo, los buenos directivos pueden ser la razón por la que los empleados deciden quedarse.

A través de los años, los directivos son responsables de proporcionar a los empleados dirección, orientación y recursos, lo que influye en gran medida en su rendimiento, motivación, recompensas y trayectorias de crecimiento. Pero, ¿qué pasa cuando los directivos cambian de equipo o abandonan su puesto por completo?

Según estudios recientes han revelado que la pérdida de una relación establecida entre un directivo y sus subalternos directos puede tener efectos significativos en las experiencias de los empleados que quedan. Se ha demostrado que la movilidad de los directivos reduce el rendimiento y las recompensas de los empleados que se quedan. Y tiene sentido: lleva tiempo construir esas relaciones, y los nuevos directivos no han estado allí para presenciar el crecimiento de los empleados. Entonces, ¿cómo se puede retener a los empleados cuando sus líderes se retiran?

En ciertas organizaciones norteamericanas, funcionan con lo que llaman estructura gremial. Esto significa que cada miembro del equipo forma parte de al menos dos equipos diferentes. El gremio es el grupo profesional al que uno pertenece —como seguridad, mantenimiento e ingeniería—, mientras que el equipo es donde ese profesional se sienta y contribuye dando aportes de diferentes clases. ¿Cómo influye esto en los efectos de la movilidad de los directivos?

Foto: Creativeart - Freepik

Una de las grandes ventajas de la estructura gremial es que permite a cada empleado trabajar con múltiples partes interesadas. Cuando tienes varios puntos de contacto que comprenden tu ética laboral, te han visto crecer como colaborador y pueden reconocer el valor que aportas al trabajo, por defecto tienes más seguidores.

Además, una estructura gremial permite a los individuos ampliar sus habilidades y desarrollar una mayor comprensión de diversos elementos del negocio. Cada empleado tiene un gerente que le ayuda a crecer profesionalmente, así como líderes de apoyo que le ayudan a obtener una visión más centrada en el equipo.

CONCLUSIONES

Dado que la movilidad de los directivos es inevitable, es importante proporcionar a los empleados dirección y orientación de varios aspectos de la organización. Las estructuras de los gremios, los programas de tutoría e incluso las reuniones poco frecuentes con los directivos pueden ser formas útiles de dar a los empleados acceso a otras partes interesadas y garantizar que tengan un sistema de apoyo.

Abraham Desantiago, supervisor de Central de Alarmas (CAMS Supervisor) de la Embajada Americana en Caracas, Venezuela.

Más sobre el autor:

DECÁLOGO PARA TENER ÉXITO COMO EL NUEVO GERENTE DE SEGURIDAD

Los 10 aspectos para ser el mejor responsable en el área de Seguridad

Foto: CreativeArt - Freepik

MÉXICO

Héctor Coronado Navarro

La gestión de seguridad está ligada al funcionamiento eficiente de las empresas y departamentos de Seguridad, así como al logro de la misión para el cual fueron contratados, por lo que es importante tomar en cuenta los siguientes puntos:

1.
La seguridad es importante, pero primero enfócate en la empresa y sus objetivos, lo demás viene después.

2.
Cuando entres a un nuevo trabajo, aprende el negocio lo más que puedas y habla su lenguaje cuando hables de seguridad.

3.
Busca ganar batallas a corto plazo, las organizaciones no tienen mucha paciencia.

4.
Toma tu tiempo para contratar, pero no te tardes en despedir.

5.
Sé asertivo. El tiempo es el recurso más valioso de tus clientes internos.

6.
Alinea tus objetivos con los de la empresa y mídelos.

7.
Sé flexible, ten plan "B" y maneja bien tus propias crisis laborales.

8.
Sé exigente más que tu jefe y que tus clientes internos.

9.
Si piensas que algo puede salir mal, así será, ahora que lo sabes, prepárate lo mejor para que no sea así.

10.
Para hacer una carrera a largo plazo: da resultados, genera confianza y sé responsable de tus actos. ■

Héctor Coronado Navarro,
VP Global de Seguridad en Kavak.

Más sobre el autor:

RENTA DE BLINDADOS

COLEMAN

Tel.: 557672.4992

krauda@seguridadenamerica.com.mx

www.rentadeblindados.com.mx

02 DE OCTUBRE DE 1968:
UNA REVOLUCIÓN FALLIDA

54 años han pasado desde los asesinatos en la plaza de las Tres Culturas (Tlatelolco, Ciudad de México), el 08 de julio falleció uno de los principales responsables de la masacre, Luis Echeverría

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

La muerte del ex presidente (1970-1976) Luis Echeverría Álvarez (08 de julio de 2022), y quien fuera Secretario de Gobernación durante el mandato de Gustavo Díaz Ordaz (1964-1970) reavivó los sentimientos de injusticia en la comunidad estudiantil y de quienes vivieron de algún extremo lo sucedido en esos años de represión absoluta.

En noviembre de 2001 se creó la Fiscalía Especial para Movimientos Sociales y Políticos del Pasado (FEMOSPP) encabezada por el Dr. Ignacio Carrillo Prieto y quien bajo sus facultades de Fiscal Especial, pidió el procesamiento de Echeverría, acusado de genocidio y desaparición forzada de personas y otros delitos durante la llamada "Guerra Sucia en México" (autor intelectual).

Foto:El País

Foto: Wikipecia

José Guadalupe Gómez Romero,
profesor de la Universidad Nacional Autónoma de México

Foto:Dgcs.unam

"El gobierno tomó la decisión de abrir fuego ante la organización estudiantil más grande de los tiempos"

Foto:Vanguardia

Luis Echeverría sólo estuvo tres años en arresto domiciliario, pues en marzo de 2009, el Quinto Tribunal Colegiado amparó a Echeverría Álvarez contra "el ejercicio de la acción penal dictada en su contra por su probable responsabilidad" en el delito de genocidio de los estudiantes en 1968, pues en toda la investigación "no existió prueba alguna de su culpabilidad".

Aún en la actualidad se desconoce el número real de los desaparecidos y asesinados en lo que se pretendía sólo una marcha en protesta de la represión y abuso de autoridad a los estudiantes en aquella época. Además de los delitos impunes, de 1968 aún quedan las narraciones vivas de quien estuvo ahí y logró sobrevivir.

"NO QUEREMOS OLIMPIADA, QUEREMOS REVOLUCIÓN"

Conforme pasó el tiempo, los expedientes, las investigaciones, el trabajo periodístico y las narraciones fueron abriendo puertas que habían permanecido bloqueadas por el autoritarismo de aquellos gobernantes de los años 70.

No cabe duda que la labor de los militares en México siempre ha estado llena de disciplina, en esas décadas la policía era abusiva y extremadamente severa, sobre todo con los estudiantes, ya que lograban una organización social que asustaba a los gobernantes del país, esto de acuerdo a las narraciones de uno de los sobrevivientes del 68, que aún enchina la piel, cuando se trata de recordar el pasado.

"Se dice que la matanza del 68 empezó por una riña entre estudiantes en la Ciudadela, pero es algo más profundo, fueron años de represión y autoritarismo lo que detonó la unión de las principales universidades, de sus alumnos y catedráticos, estábamos hartos de las golpizas y desapariciones", comentó José Guadalupe Gómez Romero, de los Romero de Santa Cruz Acayucan (Azcapotzalco, Ciudad de México), profesor de la Universidad Nacional Autónoma de México (UNAM).

Gómez Romero era estudiante de la Facultad de Filosofía y Letras cuando ocurrió la matanza de las Tres Culturas, y comenta que la prepa 3, era famosa por sus murales y fue uno de los lugares en donde la policía intentó entrar a la fuerza y agredió a varios estudiantes en julio del 68, alumnos de la Vocacional (IPN) tres acudieron a ayudar a los universitarios, lo que detonó una serie de agresiones entre autoridades y alumnos, las primeras bombas "molotov" se hicieron presentes.

Entre los diferentes sucesos violentos que ocurrían en las escuelas, uno de ellos fue cuando el Ejército derribó el portón colonial de la preparatoria 1 con un bazucazo en la madrugada del 30 de julio, a partir de ese momento, el rector de la UNAM, Javier Barros Sierra, supo que debía defender la autonomía de la Universidad, y entonces comienza la organización de las marchas estudiantiles.

El 02 de agosto de 1968, Barros Sierra encabezó una de las marchas más emblemáticas de la historia universitaria, al frente de más de 100 mil almas, entre universitarios, politécnicos, normalistas, profesores y alumnos de la Universidad de Chapingo, las calles desde Ciudad Universitaria hasta Félix Cuevas fueron invadidas por la lucha contra la represión. La ruta fue modificada (CU-Zócalo), porque se corrió el rumor de que el Ejército Mexicano ya los estaba esperando por las cercanías del Parque Hundido (CDMX).

Foto: Cadena Noticias

"Se dice que la matanza del 68 empezó por una riña entre estudiantes, pero es algo más profundo, fueron años de represión y autoritarismo lo que detonó la unión de las principales universidades"

"Mientras todo esto sucedía, en las facultades ya estaban organizando comisiones para marchas posteriores, para el cuidado de las instalaciones y de todos nosotros. Ahí surge el Consejo Nacional de Huelga (CNH), sin embargo le faltó profundidad al movimiento, había gente muy capaz, pero también aquellos que salían con peticiones fuera de lugar, sin ser concretos", comentó el profesor de Psicología.

"No queremos Olimpiada, queremos una revolución", se escuchaba en voz de Mercedes Garzón, estudiante de la Facultad de Filosofía, y es que el 18 de octubre de 1963, la 60° Sesión del Comité Olímpico Nacional dio a conocer de forma oficial la próxima ciudad para los juegos Olímpicos 1968, es decir a la Ciudad de México (Distrito Federal), con una promesa de ser los próximos mejores juegos olímpicos, incluyendo infraestructura y hospitalidad, o sea que las revueltas en la comunidad estudiantil no formaban parte de este plan.

El presidente en ese momento, Adolfo López Mateos, calificó este logro como "una forma de reconocimiento al esfuerzo del Pueblo Mexicano", Gustavo Díaz Ordaz era el secretario de Gobernación.

SE AVECINA LA TORMENTA

El 13 de septiembre de 1968, los grupos estudiantiles de la UNAM, Instituto Politécnico Nacional (IPN), Universidad Iberoamericana (UIA), miembros del Consejo Nacional de Huelga (CNH) acordaron marchar de forma silenciosa partiendo del Museo de Antropología (CDMX), hasta el Zócalo. El objetivo,

Foto: Los Noticieristas

demostrarle al gobierno que no permitirían más abusos y autoritarismo, pero con la encomienda de ser un grupo, una organización si afán de violentar ni entorpecer los próximos juegos olímpicos.

"La marcha silenciosa fue muy impresionante, miles y miles de personas caminando en silencio por la ciudad. Algunos compañeros traían masquín en la boca, el único sonido que se apreciaba era el de las botas azotando el suelo al ritmo de 'Che, Che, Che Guevara'. Las voces sólo fueron emitidas al llegar al Zócalo, los gritos de protesta fueron contra Díaz Ordaz, sin embargo no se logró el objetivo. El 18 de septiembre el ejército entró en Ciudad Universitaria, violando la autonomía universitaria".

El 23 de septiembre renunció Barros Sierra; y los enfrentamientos continuaron, granaderos y estudiantes se enfrentaron en instalaciones del IPN (Casco de Santo Tomás).

02 DE OCTUBRE NO SE OLVIDA

A 10 días de que iniciaran los décimos novenos Juegos Olímpicos en la Ciudad de México, la Plaza de las Tres Culturas se vistió de rojo. Por tarde del 02 de octubre cientos de estudiantes se dieron cita en Tlatelolco para realizar un mitin, organizarse y demostrar que no permitirían más abusos por parte del gobierno de Díaz Ordaz. Pero a las 17:55 h, dos bengalas fueron lanzadas al cielo para avisar a los militares del Batallón Olimpia, que abrirían fuego indiscriminadamente, a quema ropa a los estudiantes.

"Fernando Gutiérrez Barrios, entonces jefe de la Dirección Federal de Seguridad, reportó como información oficial la detención de mil 43 personas, 26 muertos y 100 heridos. La Agencia de Seguridad Nacional de la Embajada de los Estados Unidos en México informó que el número de muertos oscilaba entre 150 y 350 personas"[1].

"No se tiene el número exacto de fallecidos, esa noche", comenta Gómez, "pero hubo más de 700 detenidos y llevados a Lecumberri, pero como los iban siguiendo vehículos de otros compañeros, los encerraron ahí por unas horas y después los trasladaron a Santa Martha Acatitla, en donde permanecieron tres días, fueron fichados liberados, otros no tuvieron esa suerte". El profesor José Guadalupe Gómez Romero, quien aún continúa impartiendo clases en el Colegio de Ciencias y Humanidades, declaró que "el gobierno tomó la decisión de abrir fuego ante la organización estudiantil más grande de los tiempos". ■

REFERENCIAS

[1] *¿Qué ocurrió el 2 de octubre y el movimiento estudiantil de 1968? El Universal 02/10/2021 https://www.eluniversalpuebla.com.mx/que-hacer/que-ocurrio-el-2-de-octubre-y-el-movimiento-estudiantil-de-1968*

- *Fuentes consultadas: https://www.bbc.com/mundo/noticias-america-latina-45714908*
- *https://expansion.mx/actualidad/2009/03/26/echeverria-exonerado-de-genocidio*
- *https://www.animalpolitico.com/2018/08/1968-el-rector-barros-sierra-encabeza-marcha-en-repudio-al-ataque-del-gobierno-a-la-unam/*
- *https://www.comoves.unam.mx/numeros/articulo/239/mexico-68-un-legado-que-perdura*

amesis

Asociación Mexicana de Empresas de Seguridad Privada e Industria Satelital A.C.

FORTALECIENDO LA INDUSTRIA DE SEGURIDAD Y TECNOLOGÍA SATELITAL EN MÉXICO

BENEFICIOS ESPECIALES

24/365 DÍAS
Atención personalizada de nuestro centro de monitoreo

SIAMES C5
Uso exclusivo de la plataforma, para comunicación con las autoridades

ACCESO
Total acceso a reportes de estadísticas de robos

COMITÉS

- Comité Relación con Autoridades
- Comité Estadísticas del Sector
- Comité Capacitación y Desarrollo
- Comité de Relaciones Públicas
- Comité Tecnologías de Información

NUESTROS SOCIOS

sitel Seguridad Satelital · Tracking Systems · skymeduza · Holkan · ADS LOGIC TELEMATICS · ATLANTIDA · DUMAY · GEOTRACKING · GLOBAL MIT · GRUPO ALCA · INFO TRAX · RAINDE · skyguardian · SECURE WITNESS · SEGURIDAD 360 .COM · TECNO LOGISTIK · MAGNI Tracking · TTC · AISIS · GPS

SOCIOS ADHERENTES

gps

INFORMACIÓN

COMUNÍCATE
55 3334 4707
c.administrativa@amesis.org.mx
amesis.org.mx

amesis
Asociate

MEDIDAS DE SEGURIDAD CON LAS PERSONAS QUE LO RODEAN

COLOMBIA | Javier Nery Rojas Benjumea

Como ya es costumbre, nuestro colaborador invitado comparte algunos consejos de seguridad

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

En cualquier país y lugar las personas son vulnerables y pueden ser víctimas de secuestros, robos o violencia en general, afectando la integridad personal y familiar. Estamos de acuerdo que la familia es lo más importante, por ello expongo las siguientes medidas de seguridad para que las comparta con sus seres queridos:

CON LA ESPOSA

La esposa juega un papel superlativo en cuanto a la protección de su esposo; debe tener en cuenta que el domicilio es uno de los puntos más vulnerables para cometer un ilícito siendo necesario cumplir las recomendaciones que en esta guía se detallan.

Punto esencial en sus conversaciones será guardar y hacer guardar la mayor discreción, incluso con sus mejores y más íntimas amigas, sobre el cargo de su esposo, responsabilidades, actividades y viajes.

Esté informando a su cónyuge o persona de mayor confianza acerca de su itinerario diario; comuníquese frecuentemente con su residencia para que mantenga un control de su desplazamiento.

Se recomienda tener un archivo de grabación de las voces de su grupo familiar y empleados de confianza, con el fin de aportarlo a las autoridades en el evento de un secuestro o una extorsión.

CON LOS HIJOS

Tome precauciones con los hijos, especialmente en sus rutinas como la asistencia al colegio y a los sitios de recreación. Verifique las invitaciones que les hagan.

Debe informar a sus hijos del riesgo que comparten en razón de la situación de sus padres y explicarles que este motivo los obliga a no comentar con nadie la situación y permanecer alerta.

Conozca muy bien a los amigos de sus hijos y sus familias, e interésese en especial por la actividad laboral que desempeñan. Instruya a sus hijos para que:

- Eviten citas a ciegas o reuniones con personas que ellos no conocen.
- Indaguen sobre el desempeño laboral de los padres de sus nuevos amigos o compañeros.
- Informen constantemente en dónde y con quién se reúnen cuando están fuera de la casa. Explíqueles que es por su tranquilidad y seguridad, ellos comprenderán las razones.
- No se suban a carros de personas extrañas a la salida de fiestas o de cines, especialmente en horas de la noche.

- No hablen con extraños.
- No se acerquen a vehículos de desconocidos que les llamen la atención.
- No den información sobre lo que pasa en su casa, sobre sus negocios y su desempeño laboral.
- No le suministren a nadie él número telefónico o la dirección de la casa o la oficina de sus padres. Sólo deben hacerlo en caso de que se encuentren extraviados.
- No reciban dulces, dinero, ni regalos a personas de la calle o en centros comerciales.
- No entren a ningún edificio, casa o cuarto de personas que no sean de su confianza.
- No jueguen en sitios aislados u oscuros, ni en callejones o cerca a edificios o casas desocupadas.
- No dejen entreabierta la puerta principal de la casa.
- No abran la puerta a desconocidos.
- No reciban órdenes por teléfono.
- Manifestar a sus hijos que en caso de que sean secuestrados no aporten a los delincuentes datos sobre los bienes de la familia.

En cualquier actividad que desarrollen sus niños como esperar el bus del colegio y jugar en parques o espacios abiertos, siempre deben permanecer bajo el cuidado de un adulto.

CON FAMILIARES Y AMIGOS

A los familiares más allegados y amigos más íntimos debe hacerles partícipes del estado de inseguridad o amenaza en que se vive incluso a los que residen en otras ciudades con el ruego formal de que, bajo ningún motivo, faciliten la dirección o teléfono.
En lo que respecta a visitas a familiares y amigos, se deben observar, también, las precauciones ya descritas.

EN EL COLEGIO Y UNIVERSIDAD

Cuando seleccione el colegio para sus hijos, verifique usted mismo la seguridad de las instalaciones, los mecanismos de control interno y las rutas exactas de los buses e imparta instrucciones claras sobre sus niños, a los directores e instructores.

> Conozca muy bien a los amigos de sus hijos y sus familias, e interésese en especial por la actividad laboral que desempeñan

Instruya a sus hijos para que tengan en cuenta los siguientes aspectos:

- Desplazarse por grupos o en parejas.
- Jugar en áreas dentro de los predios del colegio.
- Al desplazarse, deben cerciorarse de hacerlo en el vehículo o bus asignado por el plantel educativo y, mientras lo esperan, así como durante el recorrido, deben adoptar todas las medidas de seguridad.
- Evitar salir del colegio en la noche; de ser así, comunicarse con sus padres para que éstos los recojan o para evitar preocupaciones innecesarias.
- Al colegio debe informarle los números telefónicos en donde lo puedan contactar y, acuerde con las autoridades del establecimiento, que le notifiquen antes de dejar a su hijo bajo la custodia de alguien a quien usted no ha autorizado previamente. ■

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

Javier Nery Rojas Benjumea, MBA, CPP, *Board Certified in Security Management.*

Más sobre el autor:

SIMILITUD ENTRE LOS MIEMBROS DE LAS SECTAS Y LAS FAMILIAS QUE EJERCEN VIOLENCIA

Nuestro colaborador invitado muestra las semejanzas entre los miembros de ambos grupos y la manipulación y control que ejercen en la víctima

Foto: Creativeart - Freepik

ARGENTINA | Juan Manuel Iglesias

¿Qué es una secta? El diccionario DRAE (Diccionario de la Real Academia Española) la define como una "comunidad cerrada, que promueve o aparenta promover fines de carácter espiritual, en la que los maestros ejercen un poder absoluto sobre los adeptos".

Al analizar las características y efectos que las sectas producen en sus miembros, veo similitudes con la situación con que se enfrentan los miembros de una familia que sufre violencia.

Para comenzar podemos decir, siguiendo a Amelia Musacchio de Zan (2000) que las sectas ofrecen promesas como las de encontrar una comunidad para superar situaciones de soledad, respuestas ante las sensación de vacío existencial, revivir una experiencia de apego segura, encontrar un ambiente de seguridad y protección ante la configuración de un ambiente externo y amenazante.

ASPECTOS COMPARATIVOS

Como sostiene esta especialista en psiquiatría, las sectas atraen a personas que están sufriendo problemas personales, transiciones, crisis; brindan la promesa de una curación transformadora dentro del marco de una comunidad que le tiene cariño y que la cuida.

Foto: Creativeart - Freepik

Es decir que las personas con una historia de maltrato y abuso son las más vulnerables a ser seducidas por las sectas, precisamente debido a la necesidad de seguridad, apego, amor, contención y control. Lo mismo sucede con las relaciones familiares en contextos de violencia donde la víctima busca en el agresor la protección, seguridad y amor. Ahora bien las sectas reproducen en mismo espacio simbólico que las familias autoritarias y violentas, ya que en ambas se observa lo siguiente:

1.

Las sectas operan desde la **"seducción/frustración"**, es decir que primeramente les hacen saber a los miembros que son valiosos, amados y "algo especial" y luego aparece la descalificación, le retiran esa admiración produciendo confusión, angustia y la "dependencia coaccionada" como consecuencia de haber estado sometidas a un proceso de reforma del pensamiento.

En la violencia familiar, siguiendo a Ferreira (1992), el agresor somete a la víctima a situaciones similares que se puede ver en el "síndrome del esclavo" que "surge cuando en una relación existe un poder excesivamente desbalanceado en que uno de los miembros subyuga al otro acompañado de abusos, recompensas e indulgencias. Se instala un ciclo de dependencia en donde cada vez se magnifica el poder del hombre violento y la mujer disminuye el de ella. Se va generando una necesidad cada vez mayor respecto del miembro poderoso. Se establece un vínculo afectivo simbiótico en donde la mujer se va anulando y construyendo una nueva identidad".

2.

Según Musacchio de Zan (2000) la secta aplica sobre la víctima un programa de manipulación sistemática usando técnicas psicológicas y sociales. Entre ellas en **"lavado de cerebro"**.

En situaciones de violencia familiar, el agresor también somete a la víctima a una situación similar cuando como dice Ferreira (1988) se persigue el objetivo que la persona renuncie a su libertad para transformarse en una autómata sometida a los designios de su captor, obteniéndose dos resultados: [1]. El organismo se condiciona a las exigencias de la situación, [2]. La mente adopta el sistema de ideas que quiere inculcarle el victimario.

Esta situación, al igual que en las sectas producen un desmoronamiento producto de no saber cómo luchar y en quién confiar cuando el miedo y el abandono invaden la personalidad. Las funciones de la víctima quedan reducidas a lo elemental y puede llegar a parecer retrasada o enferma mental: no se expresa ni puede hablar de lo que le sucede.

3.

Control del medio, control de la comunicación con el ambiente: es mantener crecientemente aislado a los miembros de los no miembros. Es lo que algunos llaman "clausura personal". Las víctimas están recibiendo constantemente indicaciones y órdenes de suprimir las dudas y de no fomentar pensamientos conflictivos sobre qué es verdadero, qué es falso y qué es real.

En las familias abusivas, el agresor suele aislar a la víctima impidiendo que trabaje fuera de casa, que haga algún deporte, que estudie, que se encuentre con amigas, hasta el extremo de separarla completamente de su círculo familiar.

4.

La manipulación mística. Este "mecanismo de dominación" implica presentar al líder como una figura "todopoderosa" que determina el bien y el mal. Él es el intérprete y mediador de las verdades ocultas

En las familias muchas veces el "pater patriarcal" ejerce un poder similar al de los "reyes absolutos" como si fueran los dueños de la pareja y los hijos, una pervivencia de la familia patriarcal de la antigüedad. También determinan que es justo o injusto llegando a imponer el terrorismo como forma de coacción en la familia.

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

5.

La secta usa **"principios dogmáticos" y una visión totalitaria de la verdad.** Como dice Musacchio de Zan "cualquiera que desobedece o se desvía del dogma [...] es automáticamente falso, malo, maligno y rechazable. Los líderes son jueces y pueden cambiar sus criterios para juzgar a alguien".

Una de las características de los hombres que ejercen violencia son las distorsiones cognitivas que se expresan en un pensamiento en "blanco y negro" con base en generalizaciones que no tolera la disenso. La inseguridad y necesidad de control del victimario producto de experiencias de apego inseguros impide el diálogo y lo hace desconfiar de su pareja.

> La secta aplica sobre la víctima un programa de manipulación sistemática usando técnicas psicológicas y sociales. Entre ellas en "lavado de cerebro"

6.

Identificación con el agresor. Al igual que en las sectas en las familias las víctimas desarrollan el "síndrome de Estocolmo", Siguiendo a Ferreira (1992), "la mujer construye una realidad y una narrativa deformada de los hechos objetivos ya que pierde contacto con la realidad. Es una forma de apaciguar al atacante y darle menos oportunidades que se vuelvan en su contra. ■

REFERENCIAS

- *Musacchio de Zan (2000) "Otra adicción: las sectas y su logro de inducir a dependencia y servidumbre" en Alcmeon, año XI, Vol 9, n 2.*
- *Ferreira, Graciela (1992) Hombres Violentos-Mujeres Maltratadas. Aportes a la investigación y tratamiento de un problema social, Buenos Aires, Editorial Sudamericana.*

Juan Manuel Iglesias,
magíster en Criminología, Victimología y Feminicidio; y gerente de Seguridad Corporativa.

Más sobre el autor:

UNA PERLA DE SERVICIO:

30 AÑOS DEL NÚMERO UNIVERSAL DE EMERGENCIA EN MÉXICO

El Número Universal de Emergencia (NUE) tiene el propósito de facilitar y agilizar la atención de emergencias, a fin de proteger y salvaguardad la vida e integridad de las personas y sus propiedades, objetivo fundamental de la seguridad

Foto: Creativeart - Freepik

MÉXICO | David Chong Chong

En memoria de Jerry D. Price

En una situación de emergencia, el factor crítico para evitar los posibles daños a la vida y la integridad de las personas y sus propiedades, en especial los irreversibles o irreparables, es la rapidez con la que acudan los recursos pertinentes para atenderlas. Para ello, el problema es que se requiere notificar a alguna de las diversas agencias o corporaciones especializadas para atender emergencias, por lo regular por parte de una persona presente en el lugar de los hechos, que muy probablemente estará alterada emocionalmente además de no conocer la forma de comunicarse con dichas agencias, en especial si es alguien ajeno al lugar en que ha ocurrido el evento, por ejemplo, por ser visitantes en una comunidad.

Con el Número Universal de Emergencia (NUE) se habilita un medio de contacto único con todas las agencias, de tal suerte que cualquier persona, por más alterada o confundida que se encuentre, podrá notificar a la instancia pertinente acerca del evento ocurrido.

El NUE tiene su origen en los Estados Unidos, a partir de una iniciativa de la Asociación Nacional de Jefes de Bomberos en 1957, que proponía la adopción de un número único para reportar incendios. A partir de esa iniciativa, en 1967 la Comisión Presidencial para la Aplicación de la Ley y la Administración de la Justicia, determinó la necesidad de un número único simplificado para reportar todo tipo de emergencias, lo que inició un proceso de desarrollo coordinado entre la FCC y la empresa AT&T que resultó en la adopción del código 9-1-1 como el número único simplificado, cuya primera llamada se efectuó en febrero de 1969 en Haleyville, Alabama.

Para 1987 el uso de este número simplificado ya se había extendido al 50% de la población, e incluso Canadá se había integrado a este servicio, y a finales del siglo XX, ya cubría 96% de la población en los Estados Unidos, y se había adoptado, con diversas formas de código, en muchos países[1].

LLEGADA A MÉXICO

El NUE llegó a nuestro país en 1992, específicamente al entonces Distrito Federal, a través del Fideicomiso del Servicio de Emergencia 08 dentro de la estructura de Servicios Metropolitanos (SERVIMET). Como número único se adoptó el código de dos dígitos 08 (posteriormente migrado a 080), ya que por limitaciones técnicas de TELMEX no fue posible adopta el código 911, para sustituir los más de 19 números telefónicos, algunos con código simplificado de dos dígitos, pero la gran mayoría de siete dígitos, de las diversas corporaciones de emergencia (policía, bomberos Cruz Roja, ERUM, etc.) en la ciudad.

El Servicio de Emergencia 08 (SE08) se presentó el 19 de septiembre de 1992, e inició sus operaciones el 1°. de enero de 1993 con la Delegación Benito Juárez como piloto. Posteriormente, a mediados de ese mismo año la cobertura se extendió a las Delegaciones Álvaro Obregón, Coyoacán y Miguel Hidalgo, y el 9 de enero de 1994, aún sin contar con todos los recursos, se adelantó la cobertura a toda la ciudad, a raíz del atentado en Plaza Universidad.

La versión de NUE implementada en México, fue con la modalidad E9-1-1, que ofrece mayor certidumbre acerca de su autenticidad, ya que proporciona la identificación y dirección del origen de la llamada, con lo cual se reducía el tiempo para recabar la información de los eventos. Por ello, en el aspecto técnico, el primer problema para la implementación del SE08, fue la adaptación de la plataforma tecnológica (equipo de

cómputo y sistema) diseñado para un entorno urbano totalmente ordenado y estructurado en la numeración de las direcciones, para un entorno con identificación de calles y numeración muy disímbolo como la que existía, y sigue existiendo en la ciudad, al grado de que la referencia de intersecciones de calles, que se adoptó e integró como solución, se ha convertido en la actualidad en una práctica común.

En este esfuerzo se contó con la colaboración del primer grupo de operadores, algunos procedentes de LOCATEL, así como de otras corporaciones, que recorrieron las calles de la Delegación Piloto para identificar la correlación de intersecciones con la numeración de las calles. El segundo problema, aún más crítico, fue habilitar la plataforma con su configuración inicial, insuficiente, para soportar la cobertura del servicio a toda la ciudad. El soporte técnico para ello fue proporcionado por la empresa mexicana Servicio Computarizado de Emergencia (SCE), con el apoyo de la empresa texana Public Safey Associates (PSA).

DIFICULTADES

Por otra parte, en el aspecto operativo, el primer problema fue establecer una base de coordinación interinstitucional entre las diversas corporaciones de servicio para atender los requerimientos emitidos desde el SE08, considerándolo como un canal de comunicación confiable, de manera prioritaria e incuestionable, para lo cual se contó con el apoyo de la facilidad técnica para identificar, y eventualmente sancionar, a los autores de llamadas no procedentes (bromas, amenazas, insultos), al tener identificados y ubicados los números de origen de las llamadas.

Un segundo problema, no menos importante, fue la preparación de los operadores del servicio, para lo cual, si bien se tomó en cuenta las experiencias de algunos centros en los Estados Unidos, se desarrollaron de manera local los procedimientos y protocolos, que permitieron no solo facilitar y agilizar el alertamiento a las corporaciones, con tiempos de transferencia mínimos de hasta 90 segundos, sino incluso contener emergencias médicas impartiendo instrucciones vía telefónica.

Un problema adicional, fue la recopilación de la conformidad de los suscriptores al servicio, en virtud de que se hacía un cobro mensual por el mismo, con el propósito de que no sólo la operación fuera financieramente autosustentable, sino que se contara con recursos para apoyar con equipamiento a las mismas corporaciones.

El SE08 tuvo una gran aceptación y confianza entre la población por los éxitos en la atención de emergencias, así como por un fuerte programa de difusión y concientización públicas y de integración ciudadana, que incluyó visitas de grupos vecinales y escolares a las instalaciones del servicio. La evidencia más clara de este éxito fue la reducción de las llamadas no procedentes iniciales (de primera vez) en un 40%, y de casi el 80% en recurrencia (dos o más desde el mismo número), que son causa de distracción de los recursos escasos para la atención de emergencias, con el consecuente riesgo de vidas.

Asimismo, en el contexto de la operación del SE08 se realizaron las primeras pruebas de un sistema de Rastreo Vehicular por medio de un Sistema de Geoposicionamiento Global (GPS) para el control de las patrullas de la Policía, utilizando únicamente medios de radiocomunicación, en una época anterior a la telefonía móvil de la actualidad.

Aunque su operación se canceló en el año 2002 por motivos más de índole políticos y económicos que técnicos y operativos, con algunas de sus funciones transferidas al número de atención 060, con el SE08 se dieron los primeros pasos, y en cierta forma literalmente, en el recorrido de un camino que nos ha llevado a la actual modernidad del Servicio de Número Único de Emergencias 9-1-1, en operación a nivel Nacional desde 2017, con mayores y mejores facilidades y medios de comunicación, como la telefonía móvil y las redes sociales. Una verdadera y muy valiosa Perla de Servicio, que ha contribuido y seguirá contribuyendo a ese objetivo fundamental que sustenta la misma existencia de cualquier sociedad, proteger la vida. ■

"El camino de mil millas empieza con un paso", Lao Tsé

Este artículo fue realizado con la colaboración de Carlos Cristiani Díaz, Elia Rodrigo Najar, Cinthia Castillo Calles, Ana Luisa Durón Mendoza y Julio César Rodríguez Cortés.

Puede encontrar la versión completa de este artículo en este enlace: https://www.ceasmexico.org.mx/beta/php/difusion/articulo.php?pid=000230

Foto: Creativeart - Freepik

REFERENCIAS

[1] *National Emergency Numnr Association. https://www.nena.org/page/911overviewfacts.*

David Chong Chong,
secretario general para México de la Corporación Euro Americana de Seguridad (CEAS) México.

Más sobre el autor:

A 21 AÑOS DEL 9/11: PARTEAGUAS EN LA SEGURIDAD MUNDIAL

Foto: Creativeart - Freepik

El 11 de septiembre de 2001 fue un evento crítico para la sociedad estadounidense y la seguridad nacional y en general en el mundo, ya que fue la pauta para dar pie a la seguridad del siglo XXI

MÉXICO

Erick Martínez / *Staff* Seguridad en América

En la edición 122 de esta revista se habló de este mismo tema desde una perspectiva generalizada de este trágico evento, aspectos de la cultura estadounidense, víctimas, cambios políticos y afectaciones directas. En esta ocasión, se hablará de como impactó directamente a una revolución de la seguridad aeroportuaria y aperturando también un nuevo mercado.

Foto: People en Espanol

¿QUÉ PASO EL 11 DE SEPTIEMBRE DE 2001?

Cuatro aviones fueron secuestrados presuntamente por miembros de Al Qaeda para atentar contra edificios emblemáticos del poderío de Estados Unidos. Con 2,996 muertes, el 11-S es el mayor ataque terrorista en suelo estadounidense de la historia y sus consecuencias aún se sienten.

- El primero fue el vuelo 11 de American Airlines que golpeó la torre norte del World Trade Center en Nueva York.
- El segundo fue el vuelo 175 de United Airlines que también salió de Boston y estrelló la torre sur.
- El tercer avión secuestrado fue el 77 de American Airlines que salió del aeropuerto internacional de Dulles en Washington y estrelló el lado sudoeste del Pentágono, sede del Departamento de Defensa de Estados Unidos.
- El cuarto, vuelo 93 de United Airlines, salió de Newark, New Jersey, y se estrelló cerca de Shanksville, Pensilvania. Casi tres mil personas murieron, incluidas 265 a bordo de los cuatro aviones.

El hecho de que se haya llevado a cabo el ataque con vuelos diferentes en lugares diferentes dejó en claro lo vulnerable que era Estados Unidos en ese entonces, por ello es que se decidió hacer un cambio importante en todas las regulaciones de seguridad antes de poder abordar un avión.

¿QUÉ CAMBIÓ EN LA SEGURIDAD?

A partir de ese lamentable hecho los vuelos comerciales fueron suspendidos por tres días, a su regreso todo era diferente, había presencia de militares, las filas para abordar eran largas, se adaptó tecnología que ser creía era necesaria para poder retomar los vuelos y todos se sintieran seguros, porque el pánico colectivo y el miedo a volar fue el común denominador en los pasajeros.

En cuanto a la seguridad pública se creó un área en repuesta al 11 de septiembre, el Departamento de Seguridad Nacional se creó fusionando 22 agencias gubernamentales en una, incluido el Servicio de Aduanas, el Servicio de Inmigración y Naturalización, la Guardia Costera de Estados Unidos y la Agencia Federal para el Manejo de Emergencias, la cual se encarga de supervisar la seguridad en más de 400 aeropuertos del país, entre otras funciones.

A través de la Iniciativa de Seguridad de Contenedores, más del 80% de la carga marítima en contenedores importada se preseleccionó antes de ingresar a Estados Unidos. El 12 de marzo de 2002, se introdujo el Sistema de Asesoría de Seguridad Nacional. El 26 de abril de 2011, el Sistema Nacional de Asesoramiento sobre Terrorismo (NTAS) reemplazó el Sistema de Asesoramiento de Seguridad Nacional (HSAS). El 19 de noviembre de 2001 el Congreso aprobó la Ley de Seguridad de Aviación y de Transporte, creando así la Administración de Seguridad de Transporte (TSA).

OTROS CASOS QUE CAMBIARON LA SEGURIDAD

En diciembre de 2001, apenas unos meses después del 11-S, el inglés Richard Reid, conocido como el "Shoe bomber", escondió explosivos en sus zapatos y trató de detonarlos en la cabina del avión de American Airlines que viajaba de París a Miami. El accidente fue evitado por una auxiliar de vuelo y eventualmente llevó a que millones de viajeros en el mundo tuvieran que quitarse los zapatos y pasarlos por el escáner antes de montarse al avión.

En 2006, después de que la Policía británica descubriera un plan para detonar líquidos explosivos y tratar de derrumbar al menos siete aviones que viajaban de Inglaterra a Canadá y Estados Unidos, oficiales de la TSA prohibieron a los pasajeros llevar líquidos, geles y aerosoles en el equipaje de mano. Meses después relajarían la medida a envases menores a 100 mililitros transportados en bolsas plásticas transparentes.

El hecho de que se haya llevado a cabo el ataque con vuelos diferentes en lugares diferentes dejó en claro lo vulnerable que era Estados Unidos

Foto: France 24

A partir de 2017, tras los atentados frustrados desde Australia y Yemen usando objetos electrónicos y cartuchos de impresoras como explosivos, la TSA obligó a todas las personas a pasar por rayos X los objetos electrónicos más grandes que un celular.

Todos los hechos anteriormente descritos y otros, dieron pie a adoptar nuevas tecnologías como cámaras con analíticos inteligentes, como infrarrojo, lectoras de temperatura, lectoras biométricas, además de que la tecnología no podría darse abasto en este sentido, por lo que se tuvo que capacitar al personal de seguridad en temas específicos, para poder actuar de manera más preventiva y no reactiva como se había estado manejando, incluso muchos expertos en seguridad opinan en la actualidad que la mejor manera de contrarrestar ataques intencionados o incidentes fortuitos es la prevención, mediante análisis de riesgo y protocolos de actuación, además de coadyuvar con autoridades para así dar cobertura completa en el aeropuerto.

Hoy en día un aeropuerto en cualquier parte del mundo es de los lugares con más seguridad, cámaras de videovigilancia, presencia policiaca o militar, y cientos de ojos que vigilan todo el tiempo a todas las personas que entran, salen o llegan de otro destino, porque sin lugar a dudas es uno de los hechos que cambio la historia de la seguridad y hoy sigue dando de que hablar. ■

REFERENCIAS

- *https://www.france24.com/es/ee-uu-y-canad%C3%A1/20210909-seguridad-aerea-terrorismo-atentados-11-septiembre*
- *https://www.bbc.com/mundo/resources/idt-b7a00a0b-9386-4fae-84b7-9c3e9f39d8ff*
- *https://cnnespanol.cnn.com/2021/09/10/20-anos-de-los-atentados-terroristas-del-11-de-septiembre-en-estados-unidos/*

AEROPUERTOS SEGUROS

A partir de la reapertura de las fronteras e implementados los nuevos sistemas de seguridad, la necesidad de viajar en las personas se ha reactivado

Foto: Creativeart - Freepik

MÉXICO

Lissa Elizabet Gómez López / *Staff* Seguridad en América

A lo largo de 16 años consecutivos de crecimiento aéreo en América latina, el COVID-19 trajo consigo un retroceso en la industria abismal de aproximadamente un 59.2% debido al cierre de fronteras durante un periodo considerable, por lo que el sector aéreo tuvo que replantear las estrategias de seguridad dentro de los aeropuertos con el fin de optimizar la reapertura y salvaguardar el bienestar de los empleados y por supuesto de los clientes en sí.

Es por lo que empresas como Motorola Solutions, para plantear la nueva apuesta de innovación en materia de seguridad de las empresas, abrieron paso a líderes en innovación como Darío Andrés Mojica Martínez, ingeniero de Ventas LATAM en Avigilon; y John Ávila Hernández, ingeniero de Preventa para México & Nola en Motorola Solutions.

Desde 2019, Avigilon es una empresa de Motorola Solutions con más de 20 años de experiencia en el campo de la seguridad electrónica y en el diseño, implementación y desarrollo de redes de datos para sistemas de videovigilancia sobre IP.

Darío Mojica y John Ávila se dieron a la tarea de explicar los impactos de la pandemia en el sector y a su vez el nuevo sistema de comunicación integrado que actualmente se está implementado en los aeropuertos.

¿LA PANDEMIA SANITARIA POR COVID-19 BENEFICIÓ A LA INDUSTRIA DE SEGURIDAD EN AEROPUERTOS?

Darío Mojica afirmó que pese a las pérdidas en materia económica, la pandemia por COVID-19 resultó un estímulo en materia de tecnología, pues su mirada se centró en otro tipo de implementaciones necesarias de acuerdo con el nuevo orden como: detección de temperatura corporal, el tema del aforo a partir de las cámaras de seguridad, uso de mascarillas, el cumplimiento del distanciamiento social y todo ello se da a partir de video de alta definición.

Darío Mojica,
ingeniero de Ventas LATAM en Avigilon

Por su parte, John Ávila agregó que pese a que la pandemia detuvo el desarrollo habitual en las industrias, empresas como Motorola Solutions, no se detuvieron en su búsqueda de soluciones ante las nuevas problemáticas dadas, llegando así a la fusión de tecnologías existentes y las nuevas tecnologías dadas con el fin de beneficiar a los usuarios de los aeropuertos.

John Ávila,
ingeniero de Preventa para México & Nola en Motorola Solutions

¿QUÉ CAMBIOS SURGIERON A RAÍZ DE LAS NUEVAS NORMAS SANITARIAS IMPLEMENTADAS DENTRO DE LOS AEROPUERTOS?

Uno de los motores en cuestión de nuevas implementaciones, fueron las nuevas normas a partir de los gobiernos y la misma Organización de la Salud, como el usos de mascarillas, el aforo establecido, el registro de temperatura corporal, una distancia adecuada entre individuos con el fin de impedir el avance del virus de la mejor manera y raíz de ello, surgió la necesidad de implementar nuevas tecnologías como es el caso del novedoso sistema de comunicación integrado, esto en palabras de Darío Mojica.

John Ávila añadió y resaltó que el principal interés antes inclusive de la llegada de la pandemia era la integración del sistema de comunicación en aeropuertos, debido a la pandemia el proceso debió agilizarse para registrar las anomalías que se pudieran presentar, de acuerdo con las normas sanitarias de ingreso y permanencia en los aeropuertos.

¿EN QUÉ CONSISTE EL NUEVO SISTEMA DE COMUNICACIÓN INTEGRADO?

John Ávila explicó que el nuevo sistema de comunicación integrado consta de la integración de voz, datos, video, radio, centros de despacho, intercomunicación con las empresas de emergencia y analítica, anteriormente la industria aérea en cuanto al uso de estas tecnologías, las manejaban de manera separada y por su parte Motorola Solutions creó un ecosistema para integrar cada una y atender los eventos que surjan de forma proactiva. Anteriormente, los sistemas de seguridad servían más como una evidencia de los hechos sucedidos y con la nueva tecnología funcionan como una alarma para abordar los elementos antes de que se vuelvan una emergencia y todo esto debido a las cámaras que cuentan con analítica e inteligencia artificial y en cuestiones normativas con respecto a la pandemia, permite la toma de temperatura, el uso correcto de la mascarilla, conteo del aforo y todo desde un mismo dispositivo, a su vez, una más de sus funcionalidades es detectar elementos abandonados y reportar inmediatamente por medio de una alarma a los sistemas o personal de seguridad y de igual manera si se suscita una restricción por medio de personal no autorizado a alguna área, es reportado directamente por radio.

Mojica, por su parte, agregó lo siguiente: "El nuevo sistema de seguridad busca por su parte volver la operación más proactiva que reactiva, al suministrar mejor los recursos y dar soluciones de manera más inmediata y eficiente"

Foto: Avigilon

> Anteriormente, los sistemas de seguridad servían más como una evidencia de los hechos sucedidos y con la nueva tecnología funcionan como una alarma para abordar los elementos antes de que se vuelvan una emergencia y todo esto debido a las cámaras que cuentan con analítica e inteligencia artificial

Foto: Motorola

¿CUÁL ES EL ALCANCE DE CRECIMIENTO ESPERADO EN EL SECTOR?

De acuerdo con los índices de crecimiento presentados hasta 2020 el sector aéreo disminuyó 59.2% debido a las restricciones dadas.

A partir de la reapertura de las fronteras e implementados los nuevos sistemas de seguridad, Ávila afirmó que la necesidad de viajar en las personas se ha reactivado, por su parte el crecimiento en el sector aéreo en nuestro país ha sido uno de los más frutíferos y a razón de ello, se espera el repunte con la reapertura de fronteras. Tomando en cuenta la nueva normalidad del mundo, las personas podrán tener una percepción real de la seguridad y con ello obtendrán una mejora en la experiencia al pisar un aeropuerto, ya sea el personal que labora en él o bien las personas que hacen uso de sus servicios.

Para finalizar, Darío Mojica argumentó que en América Latina la reactivación y crecimiento está mejorando a buen ritmo y es México quien encabeza dicho crecimiento con más del 73% de su tráfico, tras él Brasil con un 69% y después Colombia con un porcentaje estimado de un 53%. Se reafirma el deseo de la población en general de salir de viaje y a su vez un beneficio que trae consigo el nuevo sistema integrado, es que no sólo ayudará en cuanto a la logística y control de seguridad, sino a la misma imagen que tengan aquellos que pisen los aeropuertos, al sentirse seguros en su tiempo de permanencia, pues la primera impresión de un país se da por medio de los puertos aéreos. ■

ANIVERSARIO DE LOS TERREMOTOS EN **MÉXICO** DE **1985 Y 2017**

Foto: Unión CDMX

19 de septiembre es una fecha que queda para la posteridad debido a los sismos en 1985 y 2017, tanto que se piensa y se prevé que cada año se repita justamente en el mismo día, quedando en la memoria colectiva un sentimiento de vacío y de dolor

Foto: Tercera Vía

Foto: El Comercio Perú

MÉXICO | Erick Martínez / *Staff* Seguridad en América

México es una zona altamente sísmica y en especial la capital, ya que fue construida sobre un majestuoso lago, que con el paso del tiempo ha creado situaciones de inseguridad, ya que el suelo es extremadamente blando, según algunos especialistas en el tema. A nivel mundial existe un tipo de temblor llamado "megasismo", con magnitudes de alrededor de 9; el de Chile, en 1960, fue de 9.5, el más grande que se ha registrado hasta ahora. A lo largo de la historia de México siempre han ocurrió muchos sismos y terremotos, conocidos desde la época prehispánica, los antiguos mexicanos creían que, en ocasiones, durante su recorrido por el subsuelo después del ocaso el sol se tropezaba. Lo mismo les ocurría a otros astros, y entonces se generaba un movimiento de tierra.

Estos sismos en el último siglo han dejado daños muy grandes, aunque unos más que otros, por lo que es importante recordar algunos de ellos:

28 de julio de 1957, **7.6-7.8, Guerrero.**

El sismo tuvo una profundidad de 33 km y su epicentro fue registrado cerca de Acapulco. Fueron reportados 68 muertos, daños en varios edificios y casas de la capital del país; la estatua del Ángel de la Independencia colapsó. Por tal suceso es recordado coloquialmente como El sismo del ángel.

28 de agosto de 1973. **Entre Ciudad Serdán, Puebla, San José Independencia, Oaxaca e Ixtaczoquitlán, Veracruz, 7.3 - 8.5.**

Entre mil 200 a tres mil muertos en la zona centro de México, la destrucción completa del Este de Puebla y Centro de Veracruz, el sismo más costoso de México. 2 mil a 4 mil heridos, 310 mil damnificados, la mayoría de ellos mandados a otros lugares por sus familias. El sismo registró una profundidad de 84 km, el sismo más intenso de México hasta ahora.

19 de septiembre de 1985. **8.1 y 8.0, cerca de la desembocadura del río Balsas, frente a la costa de Michoacán.**

La cifra del gobierno fue oficialmente de alrededor de 10 mil muertos; sin embargo, fuentes extraoficiales afirmaron que pudieron haber llegado a ser más de 40 mil sólo en la Ciudad de México. El sismo tuvo un grado de intensidad y afectación variable en el Valle de México, siendo catalogado en la porción central de la Ciudad de México como VIII (destructivo) o IX (muy destructivo), mientras que en la parte metropolitana dentro del grado VI (fuerte) en la escala de Mercalli.

20 de septiembre de 1985, **7.3 y 7.5, Zihuatanejo, Guerrero.**

Réplica más significativa del sismo del 19 de septiembre de 1985, la cual tuvo una profundidad de 17.6 km. Terminó por colapsar edificaciones dañadas por el sismo del día anterior, asimismo causó alarma y pánico en la Ciudad de México y en la región epicentral. En la capital del país fue catalogado como grado VI (fuerte) en la escala de Mercalli.

7 de septiembre de 2017, **8.2. Pijijiapan, Chiapas.**

Tuvo una profundidad de 58 km y una duración de 2 minutos. Se considera el más fuerte que se ha dado en el país en épocas recientes y de los más fuertes en la historia de México. El Servicio Sismológico Nacional contabilizó más de 20 mil réplicas, dos de los más fuertes el 8 y 23 de septiembre de magnitud 6.1. El sismo causó la muerte de 100 personas, 78 en Oaxaca, 18 en Chiapas y cuatro en Tabasco.

19 de septiembre de 2017, **7.1. Tuvo una profundidad de 57 km.**

Ocurrió el mismo día del aniversario luctuoso 32 del Terremoto de México de 1985. Han sido reportados 369 muertos y 100 desaparecidos en diferentes entidades del país y más de 44 edificios dañados en la Ciudad de México. Fue percibido en gran parte del país (zona centro, capital y alrededores).

LA HISTORIA SE REPITIÓ

Una tragedia que se repite 32 años después, el 19 de septiembre de 1985 un terremoto con epicentro en Michoacán de 8.1 en escala de Richter sacudió a la capital de México. 2017, después de 32 años exactamente el 19 de septiembre un terremoto con epicentro entre los estados de Morelos y Guerrero golpea la capital mexicana también dejando víctimas y pérdidas incontables. Hechos que por naturaleza crearon pánico, caos, estado de emergencia y que habrá que conmemorar año con año.

México al estar registrado como zona sísmica, tiene la obligación de estar monitoreando permanentemente los movimientos de la tierra, por ello es que cuenta con el Servicio Sismológico Nacional (SSN) de la Universidad Nacional Autónoma de México (UNAM), y desde 1948 quedó adscrito al Instituto de Geofísica de la UNAM (Universidad Nacional Autónoma de México), el cual tiene como objetivo principal el registrar, almacenar y distribuir datos del movimiento del terreno para informar sobre la sismicidad del país a las autoridades y a la población en general, promover el intercambio de datos y cooperar con otras instituciones de monitoreo e investigación a nivel nacional e internacional.

El Sistema Nacional de Protección Civil nace después de que el terremoto de magnitud 8.1 grados Richter azotara a México en 1985, surge como un esfuerzo del Estado para crear y fortalecer una cultura con el fin de salvaguardar la seguridad, el patrimonio y la vida de todos los mexicanos.

Formadas decenas de personas sin hacer ruido alguno levantando el puño a lo alto para mantener el silencio y buscar una señal de vidas

Foto: The New York Times

1985

Jueves 19 de septiembre de 1985,

"un terremoto sacudió a México a las 7:17 de la mañana, alcanzando una magnitud de 8.1 grados en la escala Richter. El epicentro del movimiento telúrico se localizó en el océano Pacífico, en la costa del estado de Michoacán. Las zonas afectadas fueron el centro, sur y occidente del país. El temblor provocó daños severos en cientos de edificios de la capital mexicana y cambió por completo la imagen de la Ciudad de México, no se conoce el número exacto de víctimas, las pérdidas económicas superaron los 4 mil millones de dólares. Hasta el momento es el más significativo y dañino, registrado en la historia contemporánea del país. La réplica ocurrió un día después, la noche del 20 de septiembre. También tuvo una enorme repercusión en la capital mexicana, donde terminaron de colapsar estructuras y edificios reblandecidos el día anterior"[1].

Los hospitales Juárez y General, el Centro Médico Nacional, el edificio Nuevo León de Tlatelolco, el multifamiliar Juárez, el Hotel Regis y los sitios de trabajo de las costureras en la avenida San Antonio Abad fueron algunos de los 371 edificios que colapsaron.

2017

Martes 19 de septiembre de 2017, "el Servicio Sismológico Nacional reportó un sismo con magnitud de 7.1 grados en la escala de Richter, localizado en el límite estatal entre Puebla y Morelos, a 120 kilómetros de la Ciudad de México. El terremoto sucedió exactamente 32 años después del sismo de 8.1 grados Richter que azotó a México en 1985, se sintió fuertemente en el centro del país y ocurrió a 1:14 de la tarde. El temblor dejó como saldo más de 100 personas fallecidas, incendios aislados, decenas de edificios se derrumbaron y alrededor de dos millones de personas se quedaron sin electricidad durante varias horas"[2].

IMPACTO EN LA SOCIEDAD MEXICANA

Algo que caracteriza al pueblo mexicano es su solidaridad con otros, la empatía y la unión que crean al estar en sincronía por una causa, ayudar, algo que se ha visto reflejado en cada emergencia o situación de caos, el pueblo mexicano es el primero en querer ayudar, aportar con algo, sentirse útil ante la impotencia de la tragedia.

En ambos casos la sociedad mexicana se paralizó de sus actividades cotidianas y rutinarias para estar al pendiente de lo que pudiera necesitar cualquier extraño que se viera afectado por los sismos, ante eventos como éste es fácil que la apatía y la indiferencia social desaparezca, todos querían aportar su granito de arena, rápidamente se movilizaron para ubicar los edificios derrumbados, brigadas de auxilio se posicionaron, fue una coordinación de respuesta rápida, entre organizaciones civiles, autoridades, grupos de rescatistas, trabajadores, estudiantes, niños, adultos, perros en fin, todos cooperaron para remover escombros y de entre piedras, palos, cables, en "fila india" formados decenas de personas sin hacer ruido alguno levantando el puño a lo alto para mantener el silencio y buscar una señal de vidas, como si hubieran entrenado, así fue la búsqueda de personas que resulto exitosa para algunos, mas no para todos.

Los sismos que terminaron en tragedia mostraron la vulnerabilidad y fragilidad a la que todas las personas pueden estar expuestas en un segundo sin importar el poder adquisitivo que pudieran tener, el dinero en el banco, las propiedades, etc., las tragedias no discriminaron.

NUEVA LEY DE CONSTRUCCIÓN

Este reglamento, creado en 1920, es el marco normativo que establece, entre otras cosas, la altura, espacio y especificaciones de las construcciones en la ciudad. Desde su creación, el reglamento de construcciones ha sido modificado de manera importante en cuatro ocasiones, dos de éstas a partir de los sismos de 1957 y 1985, fue ahí cuando se comenzó a hablar de seguridad estructural.

Tras el terremoto del 19 de septiembre de 1985 se volvió a actualizar el reglamento para reforzar las medidas de seguridad estructural; además se agregaron especificaciones en materia de accesibilidad para personas con capacidades diferentes.

De acuerdo con la Gaceta oficial de la Ciudad de México, después de los sismos de 2017, los esfuerzos por reconstruir los inmuebles e infraestructura afectados no fueron suficientes ni integrales entre todos los órganos del gobierno capitalino de aquel entonces, por lo que se han hecho cambios, derogaciones y adiciones al plan de reconstrucción, con la finalidad de actualizar el proceso. Las modificaciones contemplan los inmuebles para vivienda, establecimientos comerciales, infraestructura de servicios, patrimonio cultural e histórico y un nuevo diagnóstico de daños.

México está preparado con planes de contingencia y emergencia de sismos, es uno de los países que más invierte en el estudio y monitoreo del movimiento natural de las placas tectónicas de América. ■

Foto: El Universo

La cifra del gobierno en el terremoto de 1985 fue oficialmente de alrededor de 10 mil muertos; sin embargo, fuentes extraoficiales afirmaron que pudieron haber llegado a ser más de 40 mil sólo en la Ciudad de México

REFERENCIAS

[1] *https://unamglobal.unam.mx/19-de-septiembre-lo-que-paso-un-dia-como-hoy/*

[2] *https://www.dgcs.unam.mx/boletin/bdboletin/2015_543.html*

- *https://www.milenio.com/politica/comunidad/como-cambio-el-reglamento-de-construcciones-tras-los-sismos*

ASIS INTERNATIONAL
CAPÍTULO MÉXICO 217

¡MITAD DE AÑO MITAD DE PRECIO!

RENOVACIÓN ASIS México 217

$1,875 MXN

Internacional
$ 120 UDS

AFILIACIÓN ASIS México 217

$2,825 MXN

Internacional
$ 60 UDS

¡ÚNETE!

Al unirte a ASIS podrás involucrarte con cientos de profesionales de seguridad de todo el mundo, para conectarse en red, compartir ideas y establecer relaciones que te ayudarán día a día y durante toda tu carrera para alcanzar el éxito.

Como miembro, tendrás acceso a una amplia gama de recursos y beneficios para estar al tanto de las últimas tendencias, desarrollos globales e innovaciones de seguridad para mitigar el riesgo y mantenerse a la vanguardia.

MÁS INFORMACIÓN

(55 3437 6890

info@asis.org.mx

ENTREGA DE DONATIVOS A VOLUNTARIADO POPOTLA

Regresar un poco a quienes protegen a todos los mexicanos

MÉXICO | Erick Martínez / *Staff* Seguridad en América

En México existen muchos héroes a los que como sociedad les debemos mucho, y nos referimos por su puesto a las Fuerzas Armadas del Ejército Nacional Mexicano, que si bien México es un país pacifista que opta en todas las situaciones por la diplomacia, el diálogo y la resolución de conflictos por la paz, cuenta con un Ejército que está al frente de cualquier situación que pueda comprometer la integridad de las personas en todo su territorio e incluso en otros países.

México se ha caracterizado por ser uno de los primeros países en aportar y apoyar ante las catástrofes naturales o situaciones de emergencia de cualquier parte del mundo, y es la Marina y el Ejército mexicano quien da respuesta pronta y oportuna mediante diferentes planes de contingencia.

El sector privado reconoce y enaltece su gran compromiso y labor diario, por lo que a través de la casa editorial **Seguridad en América** (**SEA**) y su director general Samuel Ortiz Coleman, en el evento "Los 100 más influyentes de la seguridad privada en México", múltiples representantes de empresas de seguridad privada como: Pedro Sanabria, director de Trust Group; Gustavo Espinosa, director de GSI Seguridad Privada; Josué Ramírez, director de Administración y Finanzas de CIA Kapital; Cap. Salvador López, director general de CIA Kapital; Gerardo Macías, director de Protectio; y Marcos Solórzano, CEO de SOLCAT, fueron además de galardonados, los principales donadores en especie de sillas de ruedas, *laptops*, *smartphones* y iPads, que fueron dirigidos al Voluntariado Popotla.

Esto fue posible a través de la titular Belinda Judith Solís Cámara, quien se encargó de distribuir todos los donativos a diferentes hospitales como el Hospital Central Militar (HCM), el Centro de Rehabilitación Infantil (CRI) y al propio Voluntariado Popotla de la Secretaría de la Defensa Nacional (SEDENA), casas de retiro y organismos del Ejército mexicano para poder apoyarles con infraestructura nueva a todos aquellos que han servido a la nación.

El evento de "Los 100", es un evento organizado por **Seguridad en América** cada cinco años, dedicado a reconocer el trabajo de todos los miembros que se encargan de promover y mantener la seguridad en México, así como quienes aportan con grandes ideas, tecnología o la misma administración de la seguridad.

VOLUNTARIADO POPOTLA

Voluntariado Popotla es una organización altruista de índole social, cuyas actividades están orientadas a elevar la calidad de vida de la familia militar a través del desarrollo humano. Conformada por derechohabientes de la o del militar, quienes llevan a cabo por decisión propia actividades culturales, educativas, de capacitación para el trabajo, de asistencia social y de convivencia, en beneficio de la familia militar.

A través de distintas actividades como: capacitar para el trabajo en actividades productivas, los niveles educativos y cultural, actividades de asistencia social en beneficio de la familia militar, entre las que se encuentran la atención a requerimientos básicos en subsistencia en materia de alimentación, vestido o vivienda y la orientación social, educación o capacitación para el trabajo. Se busca mejorar la vida de las familias fomentando actividades de desarrollo humano en un marco de participación voluntaria, individual o colectiva, con un amplio espíritu de servicio y compromiso. ■

Fotos: Erick Martínez / SEA

EXECUTIVE PROTECTION SUMMIT 2022

18 Y 19 OCTUBRE

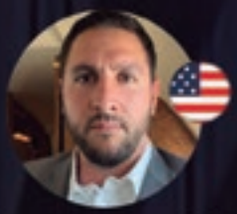
epsummit.com.mx

Rory Stein

Protegiendo a Mandela

Chris Hadnagy

The art of human hacking



Joe Lasorsa, CPP

KPI's & ROI: Proving the negative

Johnny Torres

Resultados de la avanzada hacia el mundial a Qatar

INSCRÍBETE CON EL CÓDIGO #SEA Y OBTÉN COSTO PREFERENCIAL

Kenn Kurtz

Tony Rosario

Protección de personas en zonas de alto riesgo: Medio Oriente y Frontera norte de México

Tte. Cnel. Antonio Gaona

El lado humano de la protección de personas

Michael Julian, CPI, PPS, CSP

The active shooter profile causas y detonantes históricos

Dr. Cecilio Andrade

Mitos y cine en el adiestramiento de la protección ejecutiva

Paulo de Gregoire

Geopolítica y seguridad en LATAM sucesos que han conformado nuestra situación actual y la redistribución del crimen

SEGURIDAD EN AMÉRICA

#LasCosasComoSon

COLUMNA ALAS
COMITÉ NACIONAL MÉXICO

Carlos Román Martínez Sánchez,

Más sobre el autor:

director general de Multisoluciones en Seguridad Integral TI y secretario para ALAS Comité México 2022.

Foto: Creativeart - Freepik

LA GRATITUD

MÉXICO

¿Cuántas ocasiones nos hemos sentido que se nos acaba el mundo? Nuestros problemas o situaciones, no necesariamente agradables, por las que estamos pasando nos llevan a pensamientos negativos o de tristeza. Deseamos que algo suceda mágicamente o que alguien aparezca con una varita mágica y nos solucione estas situaciones. Sin embargo, no alcanzamos a reconocer que la solución la tenemos a la mano y que la podemos ejercer en el momento que deseemos.

Y esta solución mágica se llama "gratitud". La gratitud nace del corazón y puede convertirse en una fortaleza, así como una herramienta en nuestro día a día. Cuanto más agradecemos todo lo que tenemos y todo aquello con lo que estamos interactuando, más se manifiesta lo que deseamos en nuestra realidad presente.

La gratitud es ese sentimiento de valoración y estima de un bien recibido, espiritual o material, el cual se expresa en el deseo voluntario de correspondencia a través de las palabras o a través de un gesto.

Desde la psicología positiva entendemos a la gratitud como esa fortaleza o cualidad, característica o punto fuerte de la persona que está presente desde el nacimiento de manera innata.
La mente juega un pilar importante en nuestro día a día cuando hablamos de la gratitud, ya que es una herramienta que nos ayuda con la realidad que vive nuestra mente para así poder manifestar lo que queremos. Es por eso que cada vez que agradecemos estamos diciendo a nuestra mente "si tengo", "si soy".

Entonces nos enfocamos automáticamente en todo aquello que deseamos y apreciamos en lugar de simplemente quejarnos y reconocer que todo lo que sucede en nuestras vidas tiene un por qué y eso es una lección de aprendizaje que el universo nos está enviando para aprender y evolucionar. Todo lo que en la vida nos sucede tiene una razón de ser.

¿POR QUÉ ES IMPORTANTE AGRADECER?

La gratitud es un sinónimo de la abundancia, si quieres ser abundante, agradece. Practicar el ejercicio de agradecimiento es como ir al gimnasio, te vas fortaleciendo y se convierte en una disciplina. En cambio, cuando no agradecemos, nuestra mente se va a enfocar en lo que no tenemos. Al contrario de agradecer, cuando lo hacemos, le estamos mandando un mensaje a nuestra mente en el que le decimos

tengo y cuando digo tengo, me siento suficiente, completo y afortunado.

La investigación científica en torno a la gratitud y la salud, ha llevado a una multitud de descubrimientos prometedores. Entre los muchos hallazgos significativos dentro de este campo de estudio, la Universidad de California (UC Davis Health) publicó que "ser agradecido está relacionado con la disminución de las medidas de estrés y depresión".

¿CÓMO PUEDES PRACTICAR LA GRATITUD EN TU VIDA DIARIA?

La gratitud es nuestra puerta de entrada a la abundancia. Muchas investigaciones científicas han revelado un vínculo significativo y fuerte entre la gratitud y la mejora de las medidas de bienestar y salud.

Según el Centro de Investigación de Conciencia de la Atención Integral de la UCLA, expresar gratitud cambia literalmente la estructura molecular de nuestro cerebro, y es que mantiene la materia gris en funcionamiento, nos convierte en personas más saludables y felices.

La gratitud es tu puerta de escape de esa negatividad, cuando tú agradeces algo negativo que te está sucediendo, (aparentemente, ya que todo sucede por algo y para bien) entonces la soluciones aparecen mágicamente.

ALGUNOS ERRORES QUE COMETEMOS AL AGRADECER

Uno de los errores más comunes que se cometen al querer agradecer es el pedir desesperadamente, es decir, cuando somos pequeños a la mayoría nos enseñaban a rezar y siempre se trató de: "Dios, dame esto", "Dios, ayúdame con tal cosa", "dame", "dame", "dame"… y cada que decimos "dame", le decimos a la mente "no tengo" y el "no tengo", a nosotros como seres humanos, nos genera ansiedad y no nos sentimos suficientes. Nos creemos eso, que no tenemos suficiente, pero tenemos la opción de preferir tener más manifestando. La magia de la gratitud es la que te ayuda a vivir en estado de abundancia. La gratitud la tienes dentro de ti y se puede simplemente practicar.

¿CUÁLES SON LOS BENEFICIOS DE LA GRATITUD?

- Aumenta la sensación de bienestar tanto en quien la siente, como en quien la recibe.
- Ayuda a disminuir el estrés, la depresión y la ansiedad.
- Favorece la calidad del sueño.
- Mejora las relaciones sociales al ser signo del reconocimiento del otro y su impacto positivo en nuestra vida.
- Refuerza la autoestima del otro y lo inspira a seguir siendo generoso o amable con otros.

Foto: Creativeart - Freepik

> Cuanto más agradecemos todo lo que tenemos y todo aquello con lo que estamos interactuando, más se manifiesta lo que deseamos en nuestra realidad presente

Al realizar un estudio donde participaron 238 personas con un rango de edad entre 19-44 años, los resultados obtenidos mostraron una correlación positiva entre la gratitud y unos niveles elevados de emociones positivas, como la satisfacción con la vida, la vitalidad y el optimismo.

En conclusión, desarrollar y practicar la gratitud parece tener una variedad de beneficios para la salud y la curación. La apreciación también parece tener el potencial de ayudar en el tratamiento de bastantes afecciones y trastornos de salud mental y física.

Una multitud de investigadores científicos determinaron las modalidades y la eficacia de las intervenciones de gratitud para una variedad de afecciones, trastornos médicos y de salud mental. Hay mucha investigación sólida que respalda los muchos efectos positivos que la gratitud puede tener en la salud psicológica y física. No se puede negar que practicar la gratitud es benéfica para todos. Al igual que cualquier otra habilidad, la gratitud es algo que debe practicarse y desarrollarse a propósito en la vida cotidiana. Puede lograr esto incorporando cualquiera de las muchas prácticas de mejora de la gratitud, descritas en este artículo, en su rutina diaria. ■

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

EL APEGO PATOLÓGICO PROCLIVE A **CONDUCTAS ANTISOCIALES**

El origen de la existencia de síntomas de conductas agresivas en los jóvenes, incapacidad de afecto y sentimientos de culpa, así como dificultades en establecer relaciones

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

MÉXICO | Wael Sarwat Hikal Carreón

INTRODUCCIÓN

Edward John Mostyn Bowlby nació el 26 de febrero de 1907 en Londres, del antiguo Reino Unido de Gran Bretaña e Irlanda, y falleció el 02 de septiembre de 1990 en Reino Unido. Es reconocido por la creación de la Teoría del vínculo o del apego, de su nombre en inglés: *Attachment theory*. En su concepto, "apego" significa una necesidad a mantener cercanía y contacto (lazo de afecto) con una imagen protectora, denominada "figura de apego", presente en todos los individuos, con variaciones de acuerdo a la edad (Ortíz y Marrone, 2002).

DESVIACIONES EN LOS CUIDADOS MATERNOS

Marchiori explica: "Cuando el niño carece de una relación cálida y constante sufre de una privación que él denomina privación materno-afectiva. Distingue privación total, la cual es frecuente en instituciones, guarderías y hospitales, donde los niños no cuentan con una persona que los cuida en forma individual y con la cual pueden sentirse seguros. Las privaciones parciales aun cuando viva en su hogar, la madre es incapaz de proporcionar el cuidado afectivo" (2011, p. 140).

Sobre lo anterior, los celos son causantes de muchas patologías durante la vida, si se observa que desde la infancia las figuras son aisladas, en la adultez, serán personas celosas e inseguras, que perciban casi cualquier cosa como poco tangible, un trabajo, una calificación, ingreso a algún lugar, una aceptación, una respuesta prolongada, hacía una pareja, etcétera, son percibidos con perspicacia debido a lo disfuncional que fue la relación afectiva durante la niñez (Ortíz y Marrone, 2001). Posiblemente así se puedan explicar también las relaciones intensas y hipercelosas (Muñoz y Sánchez, 2006), en la búsqueda de aquella figura ausente y que tienen miedo a perderla o que se ausente. Bowlby concluyó que es esencial una relación cálida y continua con una figura materna para un desarrollo saludable de la personalidad (Freedman, Kaplan y Sadock, 1979).

INSTITUCIONALIZACIÓN

Los niños pequeños sometidos a una residencia prolongada en ambientes institucionales pobres, desarrollan déficit y patologías intelectuales y de personalidad. Las funciones motoras prontas que más dependen de la maduración parecen ser las menos afectadas; las funciones perceptivo-cognitivas y de lenguaje parecen ser las más vulnerables (Ortíz y Marrone, 2001). Las manifestaciones de retraso intelectual y lenguaje se muestran en una época muy temprana de la infancia y se intensifican con la institucionalización continuada (Freedman, Kaplan y Sadock, 1979).

Asimismo los niños pequeños que han crecido en instituciones dejan a menudo de desarrollar pautas normales de respuesta social: tienden a convertirse en aislados e indiferentes (Medina Alva, Kahn, Muñoz Huerta, Leyva Sánchhez, Calixto y Vega Sánchez, 2015). Estas desviaciones precoces de la conducta personal social son consideradas precursoras de desviaciones posteriores de la personalidad caracterizadas por escaso dominio de los impulsos, falta de sentimientos adecuados de culpabilidad después de una conducta agresiva y destructiva y una incapacidad de establecer relaciones interpersonales estrechas y significativas (Freedman, Kaplan y Sadock, 1979).

Al analizar el impacto del cuidado institucional deben considerarse variables como las siguientes: la cantidad, calidad y variedad de estimulación sensorial y perceptual proporcionada por los cuidadores, la cantidad de oportunidades para adquirir y practicar las aptitudes, el momento y lo adecuado de las respuestas del cuidador a la conducta del niño, el grado de continuidad de los cuidados proporcionados por una figura maternal, la calidad del intercambio afectivo con la madre sustituta, la edad del niño en el momento de la institucionalización y la duración del cuidado institucional. Parece haber una relación directa entre la importancia del retraso intelectual y lenguaje y el grado de estimulación sensorial y verbal flotante en el ambiente institucional (Ortíz y Marrone, 2001).

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

El alejamiento del padre del núcleo familiar producirá una ansiedad de separación en el niño, que debe alejarse de su padre, que es una figura importante para su desarrollo

FUNCIÓN MATERNA MÚLTIPLE

La multiplicidad de cuidadores tiende a crear un ambiente impredecible para el niño pequeño; es decir, tiene oportunidades limitadas para desarrollar expectativas constantes hacia una persona. Además, no es probable que los cuidadores adapten su trato a las características peculiares del niño, limitando así los tipos de interacciones recíprocas que son básicas para que se desarrollen relaciones interpersonales significativas y pautas normales de identificación (Muñoz y Sánchez, 2006). La importancia materna no siempre se asocia a depravaciones graves o a interrupciones traumáticas en los cuidados. La presencia de más de una figura maternal puede asociarse a una estimulación más variada (Freedman, Kaplan y Sadock, 1979).

SEPARACIÓN MATERNA

Una interrupción en la continuidad de la relación con una figura materna es una experiencia turbadora para los niños, tal como lo manifiesta su conducta en el momento de la separación e inmediatamente después. Al principio, los niños separados tienden a manifestar una protesta abierta y activa buscando contacto humano en un intento aparente de encontrar una madre sustituta. Esta conducta, llamada de "hambre de afecto" se sigue habitualmente de un rechazo activo de las personas. Finalmente, el niño se aísla de su ambiente y manifiesta una conducta deprimida. En niños situados en ambientes interpersonales sin un cuidado maternal sustitutivo adecuado se produce una depresión cada vez más grave (Freedman, Kaplan y Sadock, 1979).

Las implicaciones de las experiencias de separación para el desarrollo posterior de la personalidad dependen de varios factores: de la separación temporal o permanente, de la duración de una separación temporal, del contexto total de las experiencias vitales del niño, del número y carácter de las experiencias previas de separación. No es probable que las experiencias temporales de separación breves tengan efectos permanentes graves, pero pueden desarrollarse trastornos de personalidad graves en niño que han sido sometidos a separaciones repetidas asociadas a otras experiencias traumáticas (Freedman, Kaplan y Sadock, 1979).

RELACIÓN MADRE-HIJO PATOLÓGICA

El rechazo, la contrariedad y ambivalencia de la madre hacia su hijo están a menudo arraigados en trastornos de personalidad. Bowlby llegó a la conclusión de que existe un alto grado de correlación entre problemas emocionales en la infancia y la ausencia completa de un objeto materno o la falta de uno que permita un ejercicio suficiente de las respuestas de unión y proximidad del niño (Rosas Mundaca, Galardo Rayo y Díaz Angulo, 2000; Freedman, Kaplan y Sadock, 1979).

Bowlby observó que los delincuentes jóvenes presentan un suceso de la pérdida pronta de uno de los padres, también señaló que los niños pueden sufrir otras pérdidas importantes, como el rechazo o el abandono. Además concluyó que la separación pronta tenía efectos persistentes e irreversibles sobre la personalidad e inteligencia (Ortíz y Marrone, 2001).

AUSENCIA DEL PADRE

Dentro de las diversas figuras de apego que el individuo va acumulando en su historia de vida como lo son los amigos, hermano, parejas, etcétera, destaca por su posición y cercanía familiar la figura del padre como una imagen protectora que al igual que la madre, supuestamente, acompañará a su hijo en el desarrollo. Ahora bien el siguiente análisis, está enfocado precisamente a la ausencia del padre en la constitución familiar, lo que se da a grandes rasgos por una serie de situaciones (Freedman, Kaplan y Sadock, 1979).

MADRES SOLTERAS

Hoy en día la dinámica familiar que se desarrolla en estos casos es muy común y a la vez bastante compleja, pues la madre, por un lado debe realizar su rol de madre y padre, tanto en lo afectivo como en lo de sustentador, debe trabajar para mantener a su familia y por su desarrollo personal, social y profesional.

La figura de apego central y primordial es la madre, pues es la persona que vive con el niño, lo protege y entrega cariño y confianza. Por esta razón, surge y se desarrolla un estrecho vínculo y lazo afectivo al interior de la dualidad madre/hijo. El niño en este caso encuentra la protección y socialización primera en la figura materna, por lo que es posible que la relación se fortalezca bastante, creando incluso una fuerte dependencia entre ambos (Ortíz y Marrone, 2001).

En estos casos es bastante probable que emerjan otras figuras de apego para reemplazar al padre ausente como lo son principalmente los abuelos maternos en los cuales el niño encuentra, especialmente en el abuelo, una figura masculina que pasa a reemplazar la ausencia del padre. De este modo es altamente probable que ésta nueva figura sea de gran relevancia para el desarrollo posterior del menor, pues el niño podrá encontrar en su tío, abuelo u otro, el cariño, protección y socialización de parte de una nueva figura complementaria a la de la madre (Freedman, Kaplan y Sadock, 1979).

En esta dinámica familiar es importante que la madre se conforme como una figura central de apego y que a la vez sea una madre apropiada, para así poder fomentar el comportamiento autónomo posterior. Aun así es importante mencionar que el niño siempre va a tener un miedo a la separación, una angustia de alejamiento que se verá proyectada principalmente hacia

Foto: Creativeart - Freepik

la figura materna, pues al ser esta la primordial de protección el niño, temerá perderla pues quedará desvalido (Rosas Mundaca, Galardo Rayo y Díaz Angulo, 2000).

Por esta razón es fundamental realizar un apego seguro (Ortíz y Marrone, 2001), pues de lo contrario el niño puede desarrollar problemas de afectividad en lo que hace referencia a la relación con otros, ansiedad y socialización.

SEPARACIÓN O DIVORCIO

En estos casos la ausencia del padre provoca en el niño una fuerte ansiedad de separación, pues pierde a una de sus figuras de apego centrales. Esto, entendiendo que antes de la separación, el niño encontraba la protección y cariño en ambas personas presentes, lo que al alejarse el padre de la dinámica familiar deja un vacío en el niño (Freedman, Kaplan y Sadock, 1979).

Por esta razón las crisis matrimoniales producen una angustia de separación en el niño sobretodo si este proceso es mal manejado. Las consecuencias que puede tener, aparte de la angustia de separación, es un posible apego inseguro, ya que el niño puede percibir una carencia de amor e incluso una ambigüedad en el discurso de los padres (Vaidés Cuervo, Martínez, Urías Murrieta, Ibarra Vázquez, 2011; Freedman, Kaplan y Sadock, 1979).

En este aspecto el niño puede caer en un modelo de cuidado compulsivo, pasando a convertirse en el hombre de

Foto: Creativeart - Freepik

El niño encuentra la protección y socialización primera en la figura materna, por lo que es posible que la relación se fortalezca bastante, creando incluso una fuerte dependencia entre ambos

NENA
THE 9-1-1 ASSOCIATION
LATAM

15° CONGRESO INTERNACIONAL NENA 9-1-1

05-07 OCTUBRE 2022

RIVIERA MAYA, MÉX.

HOTEL BARCELÓ MAYA GRAND RESORT

INCLUYE

- HOSPEDAJE TODO INCLUIDO
- CONFERENCIAS MAGISTRALES
- EXPO NENA
- EVENTOS PRIVADOS
- KIT DE PARTICIPANTE
- CONSTANCIA

REGÍSTRATE AQUÍ

www.911latinoamerica.org NENA 9-1-1 LATAM @nena_911mx @MexicoNENA911

la familia, preocupándose en las necesidades del otro y cuidando a su madre (Ortíz y Marrone, 2002), especialmente si esta tiene un carácter depresivo, y a los posibles hermanos menores. De este modo el niño tiende a cumplir la función de protección.

AUSENCIA DEL PADRE POR DEFUNCIÓN

Es sabido que cualquier pérdida al interior de la familia produce una serie de perturbaciones en la dinámica familiar y en las relaciones que se producen al interior de esta. El fallecimiento del padre conlleva la pérdida definitiva de una importante figura de apego para el niño por lo que se hace primordial que este viva el proceso de duelo que le significa la pérdida de un ser querido, lo que le provocará entre otras cosas, angustia (Freedman, Kaplan y Sadock, 1979).

Además se hace fundamental en este caso, que la figura materna le demuestre al niño cariño, comprensión y apego incondicional, pues al perder la figura del padre el niño se sentirá más desprotegido que cuando contaba con sus dos progenitores (Rosas Mundaca, Galardo Rayo y Díaz Angulo, 2000).

La madre debe transformar su dinámica familiar pues tendrá que pasar a cumplir además de su rol de madre, de padre en lo que a nivel afectivo y además de convertirse en la sostenedora de la familia. Es importante que en este periodo de pérdida se fortalezca el lazo de apego existente entre madre y hijo, con la finalidad de que el niño se sienta seguro y desarrolle la confianza en su madre (Ortíz y Marrone, 2002).

Foto: Creativeart - Freepik

CARENCIA DE LA RELACIÓN CON EL PADRE

Dentro de este aspecto se pueden mencionar las enfermedades y hospitalizaciones, motivos laborales, encarcelamiento u otros similares. Todos estos temas tienen en común el alejamiento del padre del núcleo familiar lo que producirá una ansiedad de separación en el niño, que debe alejarse de su padre, que es una figura importante para su desarrollo. Al igual que en los casos anteriores es importante que el niño no se sienta desprotegido ante el alejamiento temporal de su padre y que en ese transcurso de tiempo logre encontrar en su madre. Una madre apropiada que le proporcione atención, cariño y seguridad, para que de este modo se pueda suplir temporalmente la ausencia afectiva que le produce al niño el alejamiento del padre (Freedman, Kaplan y Sadock, 1979).

Bowlby realizó observaciones a jóvenes quienes habían sufrido privación materna en edades tempranas, mostrando la existencia de síntomas de conductas agresivas, incapacidad de afecto y sentimientos de culpa, dificultades en establecer relaciones (Muñoz y Sánchez, 2006). ■

Foto: Creativeart - Freepik

> Bowlby observó que los delincuentes jóvenes presentan un suceso de la pérdida pronta de uno de los padres, también señaló que los niños pueden sufrir otras pérdidas importantes, como el rechazo o el abandono

REFERENCIAS

- *Freedman, A., Kaplan, H. y Sadock, B. (1979). Compendio de Psiquiatría. Salvat Editores.*
- *Marchiori, H. (2011). Criminología. Editorial Porrúa*
- *Medina Alva,M.P., Kahn, I.C., Muñoz Huerta, P., Leyva Sánchez, J., Calixto, J.M. y Vega Sánchez, S.M. (2015). Neurodesarrollo infantil: características normales y signos de alarma en el niño menor de cinco años. Revista Peruana de Medicina Experimental y Salud Publica. 32(3). 565-573. http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S1726-46342015000300022*
- *Muñoz, A. y Sánchez, M. (2006). Estructura de la familia de origen del trastorno límite de la personalidad. Ajayu. 4(1). 59-89. http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2077-21612006000100004*
- *Ortíz, E. y Marrone, M. (2002). La teoría del apego. Un enfoque actual. Revista Internacional de Psicoanálisis Aperturas. 10. http://www.aperturas.org/articulo.php?articulo=0000198*
- *Rosas Mundaca, M. Galardo Rayo, I. y Díaz Angulo, P. (2000). Factores que influyen en el apego y la adaptación de los niños adoptados. Revista de Psicología. 9(1). http://www.redalyc.org/pdf/264/26409110.pdf*
- *Vaidés Cuervo, Á.A., Martínez, E.A.C., Urías Murrieta, M., Ibarra Vázquez, B.G. (2011). Efectos del divorcio de los padres en el desempeño académico y la conducta de los hijos. Enseñanza e Investigación en Psicología. 16(82). 295-308. https://www.redalyc.org/pdf/292/29222521006.pdf*

Wael Sarwat Hikal Carreón,
director de Proyectos en la Sociedad Mexicana de Criminología Capítulo Nuevo León, México..

Más sobre el autor:

ASIS INTERNATIONAL | LATAM

ASIS LATAM 2022

SEGURIDAD MÁS ALLA
DE CUALQUIER **FRONTERA**

PRIMER CONGRESO

LATINOAMERICANO DE ASIS INTERNACIONAL

CONFERENCISTAS INVITADOS


Brian Allen
ASIS Foundation
Past President


Mercedes Escudero
Vicepresidenta ASIS
Capítulo Yucatán


José Gonzalez
CEO Aion Group


Malu Milan
Accenture


Juan Muñoz
CPP CSMP CSyP
FSyI F.ISRM MBA


Carlos Veiga
RSOM Latin
America TWITTER


Mario Arroyo
Doctor


Servio Carney
MSc, CPP


José Murillo
CPP


Alvar McBride
CPP


Farah Urrutia
Experta Sistema
Interamericano de DDHH


MG. Fernando Murillo
Director Inteligencia
Criminal Policía


Christian Bernard
CPP, CEO
BS Consulting


Jeffrey A. Slotnick
CPP
CEO Setracon


Dagoberto Santiago
Dir. de Seguridad
PepsiCo Mexico


Salvador Morales
CPP


Lourdes Morales
Walmart Mexico &
Central America


Humberto Sanibañez
CPP, BESAFE
Consulting


Gigi Agassini
CPP,
CEO GA Advisory

RESERVA LA FECHA

OCTUBRE 23-25 2022

CANCÚN, MÉXICO. HOTEL GRAND FIESTA AMERICANA CORAL BEACH

INFORMACIÓN Y REGISTRO
https://asisonline.lat

DiDi · IPS · TPS · convergint · milestone · MSPV Seguridad Privada
AFIMAC · AXIS Communications · decysyon · EyeDetect · GIF · Grupo Salus
Lider Man · Prosegur · punto · SecuSoft · tiLatina · Altair · Concord Defense

¿POR QUÉ TIENE MALA FAMA LA TOLERANCIA CERO?

¿Cómo interviene la seguridad 4.0 en la implementación?

Foto: Twitter

ARGENTINA | Modesto Miguez

El término "tolerancia cero" puede generar reacciones negativas en quienes no conocen su significado, debido a que asumen que implica una ausencia de compasión, brutalidad policial o la represión de las libertades. Sin embargo, la esencia del concepto no es la intolerancia, sino la confianza.

Lo mal visto del concepto deviene de una degradación cultural y de valores de más de un siglo de antigüedad. Hay un ejemplo inmortalizado en el tango de Enrique Santos Discépolo: "El que no llora no mama y el que no afana es un gil".

¿Entonces? Deberíamos rever el significado de algunas palabras y de cómo este cambió en pocas décadas, cuando de pequeños nos referíamos al vigilante de la esquina, veíamos en él a una persona que ayudaba a cruzar la calle a un no vidente a quien se le podía consultar cualquier cosa y respondía gentilmente, un representante del estado respetado y con la autoridad necesaria para que su sola presencia impusiera la ley, desalentando la ocurrencia de delitos y creando un clima de seguridad y protección.

Entonces el "vigilante" era bien visto, los militares podían caminar orgullosos con su uniforme y considerados por la comunidad servidores públicos defensores del orden y de los valores. Los tiempos cambiaron y el vigilante, el militar, el policía son sinónimos de vigilante, botón, alcahuete, buchón, rati, ortiva, gorra, yuta. Todos términos asociados a la mala fama de la tolerancia cero por personas que no tienen claro donde está la línea divisoria entre la libertad y el libertinaje.

Hay antecedentes que se remontan al debate típico de los setenta sobre la ley y el orden. El conocido caso de éxito de William Braton en la ciudad de Boston, Estados Unidos, más tarde replicado en la ciudad de Nueva York a pedido del Alcalde Rudolf Giugliani y aunque la estrategia de tolerancia cero fue anterior, en varios casos vino a representar un punto final al fatalismo de lo que solía llamarse el "nada funciona"; es decir, la policía es incapaz de reducir la criminalidad, las prisiones no rehabilitan, el delito es cada vez más violento y nada de lo que hagamos funciona.

Con la tolerancia cero se decidió poner fin a todo síntoma de impunidad y dejar claro que la ley está ahí para respetarse. Con todo se pretende también alcanzar a los actos de corrupción extremadamente arraigados tanto en el ámbito público como privado. No importa el por qué se delinque, lo importante es hacer valer la ley. Quien la transgrede se tendrá que atener a las consecuencias, o en otras palabras, "guerra sin cuartel a la delincuencia" era una manera sutil de referirse a "tolerancia cero". En estos casos se trató de convencer a los ciudadanos de que se lo viera como algo positivo, que ayudará a recobrar las calles ahora ganadas por la delincuencia. En suma, la tolerancia cero es una ideología sobre el delito que recupera los principios morales.

Analizando en la historia, reacciones como la ley del Talión: "Quien mata debe morir" o la del Viejo Oeste que terminaban con el "dale otra mano de bleque", evolucionaron en la década de los 80 con la "declaración de guerra al crimen" en Estados Unidos, apalancados con una era tecnológica que supondría, a esta altura problemas de seguridad superados (cosa que no ocurrió).

La realidad demuestra que la problemática multicausal de la inseguridad no se soluciona con más cámaras. Básicamente endureciendo penas, privatizando y ampliando el servicio penitenciario. La gran duda es si en nuestros países hispanoparlantes existe el liderazgo necesario para convencer sobre la necesidad de cambios. Cambios que deberían comenzar por el poder legislativo, de quien se observa escasa dedicación. Entonces podríamos concluir que: ¿Los problemas de inseguridad no son significativos o los representantes del pueblo, están aislados y no representan sus intereses?

La seguridad y la educación son componentes indispensables para el desarrollo económico necesario para vivir en estado de libertad, de paz y bienestar. Tal vez haya que esperar a que "la sangre llegué al río" para que una parte mayoritaria de la gente y sus representantes comiencen a pensar y hablar del

tema. Si ese momento llegara convendría analizar las experiencias de otras sociedades asumiendo que siempre es mejor una buena copia antes que un mal invento. Inventos que ya se hicieron y sólo sirvieron para que algunos vivos parte del problema (corrupción) se enriquezcan ayudando al marketing político vacío de soluciones.

Si ese momento llegara, sería necesario un acuerdo que defina para el largo plazo lo que está bien y lo que está mal. Luego establecer en los códigos penas a quienes hacen el mal e incentivos a quienes el bien. Lo más maravilloso de esto es que no son necesarios recursos económicos, sino consciencia en la valoración de cuestiones como el respeto, la educación y la transparencia.

Ya existe la tecnología necesaria que permitiría la transparencia para detectar las desviaciones en los procedimientos, basados en metodologías probadas por las normas y las buenas prácticas. Mientras esperamos que ese momento llegue, los profesionales agrupados en la ONG: *monitoreo.com*, nos adelantamos ofreciendo una solución gratuita para Seguridad entre Vecinos, con las características detalladas en: *www.monitoreo.com/RSE*

Creemos que hacer "seguridad por mano propia" puede adelantarse a las consecuencias, que de seguir el proceso actual, de manera inevitable permitirán observar cada vez más frecuentemente casos de "justicia por mano propia" como el desenlace inevitable de una tendencia aparentemente irreversible.

SEGURIDAD 4.0

Un uso distinto de herramientas recientes (10 años) desafía a lo establecido y como un efecto disruptivo nace la seguridad 4.0, que consiste en una nueva generación de soluciones basadas en: 1. el uso de la inteligencia artificial, fruto del desarrollo tecnológico por un lado; y 2. de la participación de la gente que interviene en todos los estratos y niveles de un sistema.

1.

La seguridad 3.0 se caracteriza por basarse en centros de control donde convergen la información de cámaras, alarmas y operadores humanos que trabajan intermediando en la información analizando imágenes de video y señales de alarmas notificando de los hechos a quien corresponda y dando avisos a la autoridad de aplicación.

En la seguridad 4.0 los centros de monitoreo no existen, son reemplazados por sistemas 100% integrados en la Nube de Internet. No hay operadores que trabajen para los sistemas, sino asesores que trabajan con los humanos detectando necesidades, organizando y configurando sistemas que realizan verdadera prevención minimizando la ocurrencia de hechos que requerirían una reacción.

Foto:La Jornada

Foto:SSC-CDMX

> Los tiempos cambiaron y el vigilante, el militar, el policía, son sinónimos de botón, alcahuete, buchón, rati, ortiva, gorra, yuta. Todos son términos asociados a la mala fama de la tolerancia cero por personas que no tienen claro donde está la línea divisoria entre la libertad y el libertinaje

Con toda la inteligencia artificial 100% en la nube, el Big Data y la automatización, la inteligencia artificial actúan comunicando inmediatamente mediante redes IP, a quienes deben actuar (robots y humanos) sin necesidad de monitores ni operadores eliminando el espacio físico, los tiempos muertos y los errores.

En este nuevo paradigma, la figura del asesor es el rol más importante para el armado de "centrales de monitoreo virtuales" para grupos de afinidad. En seguridad 4.0 la tecnología está al servicio del humano y no al revés.

2.

Contrariamente a la seguridad anterior donde la información estaba restringida al usuario, la información fluye de forma automática por IP (Internet Protocol) entre sistemas fijos, la Nube de Internet y las aplicaciones móviles (*www.monitoreo.com/apps*).

Rescatando lo indicado en el punto cinco de la norma ISO 31000, que dice: "La seguridad no se compra ni se vende, sino que se hace entre todos los actores participantes, responsables en distintas formas y especialmente con los destinatarios de un bien cada vez mas escaso". ■

Modesto Miguez, CPP,
asesor permanente en 300 empresas de monitoreo y seguridad en toda Latinoamérica y España.

Más sobre el autor:

HABILIDADES DEL MENTOR

Aptitudes con las que un mentor debe intervenir para tener un máximo resultado en el proceso de mentoring

MÉXICO | Mónica Rodríguez

El pasado 25 de mayo del presente año fui partícipe del arranque del programa de *mentoring* en una asociación internacional de seguridad y me complace ver el entusiasmo que se tiene por generar conexión y redes con formas diferentes de interacción.

Si bien el gremio de la seguridad cada vez está más fuerte y ha ido incrementando su campo de acción, las formas de conectar interpersonalmente entre los de la asociación se irán mejorando.

El programa de *mentoring* es un buen ejercicio para ello, ya que es un proceso donde se busca ampliar el campo de acción del *mentée* a través de:

- Espacio de observación atenta y detenida.
- Experiencia de desarrollo, enseñanza y aprendizaje.
- Conectar con recursos, incluir, aportar, cooperar, recibir y dar apoyo con colegas.
- Guía en toma de decisiones.
- Estimular a la acción proyectando hacia el futuro.
- Ampliar posibilidades de conocimiento y acción.
- Incrementar nivel de competencias.

Foto: drobotdean - Freepik

Entrar en un programa de *mentoring* abre las puertas a diferentes beneficios y objetivos como:

1. Generar desarrollo estratégico de talentos. Es importante encontrar el equilibrio entre los nuevos integrantes de una organización y los más expertos. Un proceso de *mentoring* ayuda a permear las nuevas competencias con la cultura ya establecida e integrar a los nuevos colaboradores, así como el intercambio de conocimientos generacionales.
2. Mover a un colaborador hacia nuevas responsabilidades.
3. Impulsar planes de sucesión donde puedes transmitir experiencia para prevenir errores y sucesos con elevado costo económico y de prestigio.
4. Multiplicar el potencial de un proyecto nuevo con asesoramiento y acompañamiento.

Pero no sólo basta con poner los ojos en los objetivos y beneficios. Si bien es imperativo hacerlo, también hay que contemplar el "cómo" se lleva a cabo la intervención del mentor.

El "cómo" y "desde dónde" interviene el mentor pasa a ser un punto importante, ya que existen competencias de liderazgo a desarrollar que ayudan a empoderar al *mentée* (aprendiz).

Foto: drobotdean - Freepik

15 RETOS Y HABILIDADES DE UN MENTOR

Mentoring es un proceso donde la experiencia de acompañamiento se vuelve más importante que el solucionar; es decir, el respeto por el proceso de aprendizaje de los demás facilita más claridad que la misma solución en sí. Es por eso que aquí menciono a continuación quince habilidades blandas con las cuales un mentor debe intervenir para tener de este proceso un máximo resultado.

1. **Es necesario tener una nueva política de tiempo.** Donde el uso del tiempo tiene un significado importante y trascendente. Disfrutar el aquí y el ahora conectando con el compromiso y la responsabilidad que un proceso de acompañamiento implica.
2. **Cuidar el tiempo y el espacio de la sesión.** El intervalo entre sesión y sesión definida y estructurada ayuda. La estructura de un proceso se convierte en una buena herramienta para darle seguimiento y continuidad.
3. **Hacer de esto un ritual.** Generar buenos hábitos de acompañamiento genera confianza y seguridad.
4. **Crear ambiente de fluidez y confianza** en una relación para generar un buen entendimiento del otro. Ser acompañante nos obliga a poner atención en esa otra persona, saliendo de uno mismo para generar conexión.
5. **Definir meta del proceso.** Importante habilidad pues se acompañara al mentee a llegar a un determinado y especifico lugar y tiempo. Al estar clara la dirección existen pocas probabilidades de perderse en el camino.

Foto: drobotdean - Freepik

Un proceso de *mentoring* ayuda a permear las nuevas competencias con la cultura ya establecida e integrar a los nuevos colaboradores, así como el intercambio de conocimientos generacionales

Foto: drobotdean - Freepik

6. Continuar con un plan de acción. Darle seguimiento a las actividades generará emoción al ver las evidencias de avance.

7. Desarrollar la habilidad de la escucha. La escucha es una competencia que todos debemos ir mejorando tomando consciencia de lo importante que tiene en nuestras vidas. El hablar efectivo sólo se logra cuando es seguido de un escuchar efectivo.

Crear conversaciones es parte esencial de un liderazgo y la parte más activa de una conversación es la escucha. El bien entender o el mal entendido está potencialmente presente.

Guido Salmenik lo describe de esta manera: entre lo que piensas, lo que deseas decir, lo que crees que dices, lo que yo deseo escuchar, lo que en realidad escucho, lo que interpreto de lo que escucho, lo que deseo comprender, lo que creo que comprendo y lo que realmente comprendo.

Existen nueve posibilidades de que se produzca un mal entendido: simplemente sucede y termina afectando la relación. Existen diferentes niveles de escucha:

- Sólo dar la impresión de escuchar.
- Participando: escuchando poco pensando y hablando mucho.
- Enfocado en lo que se escucha.
- Enfocado en lo que percibo: escucho, entiendo, veo en el otro. Toda su expresión. La buena escucha es información.

8. Manejo de silencios. Identificar y respetar los silencios que están llenos de reflexión, análisis, pensamientos. Son momentos de contacto con lo intangible e importante para un orden posterior.

9. Intervenir con objetivo de empoderamiento del *mentée*. Cada intervención del mentor debe estar motivado por el crecimiento del *mentée*.

10. Manejo de emociones, juicios y creencias. Las creencias tienen el poder de crear y el poder de destruir proyectos. El manejo de juicios y creencias es para quitar o cambiar del camino las que estorben para el empoderamiento y logro de la meta positiva del *mentée*. Llevar las conversaciones a lo que genera una buena emoción es llevar a la acción. "Si cambia la forma de ver las cosas, las cosas cambian de forma".

11. Identificar valores. Importante elemento para la persecución de un objetivo, ya que los valores y su jerarquía dan la postura ante la vida. Son el motor previo a la emocion de la acción.

12. Ver en el problema "que si" se puede. Un mentor está comprometido con encontrar posibilidades de solución. No está obligado a saber o tener todas las respuestas, pero si a la exploración de recursos y posibilidaes que el *mentée* tiene o puede adquirir.

13. Creer en el potencial infinito humano. Creer que cada persona tiene su potencial infinito conecta con la prosperidad misma.

14. Buscar la innovación. Considerar que de la vulnerabilidad y el caos surge siempre algo nuevo, un nuevo orden, una creación. En la persecución de un nuevo proyecto siempre surgira algo diferente y creativo.

15. Respeto por el proceso de aprendizaje del otro. Significa que nada está determinado ni terminado, el ser humano es cada uno, unico e irrepetible y en esa unicidad está tambien las diferentes formas de aprender y de transcurrir en un proceso. El mentor debe practicar la paciencia y encontrar el ritmo de su mentee sin dudar de su potencial.

Les deseo mucho éxito a todos los que en este programa están participando y los exhorto a todos los demás, a implementar un programa de *mentoring* en sus empresas donde a través de la práctica se desarrollan habilidades de liderazgo, integración, aprendizaje y enseñanza, caminar en la persecución de mejores relaciones, generando una mejor comunidad. ■

"Existen causas que evitan todas las confusiones: pensar lo que deseamos, decir lo que pensamos, hacer lo que decimos y desear lo que está en nuestro potencial"

Mónica Rodríguez,
Coach de Seguridad en Universidad de las Américas Puebla (UDLAP) y Tec de Monterrey, facilitadora del desarrollo del potencial humano.

Más sobre el autor:

ACONTECIMIENTOS DE LA INDUSTRIA DE **LA SEGURIDAD PRIVADA**

Fecha:
01 de junio de 2022.

Lugar:
Universidad del Claustro de Sor Juana, Ciudad de México.

Bernardo Gómez del Campo presenta el *"Manual de Inteligencia y Seguridad en la lucha contra el crimen organizado"*

Bernardo Gómez del Campo Díaz Barreiro presentó su *"Manual de Inteligencia y Seguridad en la lucha contra el crimen organizado"*, un análisis cualitativo del crimen organizado en sus diferentes modalidades, ya que a lo largo de su trayectoria en el campo de la seguridad, fue recabando información respecto al combate del crimen organizado, y derivado del trabajo de investigación realizado en Misiones Regionales de Seguridad, en donde se realizó el análisis de la problemática, Díaz del Campo logró conjuntar toda esa información con su expertise y aprendizaje.

Dentro del evento también se llevó a cabo un acto protocolario de la asociación civil Misiones Regionales de Seguridad, en el cual su presidente y fundador Bernardo Gómez del Campo cedió la responsabilidad del cargo que ostentó durante 17 años, al Capitán Salvador López Contreras. ■

Paolo Pagliai, director de Derechos Humanos y Derecho de la Universidad del Claustro de Sor Juana; **Bernardo Gómez del Campo,** autor del Manual; y **Jafet Arreola,** investigador social

Fecha:
09 de junio de 2022.

Lugar:
Ciudad de México.

Seguridad en América realiza *Roadshow* **"Seguridad en la industria farmacéutica"**

Seguridad en América (SEA) llevó a cabo el *Roadshow* dedicado a la seguridad en la industria farmacéutica, donde múltiples expertos compartieron información precisa sobre las necesidades de esta industria, estrategias implementadas y las soluciones más innovadoras del mercado. El evento fue presentado y dirigido por Alex Parker, *Sales Manager* de esta casa editorial.

CHARLAS MAGISTRALES

Adrián Álvarez Delgado, *Dir. Supply Chain Security* de MSD Pharmaceuticals, dictó su conferencia titulada "La importancia de la profesionalización del ejecutivo de seguridad después de tiempos de COVID-19", en la que habló acerca de cómo la situación de la pandemia ha afectado en diferentes ámbitos al ser humano y la sociedad mundial. "A pesar del cercano regreso a las actividades presenciales, ya nada será igual", enfatizó.

Adrián Álvarez Delgado,
Dir. Supply Chain Security de MSD Pharmaceuticals

También participó Eduardo Téllez, *Chief Security Officer* en Laboratorios Liomont, con su ponencia titulada "Seguridad paralela a productos estratégicos y no estratégicos", enfocada en identificar los activos estratégicos para la operación de la industria. Los recursos con los que se cuenta para la operación: a) agua potable, b) drenaje, c) electricidad, d) sistema de gas.

PATROCINADORES

Más adelante participó Alejandro Espinosa, PACS *Director of Sales* en LAM North de HID Global, con su ponencia "Sistemas de control de acceso: ¿Seguridad de por vida?", en la que explicó acerca de la evolución de la credencial en el mercado, a través de la seguridad y funcionalidad.

Alejandro expuso que las generaciones de control de acceso y su tecnología 2ª generación Mifare fue diseñada para transporte público,

Eduardo Téllez,
Chief Security Officer en Laboratorios Liomont

sin embargo, muchos lo han utilizado para control de acceso, cuando no es una buena práctica y no es tecnología vigente, además que son muy fáciles de clonar, en cuanto a la 3ª generación se les integró también un objeto criptográfico, el cual permite que la tecnología tenga una renovación en cuestiones de caducidad tecnológica.

Posteriormente participó Martín Yánez, *Sales Manager* para Latinoamérica de Nedap, con su ponencia "Cómo impacta el control de vehículos en la industria farmacéutica", en la que habló acerca del portafolio de soluciones que ofrecen al mercado, como fabricantes de lectoras y periféricos, que a su vez están divididos en cuatro familias, cada una con tags valiosos enfocados a las diferentes necesidades:

1.
TRANSIT: tecnología activa, no necesita conexión directa, ya que cuenta con su propia batería. Trabaja bajo ambientes rudos.

2.
UPASS: de tecnología pasiva UHF (tecnología muy utilizada en la industria farmacéutica).

3.
NVITE: lector multi-tecnología.

4.
ANPR LUMO: lectora de placas. Nedap cuenta con protocolos OSDP y protocolo Wiegand, dependiendo del nivel de seguridad y las necesidades del cliente es como integran sus sistemas. ■

Fecha:
del 21 al 23 de junio de 2022.

Lugar:
Ciudad de México.

Asistentes:
más de 350 participantes por día.

Seguridad en América organiza *Roadshow* **"Seguridad en bancos"**

José Manuel Díaz-Caneja, director de seguridad en BBVA; **Maribel Cervantes,** directora de Seguridad en HSBC; **Alex Parker,** *Sales Manager* de SEA; y **Samuel Ortiz Coleman,** director general de SEA

Seguridad en América (SEA) llevó a cabo el *Roadshow* "Seguridad en bancos", presentado por Samuel Ortiz Coleman, director general de SEA; y Alex Parker, *Sales Manager*.

DÍA 1

La charla magistral "Relevancia de la capacitación y concientización en la seguridad bancaria", del primer día del ciclo de conferencias estuvo a cargo de Javier Hernández, director de Seguridad para Banorte, junto con Ciro Ortiz, director general de SEPROBAN.

César Santillán, gerente de Preventa de SISSA, participó con la ponencia "La importancia de las soluciones de seguridad física en el sector bancario". Mientras que Alexcy Poveda, *Industry and Producto Manager* de GENETEC, habló sobre la "Seguridad Bancaria a otro nivel".

Luis De Rosa, gerente comercial de SoftGuard, participó con la ponencia "Las personas son parte fundamental del sistema de seguridad en las instituciones bancarias". Maribel Cervantes, directora de Seguridad en HSBC; y José Manuel Díaz-Caneja, director de Seguridad en BBVA, hablaron sobre el "Análisis de riesgo para la seguridad bancaria".

DÍA 2

Juan Manuel Ramírez, subdirector de Seguridad para CI Banco, habló de la importancia que tiene en la actualidad la seguridad en el negocio bancario, lo cual incluye principalmente el tener una visión de seguridad física enfocada en certificación y evaluación de lo que pase en el negocio para tener una buena atención al usuario y cliente.

Omar Orozco, coordinador comercial en Adises; y Víctor Calderón, *Sales Manager* de NVT Phybridge México, expusieron "Rompiendo el paradigma en la implementación de seguridad IP en instituciones bancarias". Alberto Pérez, *Sales Director* Latam de SCATI, dio a conocer la conferencia "El video como palanca transformadora del negocio: aplicaciones prácticas en la banca".

Arturo Martínez, director general adjunto de MSPV, dictó la ponencia "La gestión de riesgos y el valor agregado a los negocios bancarios". Selene Molina, gerente de Seguridad de Bancoppel, junto con Hugo Montes, director de Seguridad en CIBANCO, hablaron sobre los delitos cibernéticos más comunes en la actualidad.

DÍA 3

Luis Meza, director de Seguridad en Citibanamex; y Fernando Gómez, director de Seguridad de Compartamos Banco, hablaron sobre cómo llevar a cabo una planeación estratégica del área de Seguridad.

Diego de la Torre, subdirector de Seguridad en BanBajío; y Pedro Villanueva, director de Seguridad en Grupo Financiero Inbursa, hablaron sobre los diferentes tipos de fraudes y estafas bancarias en la actualidad.

Pablo Villas, *Sales Director Latin American & Caribbean* de Everbridge, habló sobre la gestión de eventos críticos en bancos a través de su solución "Control Center".

Jorge Uribe, director comercial de IPS, habló sobre las medidas para fortalecer la seguridad en entornos bancarios. Marco Castillo, director comercial de CAME; y Óscar Pérez, gerente de Producto, hablaron sobre las herramientas de seguridad de alto impacto que ofrece la firma para las instalaciones bancarias. ■

Fernando Gómez, director de Seguridad de Compartamos Banco; y **Luis Meza,** director de Seguridad en Citibanamex

Fecha:
14 de junio de 2022.

Lugar:
Museo de Memoria y Tolerancia, Ciudad de México.

Conferencia de prensa previa a **Expo Seguridad México 2022**

Jorge Hagg,
director de Expo Seguridad México

Expo Seguridad México, el evento que convoca a los especialistas y a los interesados en actualizarse en temas de seguridad pública y privada, llevó a cabo una conferencia de prensa en la que anunció las particularidades de su décima novena edición, donde se mostraron los más recientes avances tecnológicos, soluciones y productos, a los usuarios, integradores, distribuidores nacionales e internacionales y al público en general.

El encuentro con periodistas contó con la presencia de Perla Liliana Ortega Porcayo, presidenta de Iniciativa Chapultepec A.C. "Seguridad por México", y Gildardo Avendaño Osogobio, director de GA Consulting, ambos especialistas en temas de seguridad, acompañados del mismo director de Expo Seguridad México, Jorge Hagg. ■

FFecha:
23 de junio de 2022.

Lugar:
Ciudad de México.

AXIS Communications presente en Expo Seguridad México 2022

Axis Communications brindó una conferencia de prensa previa a su participación en Expo Seguridad México 2022, en la que mostró algunas de sus más recientes soluciones e innovaciones tecnológicas para la industria de la seguridad.

En la conferencia de prensa presentada por Manuel Zamudio, gerente de Asociaciones Industriales, junto con Alejandro Aguirre, *National Sales Manager* México & CCA de Axis, mostraron las tecnologías que estarán próximamente disponibles para el mercado latinoamericano. Algunas de los desarrollos tecnológicos que comentaron fue acerca del Chip ARTPEC, un dispositivo de procesamiento de video que proporciona la base para capacidades esenciales como calidad de imagen, funciones de análisis y rendimiento de codificación. ■

Fecha:
24 de junio de 2022.

Lugar:
Jardines de Santa Fe, Ciudad de México.

Asistentes:
más de 150 invitados.

AMESP celebra su décimo aniversario

La Asociación Mexicana de Empresas de Seguridad Privada (AMESP) celebró su décimo aniversario de fundación, una gran celebración para la asociación que se creó con el fin de unificar a las empresas más serias y comprometidas del sector de la seguridad privada en México.

El evento de gala tuvo grandes invitados especiales, entre ellos la diputada Juanita Guerra Mena; Ignacio Hernández Orduña, DSP de la SSPC; el Gral. de Brigada D.E.M. Retirado Arturo Medina Mayoral en representación del Comte. Luis Rodríguez Bucio de la Guardia Nacional; el General de División DEM Ret. Audomaro Martínez Zapata, director general del Centro Nacional de Inteligencia; Mario Torres López, titular de la Unidad de Asuntos Jurídicos e Igualdad de Género en representación del Secretario de Seguridad del Estado de México; Ricardo Díaz González, gerente de Crédito del Infonavit, entre otros, encabezados por el Cap. Salvador López Contreras, presidente actual de la AMESP. ■

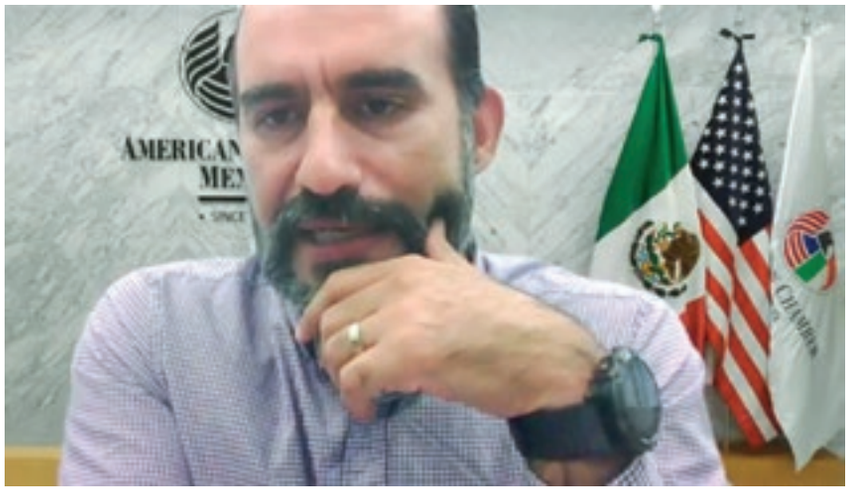
Fecha:
11 de junio de 2022.

Lugar:
Ciudad de México.

American Chamber México presenta las **"Tendencias criminales en Latinoamérica"**

American Chamber México organizó el evento en línea "Tendencias criminales en Latinoamérica", el cual fue presentado por Raúl Rojas, gerente regional de Seguridad Corporativas Américas en Cemex. El primer experto fue Rudy García, quien habló del panorama general de Latinoamérica en cuestiones de violencia y estallidos sociales que afectan directamente la economía y las operaciones de la cadena de suministro en toda la región.

También participó Julián Puentes, hablando sobre la reactivación económica pospandemia COVID-19; por su parte, Mario Arroyo Juárez comentó sobre la violencia en México, y como experta finalista en el foro, Iliana Fernández, *Regional Security Manager Central-LATAM and Caribbean* en Microsoft Corp., explicó que el contexto violento de la región ha sido un factor determinante para la seguridad de cada país y las organizaciones. ■



Fecha:
06 de julio de 2022.

Lugar:
Hotel W, Ciudad de México.

Asistentes:
más de 30 participantes.

CAME PARKARE, innovación en la gestión de estacionamientos inteligentes

La línea de negocio especializada en soluciones para estacionamientos inteligentes de Grupo CAME; CAME PARKARE convocó a líderes de la cadena de valor del sector involucrados directamente en el desarrollo, gestión y operación a ser parte de Route Parkare, una sesión de debate disruptiva, entre los conferencistas estuvo el coordinador general operativo COPEMSA de los tres estacionamientos que conforman el Aeropuerto Internacional de la Ciudad de México (AICM), Nicolas León.

Siendo su primera edición la reunión fue inaugurada por Francisco Sánchez, director general para CAME México, quien comentó que estos espacios son fundamentales para estrechar relaciones entre socios y estar al día sobre las tendencias y necesidades en los estacionamientos. Durante la sesión se compartieron diferentes enfoques, que van desde la relación capital humano y tecnología hasta estrategias de experiencia de usuario a través de la innovación digital. ■

Fecha:
14 de julio de 2022.

Lugar:
Voluntariado Popotla, Ciudad de México.

SEA y los patrocinadores de **"Los 100"** entregan donativos al Voluntariado Popotla de la SEDENA

Seguridad en América (**SEA**) mediante su director general, Samuel Ortiz Coleman, encabezó la entrega de donativos para el Voluntariado Popotla, por parte de empresas de seguridad privada, recopilados en el evento "Los 100 más influyentes de la seguridad privada en México" organizado por SEA en marzo de 2022, y que fueron donados para el Hospital Central Militar (HCM), el Centro de Rehabilitación Infantil (CRI) y al propio Voluntariado Popotla de la Secretaría Nacional de la Defensa (SEDENA). En total fueron 33 sillas de ruedas, seis *smartphones*, cuatro iPad y cinco *laptops*.

En representación de la titular del voluntariado, Belinda Judith Solís Cámara, estuvo Gloria Padilla Covarrubias, además de algunos directores de las empresas donadoras: Pedro Sanabria, director de Trust Group; Gustavo Espinosa, director de GSI Seguridad Privada; Josué Ramírez y el Cap. Salvador López, ambos de CIA KAPITAL; Gerardo Macías, director general de Protectio; y Marcos Solórzano, CEO de SOLCAT. ■

Fecha:
13 de julio de 2022.

Lugar:
Ciudad de México.

Seguridad en América organiza *Roadshow* **"Nuevo perfil de guardias y protección ejecutiva"**

Samuel Ortiz Coleman, director general de SEA; **Ivan Ivanovich, Gonzalo Senosiain** y **Pablo Ortiz-Monasterio,** organizadores de EP SUMMIT

Seguridad en América (SEA) llevó a cabo el *Roadshow* "Nuevo perfil de guardias y protección ejecutiva", presentado por Samuel Ortiz, director general de SEA; y Alex Parker, Sales Manager de la misma casa editorial.

CONFERENCIAS COMERCIALES

Juan Carlos Camacho, director de Seguridad Patrimonial de Grupo Lala, participó con la conferencia "Nuevo enfoque de la seguridad integral en México en tiempos pospandemia".

Patricia Fresnedo, directora ejecutiva de Operaciones para Latam; y Rigoberto Estrada, gerente senior de Operaciones de Emergencias Latam de FirstCall, iniciaron el ciclo de conferencias comerciales con el tema "El impacto de los centros de operaciones de seguridad (GSOC) en la protección ejecutiva y el perfil del agente de protección".

Virginia D'Errico, directora comercial de SoftGuard, habló sobre las "*Apps* y tecnología para la seguridad ejecutiva"; mientras que Jonathan Ávila Sánchez, *Country Manager* para México y Centroamérica, expuso "El valor de la inteligencia de riesgo en la protección ejecutiva, conocimiento de amenazas en 360°, inteligencia para tomar medidas informadas".

Jonathan Ávila Sánchez, *Country Manager* para México y Centroamérica de Everbridge, con la ponencia "El valor de la inteligencia de riesgo en la protección ejecutiva, conocimiento de amenazas en 360°, inteligencia para tomar medidas informadas".

Pablo Ortiz-Monasterio, Gonzalo Senosiain e Ivan Ivanovich hablaron sobre el tema: "¿Estás preparado para conocer los conceptos de los que nadie habla en protección de personas?". Ivanovich explicó cómo es que ya no hay confianza en la protección ejecutiva y es un testimonio generalizado por usuarios, lo que busca Executive Protection Summit es marcar tendencias que permitan ofrecer respuestas a problemas que la protección ejecutiva enfrenta.

Enrique Tapia Padilla, socio director de Altair Security Consulting & Training, presentó la conferencia "¿Tenemos a nuestros ejecutivos protegidos?". ■

Cap. Salvador López Contreras, presidente de AMESP

CONVENIO DE
COLABORACIÓN

PARA UN TRABAJO EN CONJUNTO POR LA CULTURA DE LA SEGURIDAD

SEGUIMOS PROMOVIENDO INICIATIVAS QUE ABRAN ESPACIOS AL DIÁLOGO, LA COLABORACIÓN Y LAS ACCIONES QUE CONTRIBUYAN A UN MÉXICO MÁS SEGURO.

/SeguridadPorMexico

@segpormexico

/in/seguridad-por-méxico-

SEGURIDAD POR MÉXICO

CNB

CONSEJO NACIONAL
DE LA INDUSTRIA DE LA BALÍSTICA®
"TRANSFORMANDO LA INDUSTRIA DEL BLINDAJE"

Súmate a nuestra comunidad por que #JuntosHacemosSeguridad

Fecha:
27 de julio de 2022.

Lugar:
Ciudad de México.

Asistentes:
más de 300 cibernautas.

Seguridad en América organiza *Roadshow* **"Soluciones contra incendios"**

Jaime A. Moncada,
director general de IFSC

Seguridad en América (SEA) llevó a cabo por primera vez un *roadshow* enfocado en las soluciones contra incendios más innovadoras en el mercado, el evento online estuvo dirigido por Samuel Ortiz Coleman, director general de la casa editorial; y Alex Parker, *Sales Manager.* La ponencia magistral estuvo a cargo del experto Jaime A. Moncada, director general de International Fire Safety Consulting (IFSC), con la ponencia titulada "Actualización en seguridad contra incendios, ¿qué está pasando?".

"En los años 80, en Estados Unidos sucedían tres millones de incendios al año, hoy en día hay 1.3 millones es decir, hay un 30% de incendios que habían hace 40 años", señaló el experto. Pese a que la población ha aumentado, los incendios han disminuido, esto se debe a que "es un país donde las cosas se están protegiendo bien, donde hay un ingeniero independiente al instalador, el cual es un instalador calificado, donde hay una autoridad competente que recibe y acepta los sistemas, y hay un usuario educado, estos son los cuatro pilares de la protección contra incendios que son totalmente independientes", señaló.

SISSA: PROYECTO TORRE SCOTIABANK

La siguiente conferencia estuvo a cargo de Elías Valencia Trejo, director comercial de SISSA Infraestructura; y Daniel Hernández García, director de Operaciones de Sistemas Contra Incendios en la misma firma, quienes hablaron sobre el "Proyecto de modernización de la Torre Scotiabank" en la Ciudad de México.

El proyecto fue liderado por la constructora líder GIA y SISSA lo ganó con sus soluciones contra incendios, quienes fueron felicitados por sus buenos resultados. SISSA diseña, implementa y gestiona proyectos llave en mano de infraestructura, estableciendo sólidas relaciones comerciales con sus socios de negocio.

Por último, Zeferino Guzmán, consultor en Seguridad Corporativa, quien habló sobre la importancia del mantenimiento contra incendios en la industria. También se contó la participación de José Arturo Ortega Porcayo, presidente de NFPA Capítulo México, A.C., quien comentó que dicha asociación sigue trabajando y profesionalizando a sus afiliados con diferentes cursos y eventos, destacando que una de las ventajas de pertenecer a esta es que la integran tanto fabricantes, proveedores como usuarios finales, y así se puede tener un panorama más amplio de las necesidades del mercado.

Para finalizar el *roadshow*, Aurora Paniza, coordinadora de Eventos en la Asociación Latinoamericana de Seguridad (ALAS), hizo una extensa invitación para afiliarse a ALAS y continuar profesionalizándose en el sector de la seguridad. ■

COMPROMETIDOS CON LA SEGURIDAD DE NUESTROS CLIENTES Y LA CALIDAD EN EL SERVICIO

Capacidades globales
Con experiencia local

Nuestros Servicios:

- **Personal de Seguridad**
- **Asesoría de Riesgos**
- **Servicios de Tecnología**

Es nuestro honor estar allí para usted; quedarse un paso por delante de las amenazas en evolución.

Contáctanos

www.ausecurity.mx

(+52) 55 5337 0400

ALLIED UNIVERSAL®
SECURITY SERVICES
There for you.

Genetec es reconocido como líder en la expansión del mercado global de *software* de videovigilancia

Según el último informe de la organización de investigación Omdia, Genetec, proveedor de tecnología de soluciones unificadas de seguridad, seguridad pública, operaciones e inteligencia de negocios, sigue siendo reconocido como el líder mundial en *software* de videovigilancia. El alcance del informe de este año se amplió para incluir VSaaS (videovigilancia como servicio) por primera vez, y Genetec atribuye su continuo liderazgo en el mercado al desarrollo de soluciones en la nube innovadoras y flexibles, y a la solidez de su plataforma de seguridad unificada, Genetec™ Security Center. "Nuestra plataforma de seguridad abierta y unificada respalda algunos de los sistemas de gestión de video más sofisticados y exigentes del mundo", dijo Guy Chenard, director comercial de Genetec. ■

Fortinet abre nuevo Centro de Atención Técnica en Colombia

Fortinet anunció la apertura de su nuevo Centro de Asistencia Técnica (TAC, por sus siglas en inglés) en Colombia. Este centro, que llega a reforzar la presencia de los puntos de soporte técnico en América ubicados en Vancouver, Ottawa, Florida, Ciudad de México y Uberlandia en Brasil, se encuentra ya operativo y tiene planes para finales de año de expandir su operación con 80 ingenieros en ciberseguridad. Para los próximos cinco años, Fortinet espera llegar a 170 expertos de soporte en ciberseguridad en el TAC de Colombia, respondiendo así a la creciente demanda de los servicios de ciberseguridad de Fortinet dentro de un tercio de las zonas horarias del mundo que cubren el continente americano. ■

Darktrace y **HackerOne** se asocian para sumar IA a Attack Resistance

Darktrace y HackerOne se asociaron para combinar la tecnología PREVENT/Attack Surface Management de Darktrace con las capacidades de evaluación continua de la seguridad de la plataforma HackerOne. La asociación amplía la iniciativa OpenASM de HackerOne y cumple con una visión compartida con Darktrace para ayudar a las organizaciones a asegurar su patrimonio digital a través de tecnología líder y una comunidad de hackers éticos. HackerOne reconoció la necesidad de un socio ASM que pudiera mejorar los esfuerzos de descubrimiento y reconocimiento de activos de la comunidad de *hackers* de HackerOne. La combinación de IA y experiencia en seguridad ofrecerá una visión continua y ayudará a las organizaciones a encontrar y eliminar los puntos ciegos. ■

hackerone

Hirotec reduce los costos de red en un 50% durante la actualización de la vigilancia IP

Hirotec, fabricante de automóviles, quería mejorar sus capacidades de vigilancia en una de sus plantas más activas en México. Sin embargo, los requisitos de preparación de la red amenazaban el proyecto de transformación digital con elevados costos e interrupciones de la actividad. Tras haber utilizado las soluciones de red de NVT Phybridge en el pasado, el Grupo SITE recomendó el *switch* Power over Ethernet FLEX. El *switch* PoE de largo alcance de NVT Phybridge FLEX suministra Ethernet y PoE++ a través de cualquier infraestructura UTP multipar nueva o existente con un alcance de hasta 610 m, seis veces más que los switches estándar. El integrador realizó una demostración exhaustiva en las instalaciones del cliente. ■

HID Global se asocia con Asygn para probar tecnología en la energía renovable

HID Global, en asociación con GE Hydro y Asygn, desarrolló una solución de etiquetas RFID inteligentes y robustas que permiten a los clientes del sector de la energía renovable optimizar la disponibilidad y evitar interrupciones no planificadas. El resistente diseño de la etiqueta abre perspectivas de uso en aplicaciones industriales. "Tanto la colaboración con HID Global como el proyecto fueron excelentes, y esto porque GE se concentró en las restricciones, el contexto de uso y el procesamiento y modelado de los datos, mientras que HID se centró en los requerimientos de diseño de la etiqueta, de manera que cumpliera con todas las especificaciones de rendimiento e integridad en entornos muy adversos", aseguró Vincent Bouillet, responsable de IIoT (Internet Industrial de las Cosas) y Desarrollo de tecnologías avanzadas de GE Renewable Energy Hydro. ■

Eagle Eye Networks presenta Smart Video Search

Eagle Eye Networks presentó Eagle Eye Smart Video Search, una nueva función para todos los clientes que hace que la búsqueda de video sea rápida y fácil como buscar en la web. Integrada en Eagle Eye Cloud VMS (sistema de gestión de video), Smart Video Search permite a los clientes buscar rápidamente en todas las cámaras y todas las ubicaciones y encontrar al instante el video exacto que buscan, así como compartir rápidamente las secuencias de video. No hay ninguna cuota de suscripción adicional, y no se necesitan cámaras especiales, *hardware* adicional ni instalación local. Mejora la seguridad y las operaciones en el comercio minorista, ciudades inteligentes, aparcamientos inteligentes, centros educativos, procesos de fabricación, logística, hostelería, centros sanitarios, y en cualquier lugar donde haya cámaras de seguridad. ■

Johnson Controls anuncia el lanzamiento de C•CURE 9000 v 3.0

Johnson Controls lanzó su innovador sistema de administración de eventos y control de acceso C•CURE 9000, que "es uno de los sistemas de gestión de seguridad más potentes del mercado, brinda protección y seguridad 24/7 para personas, edificios y activos", afirmó Luis Delcampo, LATAM *Product Marketing Manager*–Control de Acceso de Johnson Controls. Algunas de sus características son: compatibilidad con OSDP para las comunicaciones entre lectores y controladores de la serie iSTAR Ultra; admite hasta 5 mil lectores por servidor individual y 60 servidores de aplicaciones satélite para sistemas Enterprise; el cual permanece operativo durante todo el proceso de actualización con soporte de *software* multi-versión; su capacidad de acceso a C•CURE 9000 desde cualquier navegador de Internet con C•CURE Web. ■

Celebra el **CNB** su 5° aniversario y busca crecer más del 30% como sector

El Consejo Nacional de la Industria de la Balística (CNB) celebró su 5° aniversario teniendo como su principal propósito al agrupar a las empresas más representativas de su especialidad en áreas como el blindaje de vehículos de uso civil y táctico, blindaje arquitectónico, blindaje corporal, y en la fabricación de vidrios blindados y de materiales balísticos. "Hemos alcanzado un crecimiento de 30% en comparación de hace 20 años, cuando iniciamos en forma organizada; desde entonces nos hemos profesionalizado para atender la situación de inseguridad que vive el país", explicó Ignacio Baca Torres, presidente de la Comisión Ejecutiva del organismo. Su mesa directiva se compone además con Luis A. Sánchez Soto, como secretario; Daniel Portugal, como tesorero y asesor; y René Fausto Rivera, responsable de realizar enlaces con autoridades y asociaciones. ■

incluye gastos de envío

SUSCRÍBASE HOY MISMO A

Revista **SEGURIDAD EN AMÉRICA**

VERSIÓN IMPRESA

DE ACUERDO AL PAÍS EN QUE RADIQUE SELECCIONE LA OPCIÓN DESEADA. (Marque así X)

	Envío a México	Envío a otros países
Suscripción a la revista por un año (6 ejemplares)	☐ $ 650 MN	☐ $ 270 dólares
Suscripción a la revista por dos años (12 ejemplares)	☐ $ 1,250 MN	☐ $ 530 dólares
Ejemplares atrasados	☐ $ 130 MN	☐ $ 50 dólares
Directorio de Seguridad SEA 2022	☐ $ 550 MN	☐ $ 120 dólares

FORMAS DE PAGO:

☐ Depósito en banco HSBC a nombre de Editorial Seguridad en América, S.A. de C.V. Cuenta 04016012049

☐ Cargo a tarjeta de crédito o débito.

No. de cuenta: _____ Fecha de vencimiento: _____ Código: _____

☐ Transferencia bancaria: Clabe 021180040160120491

_____
Firma

DATOS DEL CLIENTE (para el envío de la revista):

Nombre: _____

Compañía: _____ Cargo: _____

Calle: _____ No. _____ Colonia _____

Delegación _____ C.P. _____

Ciudad / Estado / Provincia / Departamento _____ País _____

Tel: _____ E-mail corporativo: _____

E-mail personal: _____

DATOS DE FACTURACIÓN:

Razón social: _____ RFC: _____

Dirección fiscal: _____

E-mail para envío de factura electrónica: _____

MÉTODO DE PAGO

☐ Transferencia
☐ Depósito
☐ T. de crédito

Para mayor comodidad y rapidez, favor de enviar este formato vía: →

e-mail: telemarketing@seguridadenamerica.com.mx

Cupón válido del 1 de enero al 31 de diciembre de 2022

PROTECCIÓN DE DATOS PERSONALES

Para garantizar la protección de datos personales y la privacidad, hasta la fecha, 107 países y varios estados de Estados Unidos han establecido una legislación teniendo como ejemplo el Reglamento General de Protección de Datos (GDPR) de Europa, sin embargo pese a las multas que ha emitido, sólo el 59% de las organizaciones dicen que cumplen con todos los requisitos de GDPR. Países como México aún tienen un camino largo por recorrer en este campo, no obstante le presentamos a continuación guía práctica sobre cómo las organizaciones pueden proteger sus operaciones de una manera que respete la privacidad de todos, elaborada por Genetec Inc. (enero de 2022).

NO PIENSE "A MÍ NUNCA ME VA A PASAR"

1. **Establecer la gobernanza de la privacidad.** Designe un delegado de Protección de Datos para orientar las estrategias y cumplir con la normativa. Mapee cómo se recopilan y procesan los datos, dónde se almacenan, cuánto tiempo se conservan y quién puede acceder a ellos. Identifique a las personas ajenas a su organización que puedan necesitar acceder a sus datos y evalúe el riesgo que sus operaciones de procesamiento de datos representan para los derechos de los ciudadanos.

2. **Construir una estrategia de protección de datos.** Lleve a cabo un análisis de brechas de las operaciones de procesamiento de datos. Evalúe la capacidad de los sistemas existentes para abordar la privacidad sin agotar los recursos. Implemente nuevos procesos según sea necesario y documente sus políticas y procedimientos de privacidad. Eduque a toda su fuerza laboral sobre las mejores prácticas de ciberseguridad y privacidad.

3. **Evaluar las capacidades de la tecnología y los socios.** Busque proactivamente a aquellos que puedan ofrecer ayuda para mantener la privacidad y la protección. Infórmese sobre las certificaciones y los pasos que los socios y proveedores están tomando para cumplir con la legislación de privacidad. Elija soluciones creadas con privacidad por diseño, que habiliten funciones de privacidad de forma predeterminada.

4. **Construir sistemas de seguridad teniendo en cuenta la privacidad.** Habilite múltiples capas de defensa para proteger la información personal recopilada por los sistemas de seguridad física. Defina el acceso de los usuarios para restringir quiénes pueden iniciar sesión en las aplicaciones y qué pueden ver/hacer. Implemente funciones de privacidad como la anonimización de videos que difumina las identidades en las imágenes.

5. **Permanecer alerta.** Manténgase actualizado sobre las leyes de privacidad de datos y evolucione las políticas y los procesos con regularidad. ■

FOMENTE LA CULTURA DE LA SEGURIDAD
Consulte la revista digital en
www.seguridadenamerica.com.mx y envíe los tips a sus amistades y/o empleados.

SEGURIDAD EN AMERICA

ÍNDICE DE ANUNCIANTES

Foto: Cortesía Alberto Friedmann

Alberto Friedmann,

*director general de Procesos Automatizados **(PROSA)***

Seguridad en América (SEA): como experto, ¿cuáles considera que son los principales problemas de seguridad en el país?

Alberto Friedmann (AF): la seguridad es y ha sido uno de los principales retos para el país en los últimos 20 años; particularmente hay un fuerte rezago y carencia de planificación, administración y de estrategias públicas adecuadas para enfrentar esta situación. También existe debilidad en el despliegue de recursos, tanto humanos como materiales, para realizar labores de inteligencia y contra inteligencia, punto medular para monitorear y analizar los resultados que se obtienen a partir de la implementación de esta serie de estrategias integrales de seguridad.

SEA: ¿Cuáles son los servicios que ofrece PROSA para contrarrestar esos problemas?

AF: PROSA ofrece dentro de su cartera de productos, soluciones automáticas y sistemas inteligentes para la seguridad de nuestros clientes. Por una parte, en las áreas de la seguridad física, con el control y evaluación junto con la recolección automática de datos para operar y monitorear en tiempo real el acceso peatonal y vehicular que ayude a mejorar e incrementar los niveles de seguridad en temas como robo de activos, mercancía y el ingreso no autorizado de personas ajenas a un sitio.

SEA: ¿Cuáles son los diferenciadores de PROSA respecto a la competencia?

AF:

- **Proximidad y cercanía con nuestros clientes.** La empresa antes de proponer o presentar una solución integral y automática de seguridad, donde la mayoría de las soluciones en el mercado son inflexible y acotadas, comprende, entiende, conoce y descubre las necesidades reales del cliente.
- **Veracidad, certeza y confianza.** Nuestros productos y soluciones se basan en estas tres características de lo que el cliente busca y de lo que en realidad necesita.
- **Sincronizar el modelo de negocio del cliente con las soluciones.** Esto tiene como finalidad promover un retorno de inversión (ROI), integrando los sistemas a un entorno de productividad acorde con la dinámica operativa del cliente con resultados planificados basados en objetivos reales.

SEA: ¿Puede compartirnos algunos aspectos que un usuario final debe considerar al momento de contratar una solución de control de acceso?

AF: seguridad, eficiencia, sencillez, actualidad, sincronización con su operación, necesidades y entorno, con soluciones que generen productividad y un retorno de inversión concreto.

SEA: Platíquenos un poco sobre su experiencia profesional y su experiencia en PROSA.

AF: tengo más de 30 años de experiencia en la industria de la seguridad data, inicié con actividades y tareas de diseño e instalación de sistemas tecnológicos de seguridad; he fundado y dirigido otras empresas en los ámbitos de diseño y manufactura de *hardware*, automatización, soluciones y plataformas de alta tecnología, *software* especializado y recientemente en el área de Ciberseguridad Corporativa.

Actualmente PROSA atiende diferentes verticales de negocio abarcando la Seguridad del Proceso Productivo como un concepto central dentro del cual, se operan, integralmente y se califican: accesos, presencia, asistencia, control de objetos, control de vehículos y control de contenidos, tanto física como virtual. ■

Roadshows online 2022

ENERO
- Soluciones de Seguridad para *Retail*
  26

FEBRERO
- Gestión de Seguridad en Aeropuertos
  09
- Técnicas en Pruebas de Confianza e Investigaciones
  23

MARZO
- Seguridad en la Industria Manufacturera
  09
- Seguridad en Logística y Custodia de Mercancía
  23
- **Los 100 más Influyentes de la Seguridad Privada**
  (Evento presencial)
  26

ABRIL
- Seguridad en Casas de Empeño
  06
- Centrales de Monitoreo y GPS
  27

MAYO
- Seguridad en Parques Industriales
  11
- Seguridad en Centros Educativos
  25

JUNIO
- Seguridad en la Industria Farmacéutica
  08
- Seguridad en Bancos
  21, 22 y 23

JULIO
- Nuevo perfil de protección ejecutiva
  13
- Soluciones contra Incendio
  27

AGOSTO
- Seguridad en Plantas Automotrices
  10
- Seguridad en la Industria Hotelera
  24
- **Cumbre de Seguridad Corporativa**
  (Evento presencial)
  30 y 31

SEPTIEMBRE
- Seguridad en la Industria Alimentaria
  07
- Seguridad en Petróleo y Energía
  21

OCTUBRE
- Blindaje Automotriz
  12
- Soluciones de Seguridad en *Data Centers* & *TI*
  26

NOVIEMBRE
- Seguridad en Hospitales
  09
- Seguridad para Supermercados y Tiendas de Conveniencia
  23
- Seguridad en Casinos y Centros de Entretenimiento
  30

DICIEMBRE
- Seguridad en Maquiladoras
  07

Reunimos a los tomadores de decisiones de la seguridad en distintos sectores para que usted ofrezca sus productos y/o servicios por medio de conferencias dinámicas.

BENEFICIOS
- Usted podrá impartir su conferencia a más de 500 profesionales de la seguridad.
- Interactuar directamente con tomadores de decisiones.
- Promocionar sus productos y servicios.

EL PATROCINIO INCLUYE
- Base de datos de los asistentes.
- Reporte analítico de la estrategia de publicidad.
- Presentación de 30 minutos.

telemarketing@seguridadenamerica.com.mx
www.seguridadenamerica.com.mx
(55) 5572 6005

SEGURIDAD EN AMÉRICA

"SEPSISA se ha transformado en SER grande"

Facility Services

SEPSISA®

SEGURIDAD PRIVADA

El camino a la excelencia comienza por la seguridad.

- Guardias
- Comercializadora
- Limpieza
- Consultoría
- Custodia
- Seguridad Electrónica
- GPS / Monitoreo

REPSE

Registro de Prestadoras de Servicios Especializados u Obras Especializadas

CDMX, Estado de México, Monterrey, Guadalajara, San Luis Potosí, Aguascalientes, Hermosillo, Querétaro, Guanajuato, Pachuca, Puebla, Cuernavaca, Acapulco, Veracruz, Villahermosa, Mérida, Cancún, Mexicali, Chihuahua, Tijuana, Ensenada.

www.sepsisa.com.mx ventas@sepsisa.com.mx 55 5351 0402